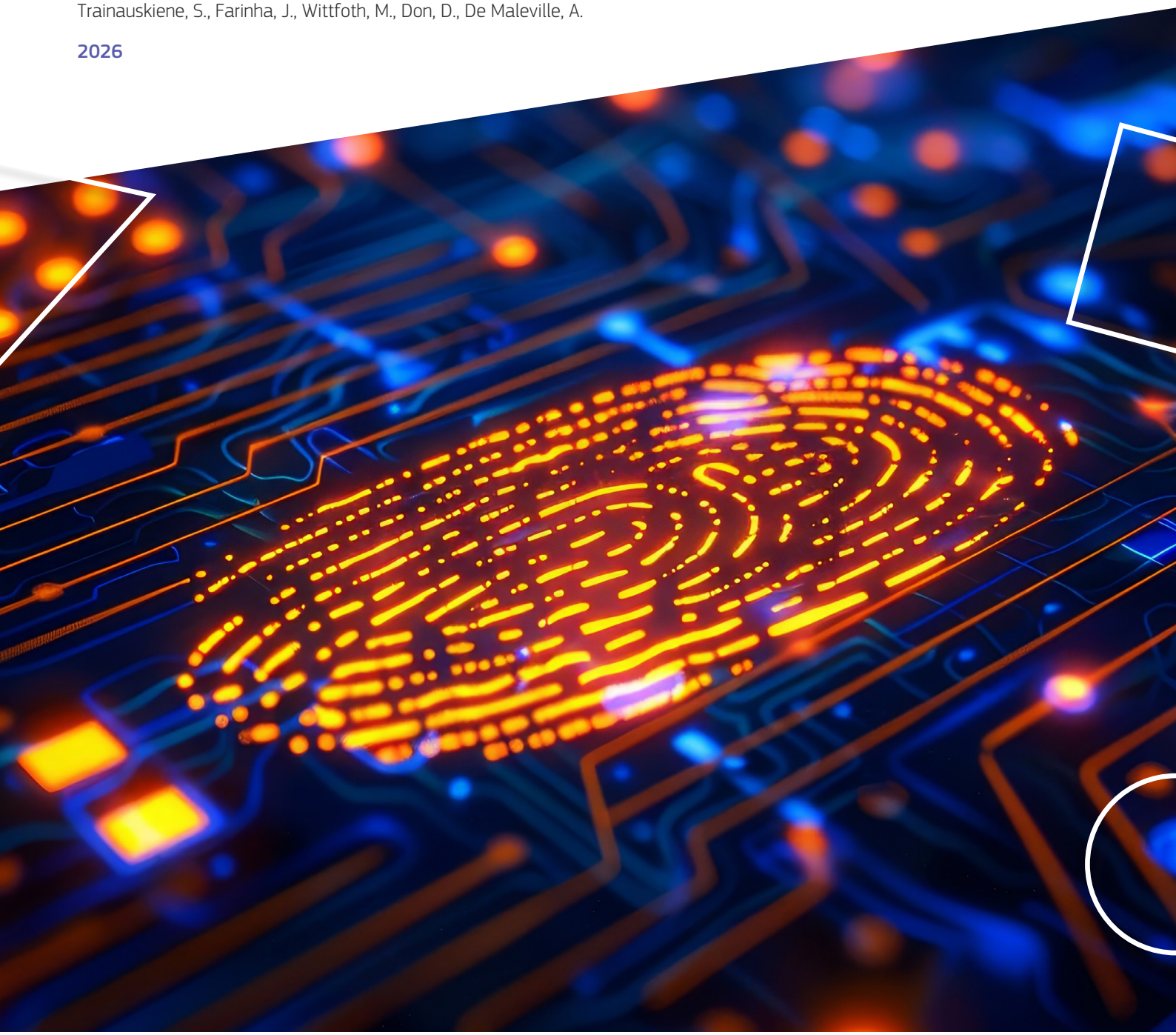
Horizon scanning on emerging privacy enhancement technologies

A participatory technology foresight exercise developed by the JRC and EUROPOL to support policy makers and law enforcement agencies

Trainauskiene, S., Farinha, J., Wittfoth, M., Don, D., De Maleville, A.

2026



European Commission

EUROPOL

Joint Research Centre
https://joint-research-centre.ec.europa.eu

EUROPOL
https://www.europol.europa.eu

JRC143326
EUR 40795

Print	ISBN 978-92-68-42190-1	ISSN 1018-5593	doi:10.2760/3743573	KJ-01-26-322-EN-C
PDF	ISBN 978-92-68-42189-5	ISSN 1831-9424	doi:10.2760/6084454	KJ-01-26-322-EN-N

Luxembourg: Publications Office of the European Union, 2026

Some content was created using AI tools, namely through GPT@JRC to summarise texts. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

How to cite this report: Trainauskiene, S., Farinha, J., Wittfoth, M., Don, D. and De Maleville, A., *Horizon scanning on emerging privacy enhancement technologies - A participatory technology foresight exercise developed by the JRC and Europol to support policy-makers and law enforcement agencies,* Publications Office of the European Union, Luxembourg, 2026, https://data.europa.eu/doi/10.2760/6084454, JRC143326.

Printed by the European Commission in Belgium

Contents

Abstract

Privacy enhancing technologies (PETs) enable data sharing and collaboration in the digital space in a way that respects privacy, ensuring that users have confidence that their data is protected. However, PETs can also be used to hide traces of criminal activities, most of which today are carried out via, or have some link to, digital communications technology. For this reason, lawful access to electronic evidence has become one of the most critical issues for European law enforcement, as it seeks to ensure safety and security while balancing this with the fundamental right to privacy.

This report presents the results of a joint horizon scanning exercise carried out by the EU Policy Lab at the European Commission's Joint Research Centre (JRC), and Europol, the EU law enforcement cooperation agency. It contributes to broader JRC efforts to support the European Commission's political priority, the 'New Era for European Defence and Security', by anticipating future technological developments. The aim of the exercise was to assess emerging PETs that could help or, conversely, hinder the future work of European law enforcement. The report underscores the importance of several PETs that experts deem crucial for this purpose.

These technologies have the potential to be either leveraged by law enforcement to enhance their operations or be exploited by criminals, depending on how they are developed and used in the future. The report also examines related complex regulatory frameworks and contextual factors that influence the development and deployment of these technologies. In light of the development of new encryption methods and other related enabling technologies such as artificial intelligence, this report also discusses new ways for law enforcement agencies to securely exchange information and integrate these technologies in the future activities.

Acknowledgements

The authors are grateful for the time and contributions of the workshop participants and the interviewees. In line with our commitment to the participants and interviewees, their names and affiliations are listed below, but no comments or statements are attributed directly:

- Adrianus Warmenhoven, Nord VPN
- Bart Preneel, KU Leuven
- Cornelia Kutterer, Considerati
- Cyril Piotrowicz, FR Gendarmerie
- Denise Mayerdorfer, Federal Ministry of Interior – Austria
- Dorine Walter, National Gendarmerie – France
- Fredrik Heintz, Linköping University
- Freek Bomhof, TNO
- Igor Nai Fovino, JRC
- Ismael Alvarez, Europol
- Johanna Laurin Gulled, Swedish Police Authority
- Juraj Kubica, DG CNECT
- Olga Batura, TNO
- Pieter Nooren, TNO
- Jürgen Freudenberger, Cyberagentur
- Kasper Rasmussen, Oxford University
- Kirsi Jauhiainen, Police of Finland
- Marjolein Lanzing, University of Amsterdam
- Miguel Fayos Mestre, Guardia Civil – Spain
- Mihai Tiganus, Romanian Police
- Ralf Zimmermann, Central Office for Information Technology in the Security Sector – Germany
- Tariq Elahi, University of Edinburgh
- Vasileios Rovilos, Future of Privacy Forum
- William Borg, Danish Online Police Patrol
- William Karlberg, Malta Police Force

Authors

- Sigita TRAINAUSKIENE (JRC)
- João FARINHA (JRC)
- Mark WITTFOTH (Europol)
- Diederik DON (Europol)
- Alexandra de MALEVILLE (JRC)

Contributors

- Gwendolyn BAILEY (JRC)
- Antonia MOCHAN (JRC)

Executive summary

Privacy Enhancing Technologies (PETs) are a group of technologies designed to process and share data safely. They are essential in ensuring that users trust digital systems and services that permeate our everyday lives. On the other hand, PETs can also be used to hide traces of criminal activity, thus hindering law enforcement's ability to investigate such crimes. As PETs and key enabling technologies like AI and quantum continue to evolve, Europe needs a timely and comprehensive approach to anticipate relevant developments and adapt policies and skills that can effectively meet emerging challenges.

This report highlights key privacy enhancing technologies (PETs) for law enforcement, following a horizon scanning exercise conducted by the Joint Research Centre (JRC) of the European Commission and EUROPOL. The exercise identified emerging PETs that could support or hinder law enforcement activities in the future. It provides insights for Europol and law enforcement agencies on the potential advantages of these technologies and on criminal activities that could be facilitated by them. The insights could also be useful for decision-makers dealing with internal security affairs, and for organisations financing and carrying out research in the area.

Policy context

Digital transformation has opened up new opportunities for connection, innovation and economic growth, but also brought new challenges in the fields of cybersecurity and privacy. Cyber-enabled crime is on the rise in the EU, with criminal networks operating across multiple EU countries, actively leveraging modern technologies to pose threats to individuals and organisations, while hiding traces of their activities. Though the precise scale and impact of criminal activities is difficult to measure, the 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) highlights their harmful consequences on the EU and its population. As most of these activities have a link to some digital component, lawful access to electronic evidence has become crucial for combating both cyber-dependent and cyber-enabled crimes.

In the context of Russian war of aggression against Ukraine', Europe has also experienced an increase in cyber-attacks, including distributed denial-of-service attacks, ransomware and other types of malware, with a particular focus on disrupting critical infrastructures. They form part of a broader spectrum of hybrid threats aimed at undermining the EU's stability and security, and highlighting the need for a comprehensive and coordinated approach to mitigate their impact and protect the integrity of EU systems and infrastructure. The European Commission has, therefore, identified a new era for European defence and security as one of its key priorities for 2024-2029 [1], stressing the need to invest in cyber defence. The Political Guidelines for the new Commission call for 'no hiding place for organised crime in Europe – either offline or online'. To address this challenge, a new European Internal Security Strategy was adopted on 1 April 2025, integrating security into EU legislation and policies. This includes equipping law enforcement with modern tools for lawful digital access to data while safeguarding fundamental rights.

This project is the result of collaboration between the EU Policy lab and Europol's Innovation Lab. The authors acknowledge the limitations of the study. It mainly reflects the results of a participatory workshop and a limited number of interviews, meaning that further research on the information provided is necessary to gain a more all-encompassing understanding of each technology mentioned in this report. The recommendations provided should therefore be considered with these limitations in mind.

Main findings

Out of nearly 200 signals[1] (covering both PETs and the relevant contextual factors that contribute to or hinder their development and uptake) collected for the participatory horizon scanning workshop, experts identified **10 emerging technologies and breakthrough innovations** as particularly important for law enforcement activities in the near future. Having analysed workshop's results, the project team identified five clusters (see below) highlighting the major domains where the key signals – and the underlying technologies – are situated, while also revealing synergies and interactions among them:

- **Artificial intelligence** – AI emerged as the dominant theme, integrating core principles like explainable AI (XAI), machine unlearning, and privacy-preserving machine learning. AI's foundational role extends to enabling other emerging technologies such as deepfake detection, predictive analytics and secure environments, reflecting its transformative potential and centrality in addressing modern technological and societal challenges. Finally, in addition to the smaller tasks it is already being used for, AI has great potential for more complex investigative tasks, for instance related to revealing hidden identities and secure environments.
- **Identity protection and biometric security** – Deepfake detection, the most important topicaccording to the participants, exemplifies the urgency of countering identity-related threats. Biometric security, incorporating different layers and methods like facial recognition and behavioural biometrics, offers enhanced security but raises concerns about criminal misuse, data breaches and ethical risks. Preventing exploitation by criminals leveraging deepfakes or compromised biometric systems demands robust safeguards.
- **Secure communications and computational environments** – Technologies such as trusted execution environments (TEEs) and disruption strategies like adversarial signal injection highlight the importance of securing sensitive data. TEEs safeguard computations with hardware-based encryption, while methods to counter adversarial attacks are critical for preserving data integrity, particularly as malicious actors exploit vulnerabilities in AI and sensors.
- **Robotics and drones** – Advances in robotics - including the development of humanoid robots and, for example, tiny solar-powered drones – are opening up new possibilities for surveillance, crisis response and operational efficiency. While boosting capabilities for law enforcement, these technologies pose challenges as they can also be abused by criminal actors. Risks in this field include hacking, illegal surveillance, and disruption of law enforcement operations. They require privacy-enhancing approaches, including robust cybersecurity frameworks and ethical deployment standards.
- **Systemic and behaviour approaches** – The internet of behaviour (IoB) integrates data analytics and behavioural psychology, enabling precise insights into human actions. By analysing patterns from the internet of things (IoT) and social media, IoB can enhance law

[1] A signal is the tangible manifestation of novelty (event, innovation or other development) that might not yet be at the radar of most people, but that has innovative, disruptive and/or strategically discontinuous potential to grow in scale and geographic distribution

enforcement strategies. However, it also raises ethical concerns around privacy, data security and potential misuse by criminals in order to carry out illicit activities.

These five clusters of technologies highlight innovations with impact over different time horizons ranging from shorter to longer term. As a substantial part of current PETs are built upon or substantiated by cryptography, the report delves deeper into new developments in this field. The exercise also looked at key enabling technologies such as AI and quantum technologies, which contribute to the development of PETs. Thus, following the horizon scanning and the workshop discussions, the authors selected additional five technologies relevant for the topic of this report. The following law enforcement-relevant insights were gained:

— **New encryption methods** – The development and adoption of advanced new encryption methods such as fully homomorphic encryption (FHE) and secure multi-party computation (SMPC) will provide better protection of data. These technologies enable the processing and analysis of data while it remains encrypted, enabling secure computation on sensitive information.
This will also mean that law enforcement may face challenges in accessing encrypted data for investigative purposes. Therefore, ensuring lawful access under judicial supervision will remain critical for law enforcement agencies. Additionally, investigative efforts could be supplemented by alternative investigative approaches, such as metadata analysis and targeted local data collection.

— **Quantum technologies** – Two emerging quantum technologies, quantum computing and quantum communications, pose both threats and opportunities. Quantum computing could enable 'harvest now, decrypt later' attacks, compromising in the future - when new technologies are available - currently secure data. This raises the need for organisations to prepare for cryptography in the post-quantum computing era, usually known as post-quantum cryptography (PQC).
However, this will also create challenges for law enforcement accessing encrypted data. Quantum communications such as quantum key distribution (QKD) offer ultra-secure communication. While QKD is unlikely to be a significant criminal threat due to its significant technical requirements, in the future it could provide secure transmission for criminals, making eavesdropping impossible.

— **Further developments in AI,** such as **neurosymbolic AI**, will enable law enforcement to perform complex ones, such as: analysing large datasets in new and more efficient ways, including detecting patterns, identifying connections in complex information structures, and revealing criminals' concealed identities.
These tools could enhance investigations and enable preparing more cases for trial, but challenges remain in verifying their accuracy and traceability. While criminals already exploit AI for malicious purposes, law enforcement could adopt these technologies more effectively. For example, federated learning (FL) could address data-sharing challenges by enabling collaborative AI model training while preserving privacy.

— However, the complex legal landscape—including the General Data Protection Regulation (GDPR), Directive 2016/680 (which sets out specific rules for the protection of personal data in the context of criminal investigations), and the AI Act—can create areas of legal interpretation that may affect the pace and manner of deploying new tools to counter evolving criminal tactics.

— **6G** presents both opportunities and challenges for law enforcement. On the one hand, 6G's integrated sensing capabilities, AI-driven network management, and satellite connectivity can provide richer data sources for investigations and security operations, enabling real-time tracking and analysis of complex information. This could improve law enforcement's ability to identify and disrupt criminal activity, manage crowds and ensure public safety.
However, 6G also introduces new challenges, such as increased complexity in tracing and accessing digital evidence, potential threats to privacy and personal data, and new attack vectors for cybercriminals. The uncertainties created by the current legal framework for the protection of personal data (as mentioned above) are also relevant in this context.

— **Blockchain and other distributed ledger technologies (DLT)** can facilitate various types of criminal activity, including illicit financing, money laundering, and collecting the proceeds of a crime. At the same time, DLTs can be a valuable tool for tracking and disrupting organised crime: by leveraging their transparent and immutable nature, law enforcement can follow the digital trail of transactions and identify patterns of suspicious activity, even if this is a challenging task. In the future, we may also see potential new threats to people's digital identities or digital currency resulting from new applications of these technologies, such as self-sovereign identities (SSI) or token thefts via identity compromise. Therefore, it is essential for policy-makers to ensure that the different possible applications of DLT do not put citizens' rights in danger.

Many of those technologies are neutral in terms of risks, and the degree of risk will depend on what the technologies are being used for. Although many of these technologies were designed with privacy in mind, it is important to highlight that 'perfect privacy' does not exist. Emerging PETs offer a much higher level of security for data, which is essential in light of increased cybersecurity risks, and it is expected that advanced PETs will be more broadly adopted. Thus, the challenge of balancing privacy and security will remain relevant in the future.

The full list of signals captured by this project is presented in the Annex. Some of these technologies are not strictly categorised as PETs in the existing literature. However, the authors' understanding is that they are relevant to this exercise, as they relate to the broader themes of identity, individuality, privacy, and personal cybersecurity addressed in the project The role of technology foresight is to operate at the fringes or intersections of existing taxonomies in order to draw out emerging topics and spillover effects from technology development and uptake. Therefore, this list can also be understood as a contribution to the discussion on the relationship between technology and privacy.

In summary, the emerging technological landscape will provide law enforcement with both opportunities and challenges. These changes will force them to adapt in order to detect and prevent crimes effectively. Major changes will come with encrypted computing, which enables computation on encrypted data.

Relevant contextual factors

This report also identifies relevant contextual factors enabling or hindering the development and uptake of PETs, such as geopolitical and economic dynamics, including the US-China technology race and its impact on digital markets. Against this backdrop, innovations in the digital sphere are crucial for enhancing European competitiveness, which will also drive the adoption of more advanced PETs amid growing concerns about cyber-attacks and mass-surveillance. Regulatory initiatives such as the GDPR, the Digital Markets Act (DMA), and the EU AI Act can act as drivers of innovation while also introducing additional implementation considerations.

The main barriers to PET adoption include a lack of resources, challenges in attracting talent to the field, despite the increasing awareness of (cyber-)security issues,the weaponisation of AI. Additionally, dark web poses persistent challenges. Initiatives like Digital Decade, as well as greater cross-border cooperation in law enforcement, regulations on e-evidence, and initiatives such as the UN Cyber-Crime Convention could further enable adoption of advanced PETs.

Finally, the changing attitudes of younger generations towards privacy may be a precursor to changes in public attitudes and behaviour: for instance, young people claim to be concerned about privacy yet provide a great deal of personal information through social media—a paradox which could be important in shaping future policies.

Points for reflection for law enforcement

Having analysed the results of the exercise, the team came up with the following points for reflection deemed of relevance for law enforcement agencies:

— It is necessary to **explore opportunities provided by advanced PETs,** like federated learning (FL), fully homomorphic encryption (FHME) and secure multi-party computation (SMPC), and to harness their potential in investigations, for example, in the analysis of encrypted data for fraud detection. While it is critical for law enforcement to access encrypted data lawfully, it could also develop **alternative investigative methods** such as using metadata, network analysis and human intelligence.

— It is necessary to **prepare for the advent of, and investment in, quantum-resistant technologies** such as post-quantum cryptography (PQC) and quantum key distribution (QKD), so that sensitive data remains secure with the advent of quantum computers; this will also require adaptation of current digital forensic techniques.

— The opportunities provided by AI and other key enabling technologies have be further explored and used for criminal investigations, such as in deepfake detection, uncovering hidden identities, predictive analytics, digital forensics, privacy-preserving investigations. While acknowledging the technologies' technical limitations, it is important to recognise that 'perfect privacy' does not exist and to weigh the alternative costs of not using them.

— There needs to be **investment in training and education** so that law enforcement agencies develop the skills and expertise needed to work with emerging PETs like encrypted computing, and with enabling technologies like AI, 6G, quantum, distribute ledger technologies (DLT) and others. Law enforcement agencies should **have access to technical solutions**, such as via the Europol Tool Repository, and should boost their capacities to understand and navigate PETs through further capability building.

Points for reflection for EU policy-makers

The following points for reflection are deemed of relevance for EU policy-makers:

— In view of rising cyber-crime and cyber threats against EU and Member States, **the securing of digital systems needs to be prioritised**, promoting the use of PETs and thus making our digital systems more resilient and sensitive data better protected against external and internal security threats.

— **Existing regulatory frameworks** might need to be reviewed to clarify and simplify compliance processes and reduce the current legal uncertainty related to data usage,

particularly in light of the challenges and opportunities that current and emerging PETs pose to law enforcement.

— **a proactive and informed approach to regulating advanced PETs and key enabling technologies** is needed to leverage the benefits of these technologies effectively and to prevent potential new risks stemming from them. This includes developing clear guidelines to include law enforcement access to data.

— **Collaboration and international partnerships are essential** to develop common standards for PETs and foster law enforcement cooperation in fighting cybercrime, including lawful access to data for law enforcement agencies; implementation of relevant international agreements should also be promoted

— **There needs to be investment in research and development,** especially in the most promising PETs such as FHM, FL, SMPC, TEEs and others, with the aim of improving privacy and security for the public.

In summary, collaboration among key stakeholders, including technology developers, service and infrastructure providers, policy-makers, law enforcement and privacy advocates, could be increased both at European and national level to ensure that emerging technologies are used in a way that balances privacy and security, helping law enforcement to keep the European population safe.

Related and future Joint Research Centre and Europol work

This work is part of the EU Policy Lab work stream on technology foresight. It continues the Joint Research Centre's broader efforts to provide policy-makers with actionable insights about the development of emerging technologies and breakthrough innovations, in order to harness their potential and address the challenges they bear.

This report is also part of Europol's technology monitoring and foresight capacity, led by the Europol Innovation Lab's Observatory. The purpose of this report is to inform law enforcement of relevant trends and to anticipate potential future opportunities and threats, with a specific focus on the impact on law enforcement operations.

1. Introduction

1.1. Background of the study

We are living in a more dangerous world. The EU security environment is rapidly undergoing a deep and long-term transformation, driven by global interconnected changes such as intensifying competition between global powers, sophisticated criminality and a growing number of actors competing for influence.

In this context, European Commission President Ursula von der Leyen has put forward *A New Era for European Defence and Security* as one of the key priorities in the Political Guidelines for new European Commission for 2024-2029 [1]. Russian war of aggression against Ukraine' has forced decision-makers to reassess the importance of both security and the protection of sensitive personal and operational data on a continent that for generations enjoyed peace, stability and security. Hence, it has been stated that in the coming Commission's term 'we will look at all of our policies through a security lens', which increasingly includes cybersecurity, data governance, and privacy-enhancing technologies as essential components of European resilience.

These growing geopolitical tensions are contemporary to other threats: organised crime is on the rise in Europe, and many criminal networks are actively leveraging modern technologies to hide their criminal activities [2]. Malicious actors are targeting European countries, their governments, financial services, transport systems, energy and healthcare sectors, as well as individual members of the public. The Political Guidelines therefore call for 'no hiding place for organised crime in Europe – either offline or online'. The new *European Internal Security Strategy* aims to ensure that security is integrated into EU legislation and policies by design. The strategy emphasises that 'we need to provide law enforcement with adequate and up-to-date tools for lawful access to digital information, while safeguarding fundamental rights' [1]. The development of the EU's cyber defence capabilities is identified as one of the key projects to be launched as part of the European Defence Union.

According to Europol's most recent Internet Organised Crime Threat Assessment (IOCTA) [3], data has become a key commodity, serving both as a target and a key enabler in the cybercrime threat landscape. Its value lies in enabling a wide range of criminal activities, including cyber-attacks, online fraud schemes, sexual exploitation of children online, and extortion. Consequently, demand for data is skyrocketing and its illicit trade is expected to become even more widespread in underground economies, contributing to the destabilisation of legitimate economies and the erosion of trust in governance structures. Data breaches and misuse – whether intentional or accidental – can have severe consequences, undermining the functioning of society and seriously impacting those affected. This reinforces the need to protect sensitive data through robust measures.

Privacy enhancing technologies (PETs) are a group of technologies designed to process and share data securely. They are essential in ensuring user trust in the digital systems and services that permeate our everyday lives, from doing business to accessing public services online. The use of PETs is increasing in light of the need to comply with the regulatory requirements, increased security concerns, and the reduced costs of the technology. New technologies such as AI and increasing computing capabilities are enabling innovative data-driven solutions and better services for consumers, opening up new opportunities as well as risks.

Encryption is one of the pillars of data security, alongside cybersecurity and other components such as access controls, network security, application security and data protection legislation. Encryption is currently used by about 50 billion devices, mostly for communicated and stored data. This field is

constantly evolving, with ongoing research and new applications being developed. However, PETs can also be misused to conceal traces of criminal activities, hindering law enforcement's ability to investigate and access electronic evidence. Notably, more than half of criminal investigations today involve cross-border requests for electronic evidence such as data from messaging services or social media [4]. This situation highlights the dual challenge of strengthening Europe's resilience to cyber-attacks and fighting crime while ensuring lawful access to electronic evidence. The European Commission reacted to this dilemma in June 2023, when it set up the High-Level Group on access to data for law enforcement. Its objectives were to establish a collaborative and inclusive platform for stakeholders, to formulate a strategic forward-looking vision and propose concrete recommendations for further development of EU policies to improve access to data for effective law enforcement operations. The work of the High-Level Group resulted in 42 recommendations and a concluding report that provides additional context [5]. Among these recommendations we find topics strongly connected with PETs such as the need to ensure that new obligations to not undermine or weaken end-to-end encryption or broader topics like the need to develop technology roadmaps by bringing together technology, cybersecurity, privacy, standardisation and security experts, in order to implement lawful access by design in all relevant technologies.

With technologies evolving, decision-makers face a continuing dilemma: how can they balance the essential task of ensuring public security with the equally important objective of preserving the fundamental right of privacy in the future?

1.2. Focus and objectives of the report

This report builds on existing knowledge in the field, seeking to uncover new technological developments and focusing on a specific perspective: to examine the opportunities and challenges that PETs present for law enforcement. It takes into account several other reports on privacy enhancing technologies recently been published, including but not limited to 'From Privacy to Partnership' [6], 'Privacy and intelligence' [7] and 'The PET Guide' [8]. To this end, a research methodology grounded on foresight was designed. This methodology aims to provide valuable forward-looking insights for decision-makers seeking to take advantage of the opportunities opened up by emerging technologies.

The main **objective of our research** is to explore emerging PETs from this dual perspective: to look for new technological innovations that could: (i) open up new opportunities for Europol and law enforcement agencies or; (ii) hinder their future operations.

We will answer the following **key research questions**:

- What are the most promising emerging privacy enhancing technologies when it comes to supporting future law enforcement investigations/operations (for example, lawful and privacy-compliant access to electronic evidence, privacy-compliant AI training, communication and collaboration between Europol and European law enforcement agencies, etc.)?
- What are the relevant key drivers, enablers and trends for the development and adoption of PETs by law enforcement and criminal actors?
- What are the emerging PETs and/or related technologies that could pose significant criminal threats or facilitate them in the future?
- What are the emerging PETs that could most hinder the work of law enforcement in the future?
- What priorities should the EU consider for funding, skills and innovation in this area?

1.3. Main collaborators

The European Union Agency for Law Enforcement Cooperation – **Europol,** has an important role to play in fighting organised crime and terrorism in Europe. The vision set out in the Political Guidelines is that this role will be further strengthened in future, so that its capacity to support national law enforcement agencies is bolstered [1]. Currently, Europol's mission is defined as 'to support its Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism' [9]. One of its operational priorities, as laid down by the European Multidisciplinary Platform Against Criminal Threats (EMPACT) 2026-2029 [10], relates to the fastest growing crimes in the online sphere: cyber-attacks, online child sexual exploitation and online fraud schemes.

The **Europol Innovation Lab** [11] was established in 2020. Its role is to help the European law enforcement community stay at the forefront of innovation and stay ahead of emerging threats. In this context, the Innovation Lab's Observatory monitors relevant technological developments and evaluates their implications for law enforcement with a forward-looking perspective.

The **Joint Research Centre** (JRC) [12] is the European Commission's in-house science service. Its mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. The JRC is spread across six different sites: Brussels and Geel (Belgium), Seville (Spain), Ispra (Italy), Petten (the Netherlands), and Karlsruhe (Germany).

The **EU Policy Lab** [13] is a space and mindset for cross-disciplinary exploration and innovation in policy-making. It applies collaborative, systemic and forward-looking approaches to support innovative policy making. Combining quantitative and qualitative research techniques, through behavioural insights and design practices the Policy Lab identifies innovative elements and key insights to increase policy effectiveness. Its Competence Centre on Foresight aims to contribute to strategic planning and to forward-looking EU policies and decision-making practices. One of its main work strands developed in the last few years is technology foresight [14]. This included several horizon scanning exercises, both in specific policy and technology domains and across multiple sectors. In this context, the authors highlight the recent Science for Policy brief on emerging technologies and breakthrough innovations in the broader field of digital and network security [15], which was developed in parallel with the current report and in collaboration with the European Innovation Council.

1.4. Overview of the content of the report

This report contains six sections:

- The first section provides an introduction, namely context, methodology and objectives of the study.
- The second section of the report presents privacy-enhancing technologies (PETs), their classification and main development trends.
- The third section summarises the results of a participatory workshop in which experts from various fields assessed signals on emerging PETs identified through horizon scanning. The ten PETs considered most relevant for monitoring in the coming years are described in terms of

their functions, opportunities, and the challenges they pose for Europol and law enforcement agencies.[2]

— The fourth section presents insights from expert interviews on the potential long-term evolution of encryption, AI and quantum technologies, complementing the workshop's near-term focus.

— The fifth section discusses key contextual factors influencing the development and uptake of PETs, combining findings from the workshop with additional desk research.

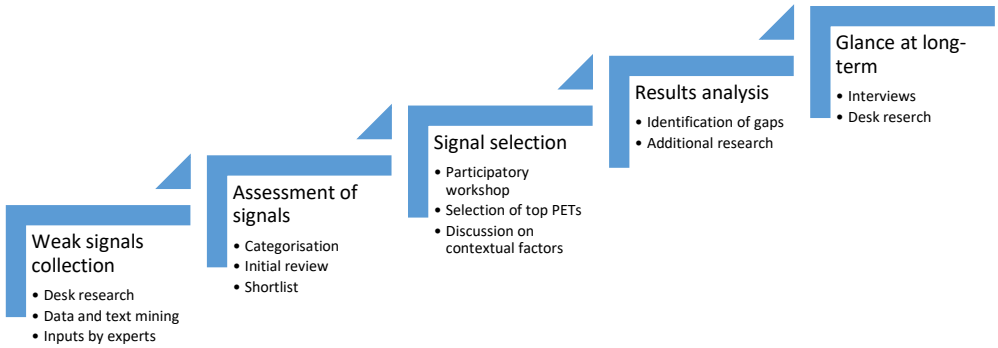
— The final section provides conclusions and points or reflexion for future actions.

An Annex compiles all weak signals collected during the horizon scanning exercise.

1.5. Methodology

The methodology used in this study is outlined in Figure 1. The joint working group of the JRC EU Policy Lab and the Europol Innovation Lab steered the 'horizon scanning' exercise on emerging privacy enhancing technologies that will impact the future work of Europol and law enforcement agencies, either supporting or hindering criminal investigation capabilities.

Figure 1. Methodology of the study



Source: authors

Horizon scanning is a foresight methodology aimed at detecting signals of change and trends [16]. It is usually run in phases, from signal scanning to validation and prioritisation of signals, to sensemaking and generation of insights for planning and programming. The understanding of what constitutes a signal, or a trend may vary [17, 18]. As it is not yet consensual, for the purposes of this project both are relevant and understood as tangible manifestations of novelty in science, technology, innovation, markets, media, and other fields. They can cover different maturity levels from basic research to commercial readiness. Although often used interchangeably, a signal is less consolidated than a trend. Horizon scanning aims to uncover future changes that remain on the

[2] Some of these topics are not strictly categorised as PETs in the existing literature. However, the authors' understanding is that they are relevant to this exercise, as they relate to the broader themes of identity, individuality, privacy, and personal cybersecurity covered by the research questions. The role of technology foresight is to operate at the fringes or intersections of existing taxonomies in order to draw out emerging topics and spillover effects from technology development and uptake. Therefore, this list should also be understood as a contribution to the discussion on the relationship between technology and privacy.

fringes of current thinking and planning. In this study, we aimed to focus on new ideas and possible new combinations and applications of emerging privacy enhancing? technologies for law enforcement.

The initial phase of the project – from July to November 2024 - was desk research and signals collection as preparation for the participatory workshop. During this phase, more than 200 initial signals were collected on PETs and relevant contextual factors, namely drivers, enablers and barriers for technological development and uptake, clustered through a PESTEL framework approach in political, environmental, social, technological, economic, legal domains.

A variety of sources were used for this process, including reports, scientific articles, news items, patents, EU-funded projects, and conference proceedings. Most sources covered the latest literature (2020-2024) in the field. Some weak signals were suggested by the experts invited to participate in the exercise, while most were obtained directly by the project team from the above-mentioned sources or through data and text mining methods.

The signals related with PETs were categorised according to their maturity level, enabling technologies and applications. As the participatory workshop focused on emerging PETs that could impact the future work of Europol and European law enforcement agencies, the project team reviewed and shortened the initial list of signals, considering the following research questions:

- What is the level of novelty of the technology?
- Which PETs are the most promising for law enforcement investigations in the future?
- Which technologies could pose or facilitate significant criminal threats / impede the work of law enforcement in the future?

From the initial list of signals, the project team selected a total of 178 signals, of which 116 were PETs and 71 were contextual factors (see Annex 1 for the full list). Out of this total, 9 signals were both PETs and contextual factors. These signals were clustered according to technological fields (PET) and PESTEL categories (contextual factors) and presented for discussion in the participatory workshop held online on 13 November 2024. The workshop was attended by about 20 technological experts (legal scholars, computer and data scientists, law enforcement professionals, policy-makers, and representatives of business and civil society).

The experts were divided into three groups, with at least two groups evaluating each cluster of signals. Through a structured process, they worked on making sense of the collected signals, selecting the top 10 signals on PETs first in the groups and then in the plenary, discussing wild cards[3], and then assessing contextual factors using the adapted future triangle methodology[4] (for

[3] In foresight a wild card is an event or development that bears a higher potentially disruptive impact than a normal signal.

[4] These factors were analysed using an adapted version of the "Triangle of the Future" framework [82], a foresight method that maps three competing forces: the pull of the future, the push of the present, and the weight of history. It can be used as a stand-alone method or in conjunction with others. For this project, the authors explored 3 types of contextual factors connected with those three temporal dimensions: drivers which are high-level factors that trigger or shape significant contextual changes and pull technological development and uptake into the future; enablers, or opportunities, that are pre-sent-day conditions that create a fertile ground for innovation to occur and therefore push technologies forward; and barriers, or challenges, that can be seen as past and present constraints ("weight") that hinder technological development and uptake.

the results see Section 5 of the report). The results of these discussions are presented in this report, along with additional desk research where appropriate (see Section 3).

With the workshop mainly focused on the near future (up to 5 years), seven additional semi-structured interviews were conducted in January-April 2025 to supplement the results of the discussions and to gain perspectives for the longer term. These aimed to capture knowledge on ongoing research and other new developments in related areas that could lead to major disruptions in the current environment. The interviews focused on several specific signals obtained during the horizon scanning process but not entirely covered by the top 10 topics that came out of the workshop. During this process we aimed to assess their possible developments and implications for law enforcement in the more distant future (see Section 4).

The authors acknowledge the limitations of the study. It mainly reflects the results of a participatory workshop and a limited number of interviews, meaning that further research on the information provided is necessary to gain a more all-encompassing understanding of each technology mentioned in this report. The reflection points provided should therefore be considered with these limitations in mind.

2. What are privacy enhancing technologies and why are they relevant for law enforcement?

In this section, we introduce the concepts of privacy enhancing technologies and data privacy, followed by a classification of PETs and what data privacy challenges they address. We also present trends for the proliferation of PETs and provide explanations of why they are relevant for law enforcement.

2.1. Privacy enhancing technologies: definition and purpose

The term 'privacy enhancing technologies' encompasses a broad set of technologies designed for **storing, processing and sharing data safely**. Although there is no single agreed-upon definition of PETs, data privacy and security are central to most definitions. The UN Guide on PETs emphasises that 'protecting data from unauthorised access, processing or distribution is the simple goal of privacy-enhancing technologies' [8]. The OECD views PETs as 'digital solutions that allow information to be collected, processed, analysed, and shared while protecting data confidentiality and privacy' [19]. ENISA, the European Union Agency for Cybersecurity, refers to PETs as 'software and hardware solutions, i.e. systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of natural persons' [20]. Although PETs involve many technologies and techniques, cryptography-based solutions constitute a substantial part of them.

Newer sources emphasise that PETs should be seen more as a **collaboration and data management tool** rather than just a privacy-preserving tool. According to the UK's Royal Society, PETs not only control potential breaches of data privacy but also reduce the threats typically associated with collaboration, motivating new partnerships even between otherwise competing organisations. It is argued that nowadays PETs serve several purposes: (i) reinforcing data governance choices; (ii) serving as tools for data collaboration; and (iii) enabling greater accountability through audits. For this reason, PETs are sometimes referred to as 'partnership enhancing technologies' or 'trust technologies' [6]. Sometimes the term 'privacy-preserving technologies' is used to describe those technologies that are aimed at building the 'privacy by design'[5] principle into the back end and front end of digital services from the start [21]. However, both this term and PETs are also used interchangeably [22].

Given the above, in this report we suggest viewing **PETs as a set of technologies aimed at protecting data privacy and security while enabling collaborations and data-driven innovations.** Although the term PETs is more commonly applied to specific technologies, in this study we analyse a broader set of technologies that can help preserve data privacy or, conversely, pose a threat to it. Enabling businesses and markets to collaborate and compute on shared data is said to be 'the next era on data economy' [23]. This also highlights PETs' potential to enable responsible collaboration that emerges from these opportunities, as PETs facilitate implementation of the principle of 'privacy by design' [24]. We will explore concepts of data privacy and data protection in the next sub-section.

[5] Data protection through technology design.

2.2. Data privacy explained

The growing volumes of data and its use have raised concerns over data privacy. Scholars note that 'privacy is more than protecting data', and there could be at least two approaches to this: in computer science, privacy can be viewed through the lens of system or information security, whereas from socio-ethical and legal perspectives, privacy is understood as an asset worth protecting [25]. In this section we will explain differences between privacy, data privacy and data protection.

Privacy, or the right to a private life, means a right to be autonomous, in control of information about yourself, to be let alone [26]. The right to privacy is considered one of the fundamental rights and is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (ECHR, Article 8) and the Charter of Fundamental Rights of the European Union (ECFR, Article 7). Article 8 ECHR grants a right to respect for private and family life and sets out the conditions of its limitations [27]:

— *Everyone has the right to respect for his private and family life, his home and his correspondence.*

— *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Similarly, Article 7 ECFR grants the right to respect one's private life and communications [28]:

— *Everyone has the right to respect for his or her private and family life, home and communications.*

Scholars identify four functions that privacy fulfils [25]:

1. the need not to be manipulated or dominated by others;
2. allowing individuals to relieve stress, be free from social pressures and expectations, and 'be oneself';
3. providing space and time to reflect on everyday life experiences, enabling an authentic, self-determined life;
4. defining the boundaries of interpersonal mental closeness or distance from others, thus allowing individuals to differentiate between the addressees of personal information.

Here information privacy comes to the fore, as privacy concerns both one's physical life (i.e. its material aspects) and immaterial life (i.e. protection of the ideas and information that are related to the individual person). A person's integrity may be considered to have been violated when others use information about him or her [29].

Data privacy is thus understood as one form of privacy derived from general privacy and is described as 'the authorised, fair, and legitimate processing of personal information' [30]. In the EU, privacy with respect to information has been covered by the special legal regulation known as data protection [29].

Data protection refers to the legal and regulatory measures that aim to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors. This concerns protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end users of communications services - are also considered personal data. In addition, some parts of personal information are considered 'sensitive' and are subject to specific processing conditions [31]. Examples of sensitive data include:

— personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;

— trade union membership;

— genetic data and biometric data processed solely to identify a human being;

— health-related data;

— data concerning a person's sex life or sexual orientation.

The reform of the EU's data protection rules, which began in January 2012, has resulted in three key pieces of legislation [32]:

— a general Regulation on data protection (Regulation 679/2016 – the GDPR), adopted on 24 May 2016 and applicable as of 25 May 2018;

— a specific Directive (680/2016) on data protection in the area of police and justice, adopted on 5 May 2016 and applicable as of 6 May 2018;

— Regulation (EU) 2018/1725 with regard to the processing of personal data by the Union institutions, bodies, offices and agencies.

One of the newest documents in the area - the *European Strategy for Data* emphasises that in a society where individuals will generate ever-increasing amounts of data, data collection and usage must prioritise the interests of the individual, in line with European values, fundamental rights, and the relevant rules in the field. The strategy also aims to empower individuals with respect to their data. This means, for instance, that individuals are in control of their data through tools and methods that enable them to decide in detail what is done with it ('personal data spaces') [25].

Scholars note that even though data protection rules aim to protect private information, they also serve other aims: data protection rules should make it possible to use personal data in a manner acceptable to society and in this way ensure that the use of modern information technology continues to flourish [29].

However, preserving privacy in the digital world has become an issue. Solove's approach considers privacy violations as resulting from problematic data actions, including [6]:

— **aggregation:** the gathering of information about an individual, which could be used to generate insights for re-identification or profiling;

— **identification:** the linking of data, which may otherwise be anonymised, to a specific individual;

— **insecurity:** the potential for data to be accessed by an intruder due to glitches, cybersecurity breaches or the intentional misuse of information;

— **exclusion:** the use of personal data without notice to individuals;

— **disclosure:** the revelation of personal data to others;

— **exposure:** the revelation of an individual's physical or emotional attributes to others;

— **intrusion:** invasive acts that interfere with an individual's physical or virtual life (such as junk mail).

PETs help to address these issues. However, they should not be regarded as a 'silver bullet' solution for protecting data privacy. As the OECD notes, PETs cannot substitute legal frameworks but must operate within them, so their applications need to be combined with legally binding and enforceable obligations to protect privacy and data protection rights [19]. One of the key challenges related to PETs is that they are constantly evolving. Given their highly innovative nature, they often fall outside the awareness of policy-makers and regulators. Yet as global data volumes continue to rise, the need for PETs is expected to increase, obliging policy-makers and law enforcement agencies to monitor the latest developments in this area. For a better understanding of various PETs, we will present different ways to classify them.

2.3. Classification of privacy enhancing technologies

There are several ways to classify PETs. Although this horizon scanning process does not use completely any of the following taxonomies to classify the signals, as part of the desk research, the authors took stock of the diversity of fields within those classification schemes, in order to ensure that the signal collection process was covering all relevant technology domains.

Within the existing frameworks, ENISA suggests the following classification for mobile and internet use: (i) secure messaging tools; (ii) virtual private networks (VPNs); (iii) anonymising networks; and (iv) anti-tracking tools [33].

The OECD divides PETs into four broad categories: (i) data obfuscation; (ii) encrypted data processing; (iii) federated and distributed analytics; and (iv) data accountability tools (see Table 1). The main opportunities and challenges related to the different types of PETs are also identified [19].

The UN distinguishes between two broad categories of PETs: (i) PETs for input privacy and for (ii) output privacy [8]. Input privacy focuses on how one or multiple parties can process data in a manner that ensures the data is not used outside of that strict context. Output privacy focuses on modifying computation results such that the output data cannot be used to reverse engineer the original inputs.

The UK Information Commissioner's Office PET guidance [34] similarly classifies PETs according to: (i) input privacy (e.g. secure multi-party computation - SMPC) and (ii) output privacy (e.g. differential privacy). In addition, it identifies: (iii) PETs that derive or generate data that reduces or removes people's identifiability (e.g. synthetic data); (iv) PETs that focus on hiding and shielding data (e.g. homomorphic encryption (HE) and zero-knowledge proofs (ZKPs)); and (v) PETs that split databases (e.g. SMPC, federated learning (FL)).

The Centre for Data Ethics and Innovation's 'PETs Adoption Guide' categorises PETs based on use cases. The two broad categories are: (i) traditional PETs, which cover encryption in transit, encryption at rest, and de-identification techniques; and (ii) emerging PETs, a group of technologies providing novel solutions to privacy challenges in modern data-driven systems, for instance, Homomorphic Encryption (HE) trusted execution environments (TEEs), SMPC, differential privacy, and systems for

federated data processing [35]. In the next section we will provide an overview of the main problems different PETs help to address.

2.4. Main problems that privacy enhancing technologies address

PETs can be useful for processing data that involves large-scale collection and analysis of personal information. The main problems that PETs currently address are [23]:

— data liability

— outsourcing risk

— processing of personally identifiable information

— collective processing

— data acquisition.

The first three are considered essential for helping a company implement responsible data practices and comply with legal requirements, while the last two are seen as potential game changers for the future, as they open new possibilities for training deep learning models and accelerating AI deployment [27]. However, those tools are not without limitations and involve certain challenges.

Table 1. Overview of major types of PETs, their opportunities and challenges

Types of PETs	**Key technologies**	**Current and potential applications***	**Challenges and limitations**
Data obfuscation tools	Anonymisation/ Pseudonymisation	Secure storage	-Ensuring that information does not leak (risk of de-identification) -Amplified bias in particular for synthetic data -Insufficient skills and competencies
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs (ZKPs)	Verifying information without requiring disclosure (e.g. age)	-Applications are still in their early stages
Encrypted data processing tools	Homomorphic Encryption ((HE)	-Computing on encrypted data - Computing on private data that is too sensitive to disclose - Contact tracing/discovery	-Data cleaning challenges - Ensuring that information does not leak -Higher computation costs
	Multi-party computation (MPC)		
	TEEs	Computing using models that need to remain private	-Higher computation costs -Digital security challenges
Federated and distributed analytics	Federated learning	Privacy-preserving machine learning	-Reliable connectivity needed -Information on data models need to be made available to data processors
	Distributed analytics		
Data accountability tools	Accountable systems	-Setting and enforcing rules regarding when data can be accessed -Immutable tracking of data access by data controllers	-Narrow use cases and stand-alone applications -Configuration complexity -Privacy and data protection compliance risks where distributed ledger technologies are used

Types of PETs	Key technologies	Current and potential applications*	Challenges and limitations
	Threshold secret sharing		-Digital security challenges -Not considered as PETs in the strict sense
	Personal data stores / Personal information management systems	Providing data subjects control over their own data	

Note: (*) Only one application has been included for the sake of readability
Source: OECD, Emerging Privacy Enhancing Technologies, 2023

So far, we have mainly discussed risks to personal privacy that PETs help to address. But as noted by the Royal Society, because of security violation or insider threats (data disclosed or reused for intended or unintended purposes), damage to privacy (privacy harms) can have a downstream effect at much broader levels. The developed taxonomy indicates the main harms that may result from problematic data actions. These can lead to the release of sensitive information of individuals, personal information being revealed or used for profiling and predictive purposes, etc. The emerging harms are classified into domains (individual, organisational, societal, national) and types (physical/psychological, relational, reputational, personal, economic, security) (see Figure 2) [6].

Figure 2. Domains of privacy harm

Source: The Royal Society (UK) [6]

2.5. Proliferation of privacy enhancing technologies: trends

Proliferation of PETs

As data production worldwide has been growing exponentially during the last decade, so too has the relevance of PETs in today's digitalised society. If in 2016 the average company managed 162.9 terabytes of data, in 2024 roughly 2.5 quintillion bytes of data were generated each day, with over 44 zettabytes of data in the entire digital universe. This growth is expected to continue with the mainstream adoption of generative AI (GenAI) [36].

The growing amount of data is just one of the several factors contributing to the proliferation of PETs, others being regulatory requirements (e.g. GDPR in the EU and the California Consumer Privacy Act) , concerns over data privacy, data migration to clouds and others. PETs are also evolving due to rapid technological advancements, such as those in AI and other domains. Countries around the world are promoting innovation in and with PETs. This involves investing in research and technology development, adopting secure data processing platforms, certifying trusted PETs, establishing regulatory sandboxes, and deploying digital identity solutions, among other measures. PETs are also being developed 'as a form of civic engagement rather than primarily for money' [23]. Additionally, PETs are becoming cheaper and more affordable, thus facilitating broader adoption.

The size of the global PETs market was valued at USD 2.60 billion in 2023. At that time, the market was anticipated to grow at a compound annual growth rate of 25.3% from 2024 to 2030. The rise of digital transformation, along with growing concerns over cybersecurity threats and data breaches, has heightened the need for advanced privacy-preserving techniques such as homomorphic encryption and differential privacy to protect sensitive information without compromising functionality [37].

Barriers to the adoption of PETs.

Some PETs are already widely used, while some more advanced techniques face barriers to adoption. For example, today there are about 50 billion devices (such as smartphones) using encryption. But adoption of more advanced PETs is not yet that widespread. Organisations are prevented from using them more widely for various reasons:

- a lack of understanding within organisations, which hampers internal buy-in;
- technology providers' insufficient understanding of the deployment environments for their products;
- uncertainty on how to assess the cost-benefit trade-off of using PETs;
- lack of resources, including expertise, which are root causes of failures to secure buy-in;
- concerns regarding the maturity of the PETs market;
- a lack of regulatory clarity, particularly on assessing the status of data when using PETs [38].

In addition, other sources indicate that there are certain risks with using PETs. These include lack of maturity, mistakes in implementation, and lack of appropriate organisational measures [34] some of which are discussed in more detail in this report. .

2.6. Relevance of privacy enhancing technologies in law enforcement

For individuals and society in general, PETs ensure trust for users of digital communication, trade, and service systems. This is particularly relevant in preventing unauthorised access to sensitive information such as credit card and banking information, health records, and social security numbers during digital transactions. In law enforcement, PETs play a critical role in:

- protecting sensitive information (ranging from personnel files to criminal intelligence);
- facilitating operational security;
- enabling the secure exchange of information between law enforcement agencies in the context of criminal investigations;
- overall increasing public trust in law enforcement's use of sensitive information.

However, PETs can also be used to conceal traces of criminal and terrorist activities, as well as to delete important pieces of information without the possibility of recovery. The type of PET used depends on the technical sophistication of the perpetrator or network, as well as the type of crime. Most commonly, PETs are used to conceal criminal communications [39].

PETs are used by criminal actors for secure communication, anonymisation, and protection of data. Criminal networks utilise various PETs, including end-to-end encrypted messaging apps, encrypted phones, and virtual private networks (VPNs), to communicate securely and anonymously. For example, Pavel Durov, founder and CEO of the popular messaging app Telegram was put in 2024 under formal investigation in France as part of a probe into organised crime. Simple PETs, such as encrypted messaging apps such as WhatsApp and Telegram, are widely used by lower-level organised crime groups and individual criminals due to their ease of access and affordability. These apps provide features like dedicated business accounts, open and closed groups, and broadcast features, making them suitable for interacting with customers of illicit goods and services.

More advanced PETs, such as encrypted phones such as SkyECC and Encrochat phones, are typically used by high-level organised crime groups and those involved in serious and organised crime such as cybercrime, drug trafficking and human trafficking. These groups often have more resources and knowledge and use encrypted phones to maintain secure communication.

Additionally, criminals with higher levels of technical expertise, such as cybercriminals, use more advanced encrypted infrastructure. These include several layers of obscurity, air-gapped communications networks, and new and complex encryption methods. The use of PETs is not limited to specific types of crime and many criminal networks use a combination of simple and advanced PETs to achieve their goals.

As technology advances, the trend towards privacy and the use of encryption to obscure and protect criminal communications is expected to increase further, driven by technological advancements and the emergence of new encrypted communications platforms. In this context, ensuring societal security solely through traditional investigative methods is no longer sufficient. Lawful access to digital evidence – such as documents, photos, conversations – has become of critical importance for law enforcement. Currently, digital data is already used in 85% of all criminal investigations [40]. In the case of encryption technologies, this could be achieved by either (i) requiring service providers to grant police exceptional access to encrypted data or (ii) compelling suspects to decrypt their own information in response to a lawful request, with criminal penalties for non-compliance [41]. In addition, data could be accessed with the help of technical solutions such as specific forensic tools and techniques.

Given that such conditions are generating public debate about the tensions between privacy rights and the technical feasibility of these solutions, it is crucial to balance security needs with individual privacy and civil liberties. This topic will be explored in more detail in this report, in light of the emerging PETs and the challenges and opportunities they pose, and the ways in which law enforcement can operate effectively.

3. Key privacy enhancing technologies for law enforcement – results of the workshop

Introduction

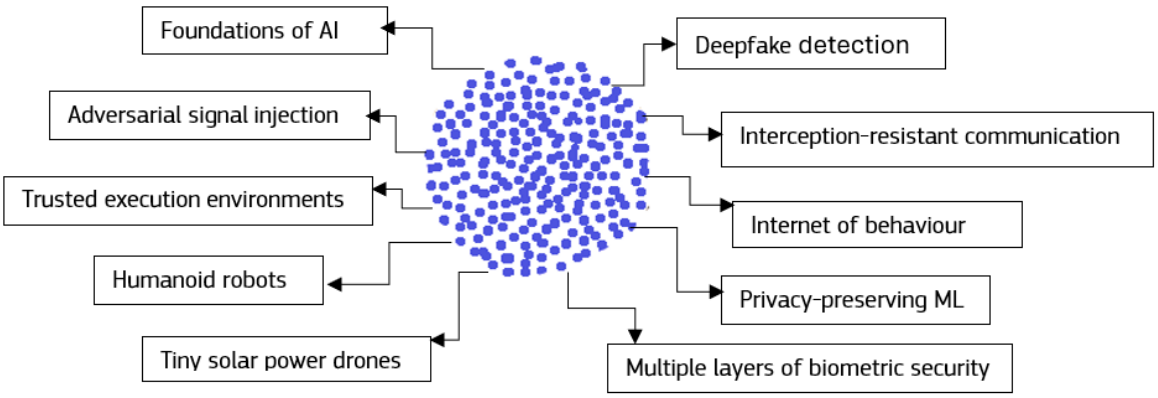
To explore emerging technologies, breakthrough innovations and future developments in the sphere of PETs (and related technologies), the project team developed a horizon scanning exercise. Signals were initially captured as deemed relevant for supporting or hindering law enforcement activities, as were new types of threats that could arise because of use of these technologies.

All collected signals were reviewed and condensed on the basis of the research questions. The longlist of signals was categorised around these six clusters:

- A1: distributed ledger technologies
- A2: quantum and post-quantum
- A3: internet of things and edge computing
- A4: identity and deepfakes
- A5: internet, browsing and VPNs
- A6: encryption.

This longlist was distributed to participants ahead of the workshop (see Annex 1). During the participatory workshop (held online on the last quarter of 2024) participants discussed the signals (at least two groups per each sub-cluster) and added additional topics they felt were relevant. Following a series of predefined steps, participants then identified what they considered collectively as the most important PETs and related technologies. In this section, we present the final selected list of key PETs and related technologies (see Figure 3).

Figure 3. Key PETs for law enforcement according to the experts



Source: authors

Some of these topics are not strictly categorised as PETs in the existing literature. However, the authors' understanding is that they are relevant to this exercise, as they relate to the broader themes of identity, individuality, privacy, and personal cybersecurity covered by the research questions. The role of technology foresight is to operate at the fringes or intersections of existing

taxonomies in order to draw out emerging topics and spillover effects from technology development and uptake. Therefore, this list should also be understood as a contribution to the discussion on the relationship between technology and privacy.

3.1. Deepfake detection

Summary description

Deepfake detection technology is advancing rapidly to counter increasingly sophisticated and accessible falsified images and videos. Deepfakes are used to adopt the likeness of another person to avoid identification or abuse someone's identity, usually to impersonate them or depict them as doing something they did not do. This is closely related to privacy, as controlling your identity or likeness is just as fundamental as your personal data.

Participants highlighted the high impact and urgency of this topic, stressing the need for short-term, actionable solutions. They also discussed the evolving sophistication of deepfakes, noting their growing societal impact and the necessity for future-proof technologies. As it becomes harder for the human eye to spot deepfakes, detecting them needs to be prioritised.

Current detection methods rely on machine learning. One method in use is 'convolutional neural networks' (CNNs) a type of deep learning model designed to process image data, identifying patterns like edges, textures and anomalies, which makes them effective for spotting inconsistencies in deepfake content. Another method already in use is to combine advanced machine learning architectures to ensure greater accuracy. One such example is the combined use of Vision Transformers and EfficientNet B0. Vision Transformers excel at capturing global image features, while EfficientNet B0 is a highly efficient neural network. Together the two technologies improve the accuracy of deepfake detection.

Novel techniques include rational augmented CNNs for real-time detection. These enhanced CNN models designed for real-time facial reconstruction help detect manipulated or synthetic faces more quickly and accurately. Forensic noise trace analysis is another novel technique. It examines subtle noise patterns left behind in videos or images by the deepfake generation process, which are often invisible to the human eye. Finally, watermarking facial identity features promise to combat tampering: embedding digital watermarks in facial features could create a unique identity label that can signal if tampering has occurred.

Analysis

This technology has a major impact on the future of law enforcement agencies, as deepfakes could be used to spread disinformation, manipulate public opinion, or impersonate individuals in legal and financial transactions. Detecting and preventing such abuses will be essential for maintaining public trust and ensuring security and justice. However, deepfake technology could also facilitate major criminal threats such as creating realistic forgeries of evidence, blackmail, and identity theft. Such threats could undermine legal processes, exacerbate cybercrime (and many other types of crime) and fuel mistrust in general.

To address these challenges, law enforcement agencies must develop advanced technical capacities such as integrating AI-driven detection tools and building forensic expertise. Training personnel to recognise and counter deepfake-related threats will be vital. By collaborating with technology

companies and researchers, law enforcement will be better placed to stay ahead of evolving threats. Meanwhile, clear legal frameworks will make their task easier and mitigate the risks.

Sources: [42] [43] [44] [45]

3.2. Interception-resistant communication

Summary description

Advances in privacy enhancing technologies are making it easier to counter interception in digital communication. Some solutions include decentralised virtual private networks (VPNs), anonymous networks such as 'The Onion Router' (Tor), messenger apps such as Session and mix networks.

Decentralised VPNs replace centralised servers with distributed nodes, leveraging blockchain, smart contracts and encryption. These networks enhance security, minimise single points of failure, and enable users to share idle bandwidth anonymously.

The Onion Router uses layered encryption to anonymise internet access by routing data through multiple nodes. It protects user identities by removing encryption layers at each step, ensuring data's origin and destination remain hidden. However, unless additional encryption like HTTPS is used, data exiting the network may travel in plaintext, posing potential security risks.

Session is an encrypted messenger that eliminates metadata collection. It uses onion routing to ensure total anonymity, requiring no phone numbers or user accounts and leaving no digital footprint.

Mix networks such as the Invisible Internet Project further enhance anonymity by obscuring metadata, including origin and destination. Messages are encrypted in layers, routed through multiple nodes, and mixed with others to prevent tracking. These networks are decentralised, resistant to surveillance, and secure against timing attacks.

Analysis

These technologies collectively strengthen interception-resistant communication by prioritising user privacy, anonymity, and resilience against surveillance and unauthorised access. But they also challenge law enforcement agencies by limiting their ability to monitor the communication of criminals' activity and limiting their capacity to gather evidence of a crime and attribute it to a particular suspect.

In short, while such technologies enhance privacy, the fact they enable secure, untraceable communications also facilitates major criminal threats such as illicit trade, cybercrime and terrorism.

To address these challenges, law enforcement must invest in advanced analytical tools, multidisciplinary teams and international cooperation. To harness these technologies responsibly, it will also be crucial to build trust with technology providers and promote ethical cybersecurity research, including ethical and lawful hacking.

Sources: [46] [47] [48]

3.3. Internet of behaviour

Summary description

The internet of behaviour (IoB) is a concept that integrates technology, data analytics and behavioural psychology to interpret and influence human actions. It builds on the wider internet of things (IoT) by including not just the collection of data but also its analysis to understand people's behaviour. This understanding can then further guide decisions in areas such as commerce, public policy and law enforcement.

IoB envisions the collection of data from various sources such as IoT devices, social media, and websites. While its potential to shape behaviour is vast, it raises ethical and privacy concerns. Addressing these issues is critical to ensure responsible implementation of IoB technologies.

Analysis

IoB holds significant implications for law enforcement. By analysing behavioural patterns from diverse data sources, it can improve investigative processes, enabling more precise identification of suspects and prevention of criminal activities and dangerous situations. This technology may also improve resource allocation and decision-making, crucial for addressing evolving threats.

However, IoB presents considerable risks. Criminals could exploit its capabilities to: (i) target vulnerable individuals; (ii) identify opportunities to refine illicit activities like identity theft, phishing and money laundering; and (iii) identify and threaten law enforcement personnel. The collection and storage of sensitive behavioural data also creates opportunities for cyber-attacks, especially phishing and ransomware incidents.

To address these opportunities and challenges, law enforcement agencies must develop advanced analytical capabilities to leverage IoB data responsibly. This includes building expertise in behavioural analytics, improving cybersecurity measures to protect sensitive data, and adopting ethical guidelines to ensure privacy and trust. Collaboration with technology experts and regular training on IoB-related developments will be critical for adapting to this emerging technology.

Source: [49]

3.4. Multiple layers of biometric security

Summary description

Biometric security is advancing identity authentication by leveraging unique physiological and behavioural traits such as fingerprints, facial recognition, iris scans and voice recognition. Unlike traditional passwords, biometrics offer enhanced security and convenience due to their uniqueness and resistance to replication. Behavioural biometrics, analysing patterns like typing rhythms and gait, add a dynamic layer of security.

The advantages include heightened security, speed, convenience and irrefutable proof of identity that prevents fraud. However, challenges like privacy concerns, potential data breaches, and ethical issues around surveillance need to be addressed. A major drawback is the irreversibility of biometric data: once compromised, it cannot be reset like a password. While it can offer strong protection, it is not perfect as it can also be vulnerable to attacks.

Emerging trends include multi-modal systems combining different biometric methods for greater accuracy, integration with IoT devices, and contactless solutions (propelled by the pandemic). Blockchain is being explored to securely store biometric data, while AI-driven advancements like deep learning and fraud detection are refining biometric systems' reliability.

Industries such as finance, healthcare and government are adopting biometric security to safeguard sensitive data and streamline processes. However, addressing privacy and ethical considerations will be crucial, alongside global standardisation, for sustainable and equitable biometric adoption. Finally, secure implementation of all components of the biometric system is essential. This applies to the robustness of the system itself, but also to the protection of other biometric systems, by preventing the extraction of biometric data from one system to be used to attack another. The future holds the promise of more accurate and personalised biometric technologies integrated with emerging platforms like augmented and virtual reality (AR / VR) and smart cities.

Analysis

Workshop participants highlighted the dual nature of these technologies. On one hand, they provide enhanced security for personal data and identity protection. On the other, they raise concerns about misuse, data breaches and surveillance risks.

Biometric identification is a growing area of importance for law enforcement agencies. Its ability to identify individuals using unique physical or behavioural traits offers better tools for identity verification and secure access. As this technology evolves, it has the potential to revolutionise investigations, enabling faster suspect identification and improving public safety.

However, the misuse of biometric security poses significant criminal threats. Criminals could exploit vulnerabilities in biometric devices, steal sensitive data, or use deepfake technology to impersonate individuals and bypass security systems. Reports of unethical practices such as paying vulnerable individuals for their biometric data or illicitly harvesting information highlight the need for stricter safeguards.

To address these challenges, law enforcement agencies must develop advanced capabilities. This includes deploying secure biometric systems resistant to tampering, training officers to handle biometric data responsibly, and investing in technologies to detect and prevent manipulation. Collaboration with technology providers, ethical oversight and clear legal frameworks are critical to ensure that biometric security is used effectively and ethically, balancing innovation with privacy and trust. Finally, public awareness regarding the need to safeguard personal biometric information is key to limiting its misuse by third parties.

Sources: [50] [51]

3.5. Privacy-preserving machine learning

Summary description

Privacy-preserving machine learning is a technology that enables the training of predictive models on large amounts of data while maintaining the data contributors' privacy. It employs techniques such as federated learning (FL), two-party computation (2PC) and differential privacy to ensure that local training data is kept confidential even when used to build shared models. The technology is particularly relevant in fields where privacy is paramount, such as healthcare, education, finance and law enforcement.

The novelty of privacy-preserving machine learning lies in its ability to maintain data privacy while allowing for collaborative model training. Unlike traditional machine learning approaches that require data to be centralised, this technology enables decentralised learning, reducing the risk of privacy breaches. It also incorporates mechanisms to protect against targeted attacks, a challenge that most existing technologies have not adequately addressed.

Furthermore, privacy-preserving machine learning introduces innovative frameworks, such as the multi-task discriminator in generative adversarial networks (GANs), to enhance privacy. It also offers solutions for privacy-preserving linear and logistic regressions that are significantly faster than existing techniques. By integrating the hardware latency of the cryptographic building block into the neural architecture search loss function, privacy-preserving machine learning also boosts energy efficiency and reduces latency in deep learning. The technology can also enable the training of neural networks in a privacy-preserving manner, a feature that has not been implemented before.

Analysis

Privacy-preserving machine learning could help law enforcement become more efficient by enabling cross-border collaboration on AI training without breaching data privacy laws. This is especially important in areas where relevant training data are scarce. By integrating datasets securely, the technology can improve predictive capabilities in areas like crime detection and public safety. However, it could also facilitate criminal threats, such as enabling adversarial attacks or protecting malicious actors' data during collaborative efforts. To leverage these opportunities while mitigating risks, law enforcement agencies must develop capacities in cryptographic techniques, inter-agency cooperation protocols, and synthetic data usage. They also need to navigate legal and ethical challenges arising from varying data governance standards across jurisdictions.

Sources: [52] [53] [54] [55]

3.6. Tiny solar-powered drones

Summary description

The rapid advancement of unmanned aerial vehicles (UAVs) and robotics is reshaping the landscape of surveillance and operational technologies. From security and law enforcement to environmental monitoring and disaster response, the integration of UAVs into these domains is increasingly driven by innovations that prioritise efficiency and autonomy.

Among these trends, the development of solar-powered drones represents a significant leap forward, offering unprecedented opportunities for continuous, lightweight and versatile aerial solutions. A recently developed drone weighing just 4 grams is the smallest solar-powered aerial vehicle to fly yet, thanks to its unusual electrostatic motor and tiny solar panels that produce extremely high voltages. Although the hummingbird-sized prototype only operated for an hour, its makers say their approach could result in insect-sized drones that can stay in the air indefinitely.

Tiny drones are an attractive solution to a range of problems in fields like communications, espionage and search and rescue. However, they are hampered by poor battery life, while solar-powered versions struggle to generate enough power to sustain themselves.

Researchers from China developed a simple circuit that scales up the voltage produced by solar panels to between 6 000 and 9 000 volts. Rather than using an electromagnetic motor like those in

electric cars, quadcopters and various robots, they used an electrostatic propulsion system to power a 10-centimetre rotor.

Analysis

This breakthrough could have profound implications across various fields, particularly for law enforcement and security operations. The potential for these drones to operate indefinitely, potentially in fleets or swarms, opens new possibilities for almost continuous surveillance of criminal activities, securing events and sites, reconnaissance and search-and-rescue missions in hard-to-reach areas. Their lightweight and inconspicuous design make them ideal for discrete monitoring, significantly improving operational capabilities.

Despite their solar-powered design, the mass deployment of tiny drones could contribute to environmental pollution, particularly through the accumulation of electronic waste and potential risks to wildlife if not managed responsibly. Although these factors are not the focus of this report, law enforcement agencies should be aware of them if they consider adopting this and other similar technologies.

This same technology could be exploited for illegal activities such as unauthorised surveillance, smuggling or coordinated criminal actions, posing serious security risks. If law enforcement is to address these challenges it will need to develop advanced anti-drone detection systems, tools for electromagnetic interference, and AI-driven technologies to monitor and counteract misuse.

Additionally, regulatory frameworks will need to evolve to manage the ethical and legal deployment of such systems while mitigating risks effectively. The technology's dual-edged nature highlights both its transformative potential and the necessity for proactive measures to harness its benefits responsibly.

Sources: [56] [57] [58]

3.7. Foundations of AI

Summary description

As already outlined in the section above on 'privacy-preserving machine learning', the foundations of AI[6], i.e. its core technologies and the infrastructure needed for its development and use, is a key topic in the advancement of privacy and the use and take-up of numerous technologies by law enforcement agencies.

In this domain, participants discussed the importance of several dimensions such as explainable AI (XAI), machine unlearning, the EU regulatory context (the AI Act and the General Data Protection Regulation), and the admissibility in court of evidence. They also considered the infrastructural dimension of AI development and use, namely AI factories and high-performance computing infrastructure.

[6] This topic was proposed by participants as 'AI core technologies / computational infrastructure'. The title was changed for editorial purposes.

Explainable AI is an emerging area of research within the field of artificial intelligence. XAI aims to clarify how an AI system arrives at a particular solution, such as classification or object detection. It can also address other 'why,' 'how,' and 'what' questions. This level of explainability is often lacking in traditional AI systems. Explainability is essential for critical applications such as defence, healthcare, law enforcement and autonomous vehicles. In these areas, understanding the decision-making process is crucial for building trust and ensuring transparency, as well as for ensuring that criminal evidence is considered admissible in court.

Machine unlearning removes specific data from models to improve privacy and security. It helps erase sensitive data, fix errors and defend against cyber-attacks without retraining the entire model. The process uses noise (small random changes) to adjust model weights. While mostly effective, some personal data traces may currently remain. Models that have undergone unlearning may remain vulnerable to certain attacks – such as membership inference or private information reconstruction – that seek to identify the specific personal data removed. Changes in the model's outputs before and after the unlearning process can unintentionally expose information about the deleted data, thereby posing a risk to privacy. This highlights the need for further research to fully protect privacy.

Analysis

Privacy-focused machine learning tools such as differential privacy or federated learning, incentivised by current EU regulations, enable law enforcement agencies to leverage sensitive data responsibly. AI technologies hold transformative potential for law enforcement by enabling faster, more accurate data analysis and enhanced predictive policing. AI's ability to provide evidence through pattern recognition or anomaly detection can streamline investigations, improve the efficiency of operations, and support evidence admissibility standards, as long as transparency and explainability are ensured.

Regulation can affect innovation where compliance costs or uncertainty in the interpretation of legal provisions influence experimentation, development, and the uptake of new tools. The restrictions on data use and sharing under the GDPR, such as requirements related to cross-border data transfers, can introduce practical considerations for the training of AI models that rely on diverse datasets. Similarly, the AI Act's focus on explainability may influence the use of complex models such as deep learning, which are often important for developing advanced PETs. Striking a balance between fostering innovation and ensuring ethical AI deployment remains important to ensure these regulations effectively support the development of privacy-focused AI solutions.

Another key topic raised by the participants was the use of AI in court evidence. This raises significant ethical and legal challenges, with one major concern relating to the previously discussed explainability and transparency of AI models used in forensic analysis. If AI systems function as 'black boxes,' it can be difficult for legal professionals and juries to understand how conclusions were reached. This potentially undermines trust in the evidence, or even its admissibility. Additionally, biases embedded in AI systems could introduce, perpetuate or exacerbate existing inequities in the justice system.

Finally, as in many other areas, the advancement of artificial intelligence capabilities for applications in law enforcement agencies hinges crucially on the development of AI factories and high-performance computing (HPC) centres. AI factories, which streamline the creation, training and deployment of AI models, could enable law enforcement to develop new solutions and process vast amounts of data quickly and effectively. Similarly, HPC infrastructure is key to providing the computational power needed to decode (for example) criminal communications, analyse complex

datasets, perform predictive analytics, and generate actionable insights in real time. These infrastructures might become indispensable for tasks such as forensic analysis, crime pattern analysis, real-time surveillance, and threat detection, all of which demand immense processing power and scalability. Thus, investing in this infrastructure not only accelerates AI adoption but also increases law enforcement's ability to address modern challenges effectively while maintaining operational agility.

Sources: [59] [60] [61] [62] [63] [64] [65] [66]

3.8. Adversarial signal injection

Summary description

Participants discussed 'adversarial signal injection', a topic not included in the pre-workshop signal collection but considered important due to the growing role of autonomous decision-making systems. A key concern is the trustworthiness of sensor data, which is essential for these systems to function effectively.

Adversarial signal injection involves introducing malicious signals into systems to manipulate their behaviour or outputs. In machine learning, this can mean crafting inputs that deceive models into making incorrect predictions. For instance, slight alterations to images can cause a model to misclassify them, a vulnerability known as adversarial examples.

In hardware systems, attackers may inject electromagnetic signals to interfere with sensors, leading to erroneous data processing. Such attacks exploit the system's reliance on external inputs, highlighting the need for robust defences against adversarial manipulations.

Analysis

Adversarial signal injection poses significant risks to the integrity of sensor data used in autonomous decision-making systems, highlighting the need for PETs to protect against malicious manipulation. By ensuring data reliability and developing robust defence, PETs can help maintain trust in AI applications, particularly in critical areas such as law enforcement and digital forensics.

Adversarial signal injection also has serious implications for the future of law enforcement, especially in the context of digital forensics, surveillance and operational decision-making. As AI increasingly supports key law enforcement functions such as threat detection and evidence collection, safeguarding the integrity and reliability of sensor data will be vital.

Malicious actors exploiting adversarial signal injection could mislead investigations, disrupt operations or even fabricate evidence, posing major criminal threats. To counter these risks, law enforcement agencies must invest in advanced capabilities, including expertise in adversarial machine learning, resilient system design, and real-time anomaly detection.

Sources: [67] [68] [69] [70]

3.9. Trusted execution environments

Summary description

A trusted execution environment, or 'TEE', is an isolated computing space that operates independently from its host system, using hardware-based encryption to secure data in memory and application-level code. TEEs ensure that external actors, including the host, cannot access or alter the code or data during execution.

Programs within a TEE are cryptographically attested to confirm that only the intended code is executed. TEEs can be utilised to protect sensitive data during processes like model inference, ensuring data remains secure and untampered. They address concerns for system owners by safeguarding against external compute providers (e.g. cloud service companies) and provide assurances to users that their data is handled exclusively for its intended purpose without unauthorised logging or storage.

The Confidential Computing Consortium (CCC) is a community-driven initiative under the Linux Foundation, uniting hardware vendors, cloud providers and software developers to advance the adoption of TEE technologies and standards. By fostering open collaboration, the CCC aims to secure data in use by performing computations within hardware-based, attested TEEs. This approach enhances security for organisations handling sensitive and regulated data, thus addressing the need for protection across diverse computing environments, including on-premises, public cloud, and edge deployments.

Analysis

For law enforcement agencies, the importance of trusted execution environments lies in their potential to secure the handling of sensitive investigative data and ensure the privacy-compliant use of intelligence tools. As agencies increasingly rely on AI-driven analytics and cloud-based solutions, TEEs provide a robust mechanism to protect sensitive data during processing, by preventing unauthorised access even in external hosting environments. This capability could revolutionise the handling of evidence, informant data and operational plans, ensuring integrity and confidentiality.

However, the same technology could facilitate major criminal threats if used by malicious actors to conceal illicit activities. Cybercriminals might use TEEs to build secure enclaves where they can execute malware, manage illegal marketplaces or shield communications from law enforcement interception. This double-sided nature of TEEs poses significant challenges to maintaining public safety while respecting privacy.

To address these opportunities and challenges, law enforcement agencies must develop advanced forensic capabilities to analyse data processed within TEEs and collaborate with technology providers to create oversight mechanisms. Enhanced cyber intelligence, specialised training in confidential computing principles, and frameworks for lawful access to encrypted enclaves will be critical. Moreover, international cooperation and legal frameworks will be necessary to regulate and ensure the responsible use of TEE technologies.

Sources: [71] [72] [73] [74] [75]

3.10. Humanoid robots

Summary description

Humanoid robots are robots that resemble and act like humans. Typically engineered to imitate authentic human expressions, interactions and movements, these robots are often fitted with an array of cameras, sensors, AI and machine learning technologies. Humanoid robots could be used in different kinds of tasks and services, for example in healthcare, production and customer services.

Recent advancements in humanoid robotics have led to significant developments, particularly in enhanced learning capabilities, as robots now exhibit improved agility and adaptability through AI-driven imitation and reinforcement learning. Another area of progress is human-robot interaction: efforts are under way to improve robots' social interactions, with some models demonstrating lifelike facial expressions, emotion awareness and conversational abilities.

Humanoid robots present both opportunities and challenges concerning privacy. Robots can be designed to respect user privacy by implementing privacy-aware behaviours and data handling practices. Specifically, this means they can be programmed to collect only necessary data, minimising the exposure of personal information.

On the other hand, the extensive data collected by humanoid robots, including audio and video recordings, poses significant security risks if not properly managed. In this light, ensuring that robots handle sensitive information appropriately is crucial to maintaining user trust.

Analysis

Humanoid robots hold particular promise for law enforcement agencies as they augment capabilities in various operational use cases. Their ability to analyse vast amounts of real-time data and interact with civilians could boost operational efficiency and safety. For instance, robots equipped with AI can assist in de-escalating volatile situations or gathering evidence in high-risk environments without endangering human officers.

However, the same advanced features of humanoid robots could, if exploited, also facilitate major criminal threats. In the mid- to long-term future, robots' potential ability to mimic human behaviour and gather sensitive data raises concerns about their use in impersonation, cyberespionage or even sabotage if deployed maliciously.

More in the short run – and this also holds true for robotics and unmanned vehicles in general – criminals could potentially exploit vulnerabilities in systems to manipulate their behaviour, disrupt police operations, or reprogram them for illegal activities. The possibility that such robots could be hacked to access law enforcement databases or be used as tools for surveillance against civilians further underscores the critical need for robust cybersecurity measures and constant monitoring.

In addition to these operational risks, as humanoid robots gain more autonomy the question of legal attribution becomes increasingly complex. Currently, machines are regarded as tools, with legal responsibility lying with the human operator, coder or deploying entity. However, future scenarios in which robots make semi- or fully autonomous decisions raise difficult questions: namely, does liability rest with the software developer, an organisation, or the person configuring the system? This evolving landscape will potentially demand updated legal frameworks that clarify accountability in cases where robot-led actions result in harm or violate the law.

To address these opportunities and challenges, law enforcement agencies need to invest in capacities such as cybersecurity frameworks tailored for robotic technologies, ethical guidelines for humanoid robot deployment, and advanced training for officers to work alongside robots effectively. Additionally, regulatory standards must evolve to define acceptable use cases, clarify attribution and protect against abuse, thus ensuring that humanoid robots serve as tools for the public good rather than threats to safety and privacy.

Sources: [76] [77] [78] [79]

4. Glancing at the long-term horizon

This section contains complementary expert insights into: (i) the potential evolution of key emerging privacy enhancing technologies and other relevant technologies in a future more distant than the topics covered in the previous section; and (ii) what those developments would mean for law enforcement.

For this purpose, several additional interviews were held after the workshop; key insights collected are presented below. As a substantial part of privacy enhancing technology is based on encryption, the interviews carried out a deep dive into new encryption methods and techniques. In addition, based on the signals collected and discussions during the workshop, additional insights were sought into the future developments of key enabling technologies, namely AI, quantum, 6G and blockchain. The authors highlight key areas that law enforcement and decision-makers should focus on to capitalise on the opportunities these technologies present in the future.

The following subsections summarise these interviews, including selected quotes from the experts where needed to reinforce their personal perspectives on the subject.

4.1. New developments in cryptography

Introduction

The field of encryption is rapidly evolving to address emerging security challenges. One of these is the need to prepare for the advent of quantum computers, which can break current cryptographic systems like RSA[7] and elliptic curve cryptography. Therefore, **post-quantum cryptography** (PQC) has become one of the major areas of research, making it a hot topic on the agenda.

Although post-quantum computers are expected to arrive within the next 10-15 years, investment in this area is needed already now because of the threat to encrypted data posed by malicious actors who use the 'harvest now, decrypt later' strategy. They aim to collect as much data as possible now, hoping to access it later with future advancements in computing power, quantum computing or cryptanalysis.

Thus, replacing all our existing public key algorithms will be a major challenge for the next decade. To address this challenge, researchers are developing new, quantum-resistant algorithms such as lattice-based cryptography and code-based cryptography. Post-quantum cryptography is expected to be refined within the next 5 years, but its impact on law enforcement may not be immediate.

The transition to post-quantum cryptography will be complex ('annoying according to one of the interviewees and require significant investments, but it will replace existing public key algorithms with faster, more secure alternatives. This change will have a significant impact on all applications, particularly communications, with a possibly smaller effect on stored data. End users are unlikely to notice much difference. The standardisation of PQC is already under way, and the evolution of cryptographic standards may diverge between different geopolitical blocs, potentially leading to varied approaches in Europe, the US and Asia. As cyber threats escalate, the growing divergence in

[7] RSA is a widely used public key cryptosystem, also known as asymmetric cryptography.

global encryption policies could make it increasingly difficult for law enforcement to access digital evidence.

Meanwhile, another major trend in cryptography is **performing computations on encrypted data**. This enables operations to be performed on encrypted data without the need for decryption. This will bring significant changes to the field, as it shifts the focus from securing data in transit and in rest to securing data while in use. According to one of the interviewees, it is 'more or less the dream of cryptography' to be able to extract value from data while it remains encrypted. While these ideas are not new, it is only the recent emergence of techniques such as fully homomorphic encryption (FHE), multi-party computation (MPC) and zero-knowledge proofs (ZKPs) that is making this more practical, with some startups and major technology companies alike beginning to explore real-world applications.

These techniques are transformative on their own, but effectiveness of encrypted computing is amplified when combined with other privacy enhancing technologies. For instance, SMPC enables collaborative computation without exposing raw data, while TEE provides hardware-based security measures. The synergy between these approaches strengthens data privacy, particularly in sensitive fields such as finance, healthcare and law enforcement.

However, encrypted computing currently still faces some challenges, one of them being scalability. Current research is exploring lattice-based homomorphic encryption. This offers promising security properties, though it remains computationally demanding Hybrid cryptographic approaches combining multiple encryption methods are also being considered as potential solutions to improve both performance and security. The evolution of these technologies will determine how effectively encrypted computing can be deployed in real-world applications.

Another challenge in encrypted computing is computational efficiency. The reliance on bootstrapping, a technique used to reduce encryption noise, adds significant overhead, making large-scale applications resource-intensive. As dataset sizes increase, performance bottlenecks are becoming a pressing concern. Addressing these limitations requires further advancements in cryptographic algorithms and computing power, particularly as encrypted computing gains traction across various sectors.

In addition, these techniques currently come with a performance overhead compared with traditional cryptography. This makes them computationally demanding– currently 100 times slower than standard processing. Processing of encrypted data also requires significant (energy) resources. As a result, they are likely to be used primarily in markets like healthcare and finance, and perhaps also for some government data, where the need for high security outweighs the need for high performance.

Despite these challenges, these developments hold great promise for improving data security – our data will be much better protected by service providers in the cloud or in external parties.

Linkages with other emerging technologies

Advances in encryption methods are linked to other key enabling technologies, including AI. For instance, privacy-preserving machine learning is an area where encryption and AI intersect. By integrating AI with encryption, it is possible to gain valuable insights without compromising privacy. For example, computing on encrypted data enables federated learning, where multiple parties can collaboratively train AI models on private data without sharing the data itself. Another example is the combination of AI and homomorphic encryption, which allows for AI-driven analysis of

encrypted data and unlocks new opportunities for deriving valuable insights from sensitive data, for instance, in healthcare.

Looking ahead, encryption will also play a critical role in securing emerging technologies like brain-computer interfaces and robotics, where sensitive data is involved. The increasing integration of AI and robotic systems requires real-time cryptographic authentication to prevent manipulation, particularly in applications where human cognition and autonomous decision-making intersect. As these technologies continue to evolve, the need for robust encryption methods that can ensure the confidentiality, integrity and authenticity of data will become even more pressing.

Opportunities and challenges for law enforcement agencies

The new developments in encryption will bring certain challenges for law enforcement as data will not be easy to access. Currently, most often our data is stored in the cloud, and sometimes on a local device. Law enforcement agencies can now access data stored in the cloud through a judiciary authority. However, if the data is encrypted and the key belongs to the data owner, even the cloud provider will not be able to provide law enforcement with access to it.

There is also a positive side to computing on encrypted data: for instance, it would enable fraud detection to be performed in the encrypted domain. In this way, law enforcement agencies will be able to conduct full analyses of encrypted data sets to identify fraudulent activity without the need to access individual data points. However, important questions will still remain, namely who is authorised to do (what) computations, and how to ensure their correctness? For example, for data access to individual data points within a given dataset, even simple operations like retrieving a specific record (e.g. 'give me record one') should be considered a computation and not allowed. In the future, the question will not be *if* data protected, but rather what calculations can and cannot be done, and how to control this while still protecting human rights.

In addition, law enforcement will experience new opportunities to work more with local data and to perform metadata analysis, which is becoming a more powerful tool for investigations. On the one hand, given increasing amounts of data globally – both stored centrally and locally, for instance from internet protocol (IP) or door cameras, it could be more difficult to access that data (or audit who is collecting it). On the other hand, in investigations, it should be possible to go to the place where the data is stored – physically or digitally – and get the data. As one interviewee pointed out, while it is difficult to imagine that ordinary people with cameras at their doors would refuse to share the data with investigators, this might not always be the case with big cloud players accompanied by lawyers and an abundance of infrastructure.

Even if message content is encrypted, authorities can still track network activity, device locations, and communication patterns. As was already evident during the COVID-19 pandemic, contact tracing apps were available all over Europe, but neither governments nor database data owners knew what the contacts were or what the risks were for individuals. Similarly, there are technologies in place for pricing car insurance based on driving habits, as well as technologies in autonomous cars that allow for the collection and analysis of local data. There was already a terrorism case in Belgium investigated based on data from car rentals in Germany.

Advancements in encryption hold other potential benefits for law enforcement, particularly in verifying digital evidence and securing communications. If cryptographic methods can be seamlessly integrated into information verification systems, they could counteract the growing risk of AI-generated misinformation, help preserve authenticity in the face of the increasing volumes and improving quality of synthetic data. Encrypted computing and homomorphic encryption could

enable secure and privacy-preserving data access, allowing for controlled investigations and secure cloud computing, where law enforcement agencies can analyse sensitive data and access encrypted evidence without exposing unrelated information or compromising data security.

Another interviewee suggested the need for effective lawful interception mechanisms that do not compromise individual privacy. However, ensuring that these frameworks are effective and resistant to abuse remains a complex legal and technical challenge.

Criminal activities facilitated by cryptography

All these new technologies can also be used by criminal networks. One expert noted, for instance, that while encrypted computing offers strong privacy protections, it may also enable illicit activities to go undetected. Criminal actors could leverage encrypted computing to operate secure, hidden networks, making it difficult for authorities to track illegal transactions, communications or data exchanges. Privacy-preserving computation could also complicate efforts to monitor financial crimes, as encrypted transactions may become more difficult to trace.

Moreover, encrypted computing could facilitate new forms of cybercrime. Ransomware attackers, for instance, might use homomorphic encryption to process encrypted ransom payments in a way that remains hidden from authorities. Law enforcement must therefore explore alternative approaches, such as targeting endpoint vulnerabilities, behavioural analysis and forensic techniques that do not rely solely on decrypting digital evidence. The use of fully homomorphic encryption could enable criminal actors to optimise their operations, creating encrypted information-sharing platforms that are beyond the reach of law enforcement. These developments underscore the urgency for law enforcement agencies to invest in detection capabilities that identify hidden patterns in encrypted data, rather than relying on traditional interception techniques.

On the other hand, according to another expert, to 'take the helicopter view', doing things 'out of the radar' is becoming harder now because of digital traces and connectivity. What is currently absent is network-level privacy, which means your IP address is everywhere. Despite the existence of technologies like Tor[8] and emerging startups working on solutions to hide IP addresses, these efforts face an uphill battle and have not achieved widespread adoption. While virtual private networks have gained popularity as a privacy tool, they are not without limitations, as they essentially funnel all user traffic through a single point, creating a centralised repository of data. While encrypting content is becoming easier, it is increasingly difficult to protect metadata (location, IP addresses, communication patterns). In response, law enforcement should focus more on metadata analysis – in the view of one expert, this is 'where law enforcement will win in the end'.

Also, considering the way other technologies operate – be it your phone contacting wi-fi networks, or cashless payments performed even for parking the car – your digital traces are left everywhere. In the view of one interviewee, the problem is not that it has become harder for law enforcement to catch criminals, but the other way round: with current technologies it's 'very hard for [criminals] to do something and not be traced'. With the data owned by private companies, the difficulty nowadays for law enforcement is to access that data, not that it does not exist. It is just a very small proportion of criminal networks, based in 'some third countries', with access to very

[8] Tor (The Onion Router) is a free, open-source software that enables anonymous communication over the internet. It enables users to browse the web, send emails, and chat online without revealing their IP address or location.

sophisticated technologies and using cryptocurrencies in a special way, that might trigger the need for a very specific type of response.

Insights for policy-makers

As our societies become increasingly digital, and thus also more vulnerable, the expectation is that encryption should be widely used to make sure our systems are secure and robust against possible cyber-attacks and outages. Indeed, this is precisely what some interviewees recommended. This is not just a matter of individual privacy but also of national security. As the recent US example shows, it is now mandatory to use encryption for all governmental communications [80]. However, balancing security with the right to privacy will remain an important issue, while also bringing some new considerations and perspectives.

First, legal frameworks must evolve to accommodate the growing reliance on encrypted computing, as existing laws on data access and privacy were not designed for a world in which computations can occur without exposing raw data. New policies must clarify under what conditions encrypted personal data may be accessed or analysed and what calculations can (or cannot) be made, while ensuring that law enforcement agencies can still perform their investigative functions without undermining privacy rights.

One of the first steps in this process is to clearly determine the contexts in which encrypted computing can be used. Understanding its relevance across different sectors, from healthcare and finance to law enforcement, will help shape rules that support innovation while addressing security concerns. Regulatory frameworks should ensure that personal data remains secure while allowing for controlled access in the context of criminal investigations. Additionally, law enforcement agencies should explore the possibility of improving their analysis of metadata to make it more resilient, as well as further improve, investigative capabilities.

Furthermore, there is a need for sustained investment in the infrastructure and expertise required to support encrypted computing. Governments and industry leaders must allocate resources to develop more efficient cryptographic techniques and ensure that institutions have the technical capabilities to work with encrypted computing securely. Without sufficient funding and expertise, the practical adoption of this technology will remain limited, and its potential benefits not fully realised.

To sum up, law enforcement and policy-makers should adopt a proactive, forward-thinking approach to address changing technological landscapes and emerging risks. Collaboration between law enforcement, policy-makers, research institutions and technology developers will be crucial in order to navigate the complexities of encrypted computing and shape the regulatory regime for emerging privacy enhancing technologies. By staying informed about emerging advances and addressing challenges proactively, policy-makers can help create an ecosystem where encrypted computing enhances privacy and security without impeding law enforcement.

4.2. AI: new developments related with privacy

Introduction

AI is not a single, uniform technology. It is an umbrella term for a broad spectrum of tools and methodologies. Some areas of AI are highly mature and already being widely deployed, while others are still in early stages of research. What is special about AI is that it differs from other technologies due to its highly applied nature. Unlike other areas of technology, with AI it is possible

to rapidly progress from concept to practical application, largely because AI typically requires real-world data to develop meaningful and useful solutions.

The foundation of AI technology rests on two approaches. The first relies on machine learning (ML) – the fundamental technology underpinning AI – and neural networks, which learn to identify patterns in data through probability-based analysis. These systems either structure data or predict likely outcomes by analysing previous steps. This approach forms the basis of much current AI research and applications in natural language processing or computer vision.

The second approach, **symbolic AI**, builds on deductive inference and logic-based systems. Rather than learning from data patterns, symbolic systems use explicit rules and structured logical reasoning to solve problems, which enhances trustworthiness and explainability.

Recognising that each approach has distinct strengths and limitations, researchers are now exploring ways to combine them: '**neurosymbolic AI'** merges neural networks' powerful pattern recognition capabilities with symbolic systems' rules-based logical reasoning. Such integrated systems can address complex and data-rich tasks with improved transparency and interpretability.

Recognising that each approach has distinct strengths and limitations, researchers are now exploring ways to combine them: 'neurosymbolic AI' merges neural networks' powerful pattern recognition capabilities with symbolic systems' rules-based logical reasoning. Such integrated systems can address complex, data-rich tasks with improved transparency and interpretability.

'**Privacy-preserving AI**' or privacy-preserving technology, is a separate research field of its own, making use of tools such as synthetic data. Synthetic data is artificially generated data to mimic the statistical properties, patterns, and structure of real-world data. The benefits of synthetic data is that it addresses concerns both about privacy and fairness. This type of data allows to remove connections to sensitive personal attributes of an individual. It can also be tailored to include underrepresented groups that are often missing or insufficiently represented in real-world datasets, thereby helping to mitigate biases in AI systems.

Another category is **federated learning (FL),** a distributed ML approach in which the training of a global AI model occurs locally on devices or servers storing the data, rather than transferring data to a central server. This differs from a more traditional or centralised approach in which the data is moved to some central server or data centre where the training takes place. FL makes it possible to conduct training in a distributed way, after which it is then possible to share partially trained models (or parameter gradients[9]) to improve the global model. By keeping data decentralised, FL enhances privacy and reduces the risk of data breaches. Additionally, FL enables collaboration between partners (e.g., hospitals, banks) by allowing them to jointly train a model while preserving data confidentiality.

One more key development in the area of cybersecurity and data protection is **tokenisation**, which converts original data into tokens (usually smaller components of larger data). In the tokenisation process, original data, such as text or credit card numbers is replaced with non-sensitive data (tokens). This means that the original data is stored securely in a separate database, and tokens are

[9] In ML, gradients guide the computer to automatically adjust the model's settings (parameters) to improve its performance.

used instead for processing or analytics. These tokens can usually be reversed back to the original data (known as **reversible tokenisation**).

One idea currently being explored by researchers is that of '**irreversible tokenisation**' which is designed to permanently anonymize sensitive data, such as private data. This method is similar to a one-time encryption without a decryption. This approach offers a way to hide data by making the tokenisation process irreversible.

The advantage of tokenised data is that it can be securely shared with trusted parties or stored for later access. However, there are key differences between the two approaches. Reversible tokenisation is used when access to the original data is necessary under certain conditions, such as in financial services to process credit card transactions. In contrast, irreversible tokenisation is applied when the goal is to ensure anonymity, such as sharing anonymised healthcare data for research without exposing patient identities.

Linkages with other technologies

AI can be linked with several other emerging technologies, like the IoT, blockchain, biometrics, digital forensics, autonomous systems (such as drones and self-driving cars), etc. Linking AI to these technologies could make it possible to produce tools for use in in predictive policing, intelligent surveillance, digital evidence analysis and other areas.

According to one of the interviewees, AI is a useful tool, but is also a 'double-edged sword'. This can be seen, for instance, in the area of data analysis. There is now much more data available than a decade ago, and performing data analysis has become much easier and less costly than even a few years ago, thanks to tools like ChatGPT and Co-pilot.

In the past, acquiring data was expensive, and analysing it was even more so: it often required hiring data analysts and data scientists. But now these tools can help automate data-analysis tasks. Despite this progress, there are concerns about the accuracy, risk of abuse and legitimacy of analyses performed by such tools. These machines have internal memory, and the analysis done by them is becoming more complex and sophisticated. Most everyday users of these tools do not fully understand how LLMs work – they provide the user with what appear to be fantastic results, but these users cannot explain how the LLMs arrived at these results. If you ask an LLM how it arrived at a certain conclusion, it can even provide you with data to substantiate its own analysis, but it is not necessarily accurate or verifiable[10]. These functionalities carry tremendous potential but also enormous risks. In the future it will become much more difficult to keep track of what is happening in datasets as anyone could change them by inserting just a few lines of code into them.

Opportunities and challenges for law enforcement agencies

AI is already being used in law enforcement. There are many discrete tasks in this area where AI tools can be used, making it possible to both investigate more cases, and ensure that these cases are better prepared if they go to court. These discrete tasks include tasks currently performed

[10] For instance, AI can produce so-called "hallucinated data", meaning fabricated or false information generated by an AI system—particularly large language models (LLMs)—that is presented as if it were factual or accurate.

exclusively by humans, but which AI enables humans to do in a more efficient way, such as collecting and analysing data, gathering evidence, and redacting documents. For example, AI is already being used for video-footage analysis, which otherwise requires humans to spend thousands of hours reviewing video footage during investigations. Another example of the utility of AI in law enforcement was a case in one EU Member State where AI was used to count pills of illegal drugs that had been seized during a police operation. A digital camera and computer completed the calculation in a matter of seconds. This saved the need for people to manually count the pills.

AI can also help law enforcement bodies perform new and more complex tasks, such as analysing social media. For example, AI can help to identify individuals behind anonymous social media accounts by examining their linguistic 'signatures'. 'Signatures' in this sense does not mean the name that people use to sign paper documents with, but instead refers to the way a person writes, and the way that they express themselves - for example if they' re using uncommon words or unusual language patterns. This makes it possible to find connections between writing patterns and so on, although this use case for an AI tool would raise issues from a privacy perspective. Criminal actors are becoming more sophisticated in hiding their activities, often using many layers of identities, different companies, different names, and different organisations. This sophistication on the part of criminals makes it all the more important to be able to identify unexpected connections and complex patterns in data, and this is exactly where AI can be of help, detecting these patterns and analysing large amounts of data.

However, privacy considerations can arise when using AI in certain contexts, as it may be challenging to interpret existing privacy regulations in relation to some AI applications. For example, questions around how the GDPR applies in practice can influence the adoption of certain AI techniques in areas such as law enforcement, particularly where it is not always clear how existing rules apply to the use of large language models. For instance, if an LLM generates information about a person and this is considered personal data, it may raise questions about responsibilities among the different actors involved, such as model developers and those who use or query the system. According to the GDPR, there are conditions that must be met before anyone can collect and process information about specific individuals[11]. But this raises issues.

For instance, when analysing video footage, police need to search for specific individuals. However, one of the interviewees highlighted challenges in improving search systems due to privacy restrictions that prevent sharing models or training data. Synthetic data might be suggested as a privacy-preserving solution, though it has limitations when specific individual recognition is required.

Or another problem: a court wants to find sensitive information in its documents so that this information can be removed before making the documents public. But if they use an AI to find this

[11] Nevertheless, the GDPR allows exceptions for law enforcement agencies. For example, Article 23 of the GDPR: Derogations for Law Enforcement - allows Member States to decide on exceptions and derogations from the GDPR to permit the investigation of crimes and the fight against terrorism. In addition, Article 26 of the GDPR: Specific Processing Situations - allows Member States to draw up specific rules for the protection of personal data in the context of cooperation between law enforcement and judicial authorities in criminal matters. Also relevant in this context, the following pieces of legislation were created to balance the need to protect personal data with the need to prevent and investigate crimes, and to combat terrorism:
(i) the Law Enforcement Directive (LED): Directive (EU) 2016/680; (ii) the Police and Criminal Justice Authorities Directive: Directive (EU) 2016/680; and (iii) the Terrorism Directive: Directive (EU) 2017/541; Interinstitutional Agreement: Regulation (EU) 2018/1805.

information, then the AI will have had access to someone's personal information, potentially violating the GDPR. As one of the interviewees said, 'the legal uncertainty is such that the lawyers don't dare to use it. It may be legal, but no one really knows'. So, even if the law enforcement body wants to do the right thing, and even if the researchers want to be on the right side of the law, if the law is unclear, it remains impossible for researchers to help law enforcement to use AI in many areas. As one of the interviewees said, the consequence of this uncertainty is that 'you do nothing, and that's even worse thinking about the alternative costs'. This raises the uncomfortable prospect that those that do not care about the law in the least will ultimately have a major advantage in the use of AI.

Criminal activities facilitated by AI

The increasing use of AI has enabled various criminal activities, including misinformation and disinformation campaigns. With the increasing ease of creating realistic fake information, it has become challenging for many people to distinguish between fact and fiction. For instance, manipulated photos and videos can be made to look almost authentic, making it difficult to verify the authenticity of evidence. As a result, we can no longer trust our senses to determine what is real and what is not. Other criminal activities that have been made easier by AI include phishing, cyber-attacks, and financial crimes, which can now be carried out with greater sophistication and ease.

Insights for policy-makers

There are also some other important points for policy-makers to consider. Firstly, an important issue in dealing with AI is establishing boundaries. As most of AI is probabilistic, it is important for policy-makers to ask themselves what they consider an acceptable level of probability for data re-identification – that is, the process of linking the anonymised or de-identified data back to specific individuals: Is a 10% probability of re-identification too high? How about a 1% probability? How about a 0.1% probability?. We should acknowledge the fact that 'perfect privacy' probably does not exist, as re-identification remains possible despite efforts to hide the data. Even if protective measures are taken, with sufficient external information, it is often possible to find out the concealed information.

Another key issue is the absence of AI-specific skills in this area. Legal departments in companies and governments often lack a comprehensive understanding of how certain technology works. This can lead to decision-making that doesn't fully take into consideration technological possibilities and the potential consequences of different choices. The lack of AI-specific skills, organisational constraints, and questions regarding the interpretation of privacy regulations were identified by interviewees as key factors limiting the more effective use of AI.

An additional area of concern is baselines. There is a tendency for users to expect technical systems to be perfect. One interviewee lamented the quite straightforward and binary approach to technical systems often taken by users in this area: 'either they are perfect or they are broken'. But perhaps a more nuanced approached is needed: as long as the systems are significantly better than what we have at present, then they can be considered an improvement. The bar of expectations can be set unnecessarily high, such that we get worse outcomes in the end. This is partly due to the challenge from the legal perspective, which is that there is no difference between being 5% compliant and 95% compliant. But in practice there is a huge difference between two systems. In some sense, we are currently failing to use a 95% compliant system as it is not good enough. Instead, we use something else, which is maybe significantly worse. There is no question that we need to make sure

that we make significant improvements to our AI tools. But it will be hard to benefit from the advantages of AI if we demand 100% perfection from AI tools.

Then there is an issue about the extent to which AI tools are allowed to benefit from memory gained in other domains. Employees are often valued if they have experience. If a person has worked in many different parts and in many different organisations and learned from all of this, then they are often more valuable to a company. But current rules surrounding the privacy of data make it difficult for an AI to become 'experienced' by trying to do the same thing – namely learn from a wide variety of contexts. As one interviewee complained, the attitude towards an AI learning from a wide variety of fields is 'no, no, no, you're not allowed to share anything you learned from working in a different case now that you go to this case - it's weird'. This interviewee believed that maybe we need to consider AIs more like the way we consider people (both grow and gain in experience) rather than the way we have dealt with other technologies. The interviewee also stressed that it was important to consider the alternative costs of failing to use AI: how many more cases could have been solved, how many lives could we have spared if we had used that technology? 'There's a cost associated with doing it,' said the interviewee. '[But] there's a cost associated with not doing it. There's no neutral alternative here.'

4.3. Quantum communications: safer than ever

Introduction

Quantum communication revolutionises secure data transmission by harnessing quantum physics to address encryption vulnerabilities [81]. One of the most promising applications is quantum key distribution (QKD), where security relies on the laws of quantum mechanics rather than mathematical algorithms. In QKD, two parties generate a secret key using qubits, and this key is then used to encrypt and decrypt messages. This key remains secure against quantum computer attacks, as its transmission is based on quantum states. Meanwhile, the data itself can travel through conventional channels. QKD also allows for the detection of eavesdropping attempts.

QKD is already being implemented beyond the prototype stage and is in use within specific niche areas. However, its widespread adoption is limited by technical challenges because it is so technically demanding. QKD requires specialised hardware, dedicated links, and 'point-to-point' connections, restricting communication to secure endpoints. Currently, the span between nodes on terrestrial lines across which QKD can still be useful is limited to a few hundred kilometres – typically 200 to 400 kilometres – with no capability for transatlantic connections. The construction of a broader quantum network or 'quantum internet' depends on advances in quantum routing technology, which have not yet occurred.

Another option for enabling secure long-distance key exchange is to use satellites, specifically satellite constellations, to facilitate communication with lasers from the ground to the satellite. This technology is still in its early stages. The first European satellite being built for this purpose, Eagle One, is currently under development and is expected to be launched around November 2026. However, the concept for this technology was already demonstrated in 2016 by the Chinese satellite QUESS, with similar demonstrations occurring in the US, Japan, and other countries. Many nations are developing satellites for QKD, moving beyond prototyping to planned constellations similar to Starlink, but using optical links to the Earth. This technology may become available for routine use in Europe within five to seven years. Nevertheless, QKD will probably not be used by

ordinary individuals and is instead likely to be limited to institutions, such as banks, power stations, health data centres, and large telecom centres.

Linkages with other emerging technologies

Quantum communication stands somewhat alone as a technology. It primarily requires high-quality lasers, optical fibres, cryogenics, and nanotechnology, particularly for components like single-photon nanowire detectors. Quantum communication also does not have any direct link to other technologies that are frequently discussed in the media, such as AI or biotechnology. Although AI is currently utilised in quantum computing for tasks like error correction, AI is not at present directly used in quantum communication[12].

Another group of early-stage emerging technologies that shows promising potential to protect privacy is the group of steganography technologies. These technologies cover methods and tools used to hide information within other seemingly innocuous data or media (such as images, audio, video, or text) in such a way that the presence of the information itself is concealed. Unlike encryption, which hides the content of a message, steganography hides the fact that a message exists at all. For instance, quantum steganography is an emerging and highly theoretical branch of steganography that combines principles of quantum mechanics with traditional covert communication techniques. Quantum steganography makes use of quantum cryptography to develop new methods for hiding secret information in quantum communication channels, ensuring that the very presence of a message remains undetectable, even to adversaries equipped with quantum-aware capabilities. This approach also ensures that any attempt to measure or eavesdrop on a quantum system will disrupt that system, alerting users to potential tampering, and thereby guaranteeing secure communication.

Opportunities and challenges for law enforcement

Quantum communications are currently the most secure transmission methods available because it is physically impossible to copy this data. And given the threat of global harvesting of encrypted data, quantum communications are a way to protect the transmission of keys that are used to encrypt sensitive data. For this reason, quantum communications could be useful in helping law enforcement to secure and share sensitive information.

Criminal activities facilitated by QKD

Due to its demanding technical hardware requirements, QKD is less accessible to low-budget actors, including many criminals, thus making it less likely for them to use QKD than other technologies. Additionally, current QKD deployments are often concentrated in regulated and well-monitored sectors (e.g., governments, research institutions). As a result, it is still feasible for them to maintain a list of QKD users, as installing these systems without detection is difficult. Consequently, QKD is unlikely to become a significant threat in this context. However, if QKD becomes more accessible and commercialised (e.g., via satellite networks, cloud-based services, or open-source tools),

[12] Some research suggests that AI could enhance QKD by enabling error correction, detecting security breaches, and optimising key generation rates

maintaining a comprehensive user list will become increasingly challenging. This may open opportunities for malicious actors to exploit the system covertly.

However, if a QKD network were to be installed by criminal organisation, it would provide secure transmission, making it impossible to eavesdrop or obtain the transmitted information.Insights for policy-makers

Policy-makers should promote the installation and adoption of this technology by eligible and verified end users, and identify legitimate use cases for it as a means to secure the sharing of sensitive information.

4.4. 6G: the next generation of wireless communication technologies

Introduction

While 5G networks are still being deployed and refined, researchers and industry experts are already exploring the possibilities of 6G - the sixth generation of wireless communication technologies. 6G is currently in the applied research phase (TRL 3-5), with some components of the 6G infrastructure more advanced than others. While many vendors have been working on 6G since before 2020, full deployment of 6G is expected around 2030-2031, following the completion of standardisation efforts by 2028. Unlike previous generations of wireless networks, 6G is envisioned as more than just a communication technology – it will also integrate sensing capabilities, AI-driven network management, and satellite connectivity. It represents a major leap forward in digital connectivity, and it will mean much more than just an incremental improvement such as the transition from 4G to 5G.

A defining characteristic of 6G is its three-dimensional network structure, which will extend beyond traditional terrestrial infrastructure. Low-earth-orbit (LEO) satellites, high-altitude drones, and intelligent surfaces[13] will form part of a layered connectivity system in 6G, enabling seamless communication and ubiquitous coverage, even in remote areas. This convergence with satellite networks will make it possible for ordinary mobile devices to communicate directly with LEO satellites, further expanding connectivity options.

Another benefit of 6G is network-integrated sensing, in which 6G infrastructure can be equipped with radar-like capabilities, giving it a type of environmental awareness. This could be used in applications such as traffic management, smart cities, and security monitoring, though the exact arrangements for implementation necessary to address privacy concerns remain a topic of discussion.

Linkages with other emerging technologies

6G will be deeply intertwined with other frontier technologies. For example, AI will play a crucial role in managing and optimising the 6G network, enabling real-time adjustments for efficiency and

[13] Intelligent surface, or Reconfigurable Intelligent Surface (RIS) is an ultra-thin, planar structure embedded with a dense array of meta-atoms (programmable elements) that can dynamically control the reflection of electromagnetic signals in real-time. RIS is aimed at enhancing wireless communication

security. There is an ongoing debate about whether significant progress in AI will be required for 6G, or whether existing AI systems will be sufficient.

Photonics and light-based communication will be instrumental in improving network performance, particularly in space-based communication. Quantum networking will eventually have to be integrated into our regular communication network infrastructure, such as 6G, in a way that will make it possible to provide new capabilities in secure communications and cryptography. However, this will require significant improvements in the area of semiconductors, antennas, and cloud-based processing.

Another key technological link is secure multi-party computation (SMPC), which could improve data integrity and trust in digital interactions within 6G networks.

However, geopolitical factors may influence standardisation, supply-chain access, and hardware availability, potentially leading to fragmentation in global implementation.

Opportunities and challenges for law enforcement agencies

6G could be a powerful tool for law enforcement, providing richer data sources for both investigations and security operations. The 6G network's built-in sensing capabilities could allow authorities to track movement patterns, detect anomalies in these patterns, and increase situational awareness in real-time. Crowd management and public-safety applications could be significantly improved through these capabilities. At the same time, the use of this aspect of the technology could pose a threat to the privacy and personal data of 6G users – and of the public more generally – in the case of 6G sensing. This calls for the timely and integrated consideration of all policy aspects.

In addition, the increased volume of data and the distributed nature of 6G networks present new challenges. With AI embedded at various network layers – including the radio access network, core infrastructure, and edge devices – it will be harder to trace and access digital evidence. The mobility of data – shifting between the cloud, other networks, and user devices – raises concerns about data jurisdiction, lawful interception and the practical execution of that interception.

Law enforcement will also face difficulties in interpreting AI-driven decisions within the network. If AI is autonomously managing traffic, security protocols, or even surveillance mechanisms, understanding and challenging the AI's decisions in legal proceedings may be complex. The opacity of AI-driven network operations may create barriers to accountability and transparency.

Criminal activities facilitated by 6G

The integration of AI, sensing, and decentralised data processing in 6G increases the risk of exploitation by cybercriminals, hostile entities, and rogue actors. The vast amount of real-time data collected through sensing technologies could enable large-scale surveillance, raising concerns about privacy abuses by authoritarian regimes or private entities. With every object and individual generating data, the risk of mass tracking and profiling increases. The protection of both privacy and personal data is therefore an important consideration in the current debate about standardisation in 6G.

AI-driven network automation introduces new attack vectors, where adversaries could manipulate AI decision-making processes to misdirect traffic or disrupt services at unprecedented speeds. The ability to interfere with AI-controlled infrastructures, such as traffic systems or energy grids, could lead to cascading failures in essential services.

In addition, the distributed nature of 6G will make it more complex to track digital evidence, as data will continuously shift between cloud environments, network nodes, and edge devices. Criminal actors could exploit this mobility to evade detection, making lawful access to e-evidence increasingly challenging. The increased bandwidth and real-time computing power required by 6G will also facilitate more sophisticated cyber-attacks, deepfake generation, and misinformation campaigns. Without early safeguards, 6G's greater capabilities could be exploited for highly disruptive cyber and physical threats. This calls for urgent adaptation in security policies and law enforcement strategies.

Insights for policy-makers

The rapid evolution of 6G requires urgent policy adaptation. As one interviewee stated: 'as standards are being discussed by industry, now is the time to act'. Policy-makers should develop a deep understanding of the technology to ensure that the legal frameworks they draw up to regulate the technology are both effective and enforceable. Without this, there is a risk that incomplete or outdated legal frameworks could slow down innovation or fail to address security concerns.

A major policy challenge lies in the governance of AI, cloud infrastructure, and data flows within 6G networks. Until recently, cloud services and AI models were seen as something that should be available on open markets. However, they are increasingly seen as strategic assets, and governments are therefore reconsidering how they are controlled and regulated. Ensuring that essential infrastructure remains under sovereign control (for instance, requiring European telecom providers to use EU-based cloud services) could increase digital autonomy and prevent overreliance on non-European hyperscale cloud providers.

Policy-makers should also address the issue of resilience in network infrastructure. Given Europe's high dependency on digital connectivity, there should be policies in place in the EU to mandate redundancy – such as requiring operators to use multiple cloud providers to avoid single points of failure. This approach would increase resilience in the face of cyber threats or geopolitical disruptions.

For law enforcement and policy-makers, the stakes are high. The sheer volume of data and increased automation in network management could offer new tools for security, investigations, and public safety, but they also introduce complex risks related to AI transparency, cyber threats, and the potential for abuse. Criminal actors could exploit AI-driven network controls, inject malicious nodes, or exploit sensing technologies for illicit purposes.

To navigate these challenges, policy-makers should act now, even with incomplete information, because waiting too long to act will leave them behind. Policy-makers should be proactive in ensuring that 6G develops in a way that aligns with the public interest and the EU's security and democratic values. 6G technology will be developed based on standards that are drawn up today. Waiting for the complete technological picture to develop before drawing up standards would mean that these standards are finalised after the technology has been developed, and by then it would be too late to have an impact on the technology through regulation. Investing in education, legal frameworks, and digital sovereignty will be crucial to ensuring that 6G is developed responsibly. Collaboration between law enforcement, technology providers, and research institutions will be essential in shaping a secure and equitable digital future.

4.5. Blockchain: look for new use cases

Introduction

Blockchain, like other distributed ledger technologies (DLTs) is already being used today in various niches and industries, such as cryptocurrencies and digital assets. Nevertheless, it remains a relatively new and emerging technology. When these DLT technologies originally emerged, there was a lot of misunderstanding and confusion around them. Certain advocates for DLTs oversold the technology, implying it had an almost limitless number of use cases. However, these claims about the utility of DLTs are exaggerated – the technology itself is subject to different types of constraints related to performance, scalability, and other technical aspects.

It is therefore important to look for specific use cases where blockchain technology is being used, or could be useful, such as supply-chain management, goods traceability, and other similar applications. In some cases, it's not the blockchain itself that is relevant, but rather the use of smart contracts, which enable immutable code execution and ensure consistent, tamper-proof execution. Today, the languages used to implement smart contracts have limitations in terms of power and complexity if compared to commonly used programming languages. This means that one of the things that we will most likely see change in the future in this area is both the power and the capabilities of the language used for smart contracts.

Another potential area of evolution in blockchain technology is related to the type of cryptography that is used to guarantee important features, like immutability.

For example, there is currently an active debate among blockchain experts about the possibility of changing the type of algorithms that are used in blockchain to transition to a post-quantum era. The algorithms currently used by blockchain are in fact potentially prone to quantum attacks. This means that even a data structure that is hyper-replicated[14] and distributed, risks beings successfully exploited when quantum computers become available. There is therefore already an effort underway to try to implement new algorithms that are post-quantum resistant in blockchains. And this effort has been accelerating since 2024 because the US National Institute of Standards and Technology published the first official suite of algorithms that are recognised as post-quantum resistant.

Another area where we might see development is in the interplay between AI and blockchain. However, according to one interviewee it is difficult to foresee further technological developments in this area without understanding eventual the use cases.

There may also be further technical developments in the evolution of blockchain itself. For example, there is already a trend for various services and infrastructures to design their own blockchains to deliver specific solutions. However, as the blockchain ecosystem continues to grow, different blockchains, potentially with different architectures and paradigms, will need to interact with each other. And although there are already some interoperable solutions in this area to make this interaction possible, it will be necessary for blockchain developers to decide on further interoperability protocols and processes that make it possible to compose services built from

[14] In the context of blockchain, "hyper-replicated" refers to the extensive and redundant duplication of blockchain data across a vast network of nodes.

existing blockchain-based building blocks. This will enable the creation of more complex and sophisticated applications and even ecosystems, although it also raises the possibility of new technical vulnerabilities.

Linkages with other technologies

One area where blockchain could become more relevant in the future is in critical settings, such as critical infrastructures (such as the infrastructure for electricity, gas or water). As an example of how blockchain could become relevant in this area, one interviewee gave the example of a pilot study conducted by their group a couple of years ago on using blockchain in the energy sector to implement energy communities. This highlights the importance of considering the potential challenges of implementing blockchain in critical settings. One key challenge that became apparent to the group is network availability, as a distributed system like blockchain can be affected by network outages. Although the blockchain's distributed nature makes it highly resilient, a network outage could still cause imbalances in the blockchain network, leading to uneven information dissemination. In such cases, some parts of the network might not be working, while others would continue to function, resulting in inconsistent data distribution.

This issue of network availability highlights the importance of next-generation internet. Since blockchain relies on a network to function, the development of next-generation internet – which will be much more resilient and less prone to outages than earlier versions of the internet – is essential to the growth and adoption of blockchain. In fact, without a robust and secure network, blockchain would not be possible, making network resilience in general – and next-generation internet in particular – a critical component of the blockchain ecosystem.

As mentioned earlier, there are also potential linkages between blockchain and emergent technologies like PQC and AI. Although there is no current direct link between quantum cryptography and blockchain, there is a need to protect blockchain from future quantum threats. PQC is relevant in this respect because it can help to ensure the long-term security of blockchain systems against potential quantum computer attacks.

Finally, another potential area of concern relates to data leaks and the availability of data. As we start to use blockchain in more and more ways, there will be a growing need to both: (i) access and feed data into smart contracts; and (ii) ensure the security and integrity of blockchain systems.

Opportunities and challenges for law enforcement

According to one of the interviewees, the challenges and opportunities for law enforcement in this area really depend on the type of use case at which law enforcement is looking. For example, it is well-known that organised crime is still using some cryptocurrencies to hide their own activities or to launder the financial proceeds of their crimes. One of the challenges/opportunities for law enforcement is therefore to try to track down and trace the entire process used by organised crime groups to launder money, and then recycle this money into other legitimate business. Doing this is a challenge because it is often difficult to follow the entire chain through which financial proceeds of crime travel as they are laundered. This becomes even more complex when decentralised technologies are involved, raising critical questions around jurisdiction. These questions include: how should law enforcement respond when the perpetrator is a decentralised community? How can illicit content be removed from a blockchain, and who receives a warrant in the context of decentralised applications (DApps) where criminal content or evidence may reside?

Since their creation, cryptocurrencies caught the attention of organised crime groups because they promised untraceability and anonymity via the blockchain. However, in most cases, it is now possible for investigators with enough resources to track down these transactions, especially because there is now a much more regulated environment for what are called the 'exchange companies' that are in charge of converting fiat money into different cryptocurrencies, and vice versa. The fast-paced development of AI and its capacity for large data analysis and pattern recognition might expand this capacity in the future.

One of the interviewees said that this work of tracing cryptocurrency transactions – in particular through the exchange companies – was an area of particular – and likely growing – relevance for law enforcement.

Criminal activities facilitated by blockchain

Self-sovereign identity (SSI) is a digital identity framework in which individuals themselves, rather than third parties like governments, control their personal data and credentials. SSI allows users to decide what information to share, with whom, and when. When implemented using blockchain, new risks can arise, such as theft or private key or exploitation of smart contract vulnerabilities. However, blockchain also reduces traditional identity risks such as data breaches and single points of failure. The ongoing debate around SSI includes security concerns as well as challenges related to scalability, regulatory compliance, and user adoption.

Another increasing discussion in policy circles is about introducing a digital euro. This digital euro would be like the euro already in use, but its use could be more easily traced, in theory making criminality more difficult. There are different types of technologies that can be used to implement a digital euro, but one of these types of technologies would use distributed ledgers and blockchain. If a digital euro based on distributed ledgers and blockchains is adopted, then the security and integrity of blockchains could be challenged by criminals to try to steal digital money. Such scenarios reveal that vulnerabilities in this area are not simply based on blockchain itself. They are also a matter of the security of the entire ecosystem deployed to make digital money usable (e.g. digital wallets, smartphone-secure hardware, etc.).

Insights for policy-makers

The potential risks and benefits of blockchain technology depend on how it is used and implemented, according to interviewees. Like many other technologies, blockchain is not risky in and of itself – it is the use to which it is put that can make it risky. Connected to this, what makes blockchain technology interesting from a regulatory perspective is how it can be used to implement something. This means that advice on the use of blockchain technology could vary depending on the different domains it is deployed in. It is very difficult to give generic advice on the blockchain without knowing the use to which it will be put.

4.6. Section endnote

In summary, as PETs and key enabling technologies continue to evolve, it is becoming essential for both law enforcement and policy-makers to get a deeper understanding of the opportunities and challenges these technologies bring to society. The emerging technologies overviewed in this section seem to be promising in that they support or open up new possibilities for law enforcement agencies in their activities. However, they can also be a double-edged sword, as they also open up new opportunities for criminals. Decision-makers should take this into account when reviewing or adopting new regulatory frameworks, while law enforcement authorities should proactively prepare for upcoming changes that pose both limitations, but also open up new opportunities to prevent or investigate crimes. These challenges will also have to be addressed while balancing the right to privacy and security.

5. Contextual factors for the development and uptake of privacy enhancing technologies (PETs)

In this section, we present an overview of relevant contextual factors that will affect the development, uptake and use of PETs in the future. The overview is based on the results of the workshop discussion. To assess these contextual factors, an adaptation of the 'futures triangle' methodology [82] was used during the workshop. To assist in a broader reflection on relevant contextual factors according to the PESTEL methodology[15], we provide a summary of the groups' discussions together with the additional desk research based on selected signals.

Drivers, enablers and barriers

An adaptation of the 'futures triangle' methodology was used during the workshop to identify the most relevant contextual factors that have affected – and are likely to continue to affect – the development, uptake and future use of PETs. This methodology helps to outline past, present and future dimensions of the context of the technologies in question as a result of three interacting forces: the pull of the future, the push of the present and the weight of the past. These forces, or factors, are categorised as drivers (the pull of the future), enablers (the push of the present) and barriers (the weight of the past) with each factor occupying one point on the triangle. These factors are theoretically distinct even though the same factor can often be categorised as being on two or more angles of the triangle, depending on the issue in question.

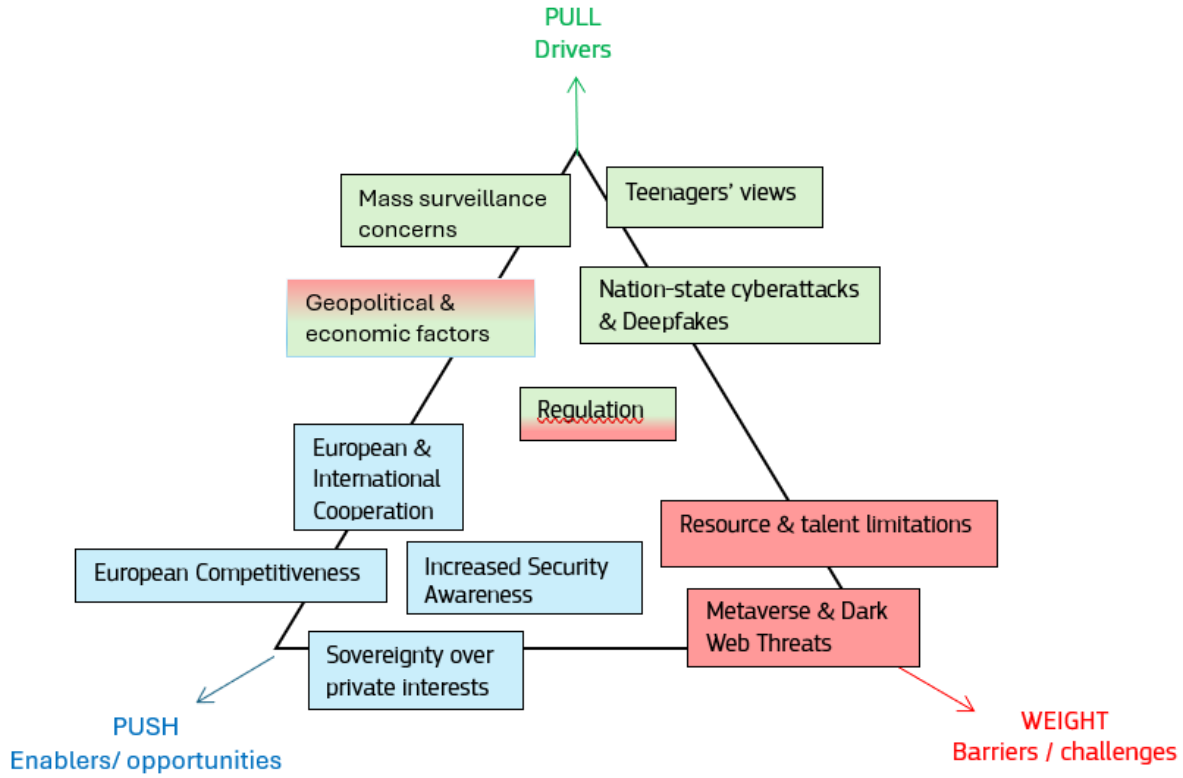
In this adapted method, assigning certain phenomena to a specific force or factor is less important. It is instead more important to discuss the impact and relevance of each phenomena for the wider scope of the exercise. The discussions during the participatory workshop were based on the initial desk research conducted by the project team, supplemented by expert suggestions. Participants also discussed additional factors that helped to paint a contextual environment characterised by both: (i) increasing challenges to personal privacy and security; and (ii) increased awareness, demand for and adoption of PETs (see Fig. 4).

Interestingly, the views of the three workshop breakout groups' converged in highlighting the importance of the following factors: (i) the impact of regulatory initiatives such as the EU AI Act and the EU's Digital Markets Act, which can act as both a driver and a hindrance; (ii) the US-China technology race; (iii) the digital economy and the US leadership in cryptocurrencies in particular, which is pulling the EU towards progress and innovation in the digital sphere; and (iv) increased awareness of security issues due to rising cyber and other threats.

The changing attitudes of younger generations towards privacy (increased awareness of the importance of privacy combined with a somewhat contradictory enthusiasm for sharing a lot of private information on social networks and other online services) may be a precursor to changes in public attitudes and behaviour. The sections below set out the overall outcomes of the three groups' discussions.

[15] PESTEL – Political, Economic, Social, Technological, Environment and Legal factors.

Figure 4. Combined results of discussions on relevant contextual factors



Source: authors

Drivers

— **Regulation.** The EU's Digital Markets Act could potentially spur incumbent platforms to adopt more privacy-preserving solutions and allow interoperability, but on the other hand it could also be a barrier as incumbents might find it very difficult to implement.

— **Geopolitical and economic factors.** The US-China tech race, the digital economy, and US leadership in cryptocurrencies are all driving the need for the EU to catch up and boost its competitiveness while remaining vigilant about citizens' rights.

— **Teenagers' perception of privacy.** The changing attitudes towards privacy among younger generations - a deeper awareness of privacy online combined with a different perception of privacy risks - may be a precursor to changes in the attitudes towards privacy of society as a whole (with the attendant changes in behaviour) that law enforcement should take into account.

— **Mass surveillance concerns.** The risks and privacy concerns associated with mass surveillance drive resistance to it, although these risks and concerns should not detract from the need to balance individual privacy with societal needs for safety, acknowledging the inherent tension between these two priorities.

— **Nation-state cyber-attacks and deepfakes.** The increase in cyber threats against nation states and the use of increasingly automatically produced deepfakes highlights the need for detection and mitigation mechanisms in this area.

Enablers

- **European collaboration.** Initiatives like data spaces (especially when PETs are included), the European Digital Decade and others, could improve secure data exchange and enable further progress in PETs.
- **International cooperation.** Greater cross-border cooperation in law enforcement, regulations on e-evidence, and initiatives such as the UN Cyber-Crime Convention help to both foster a common understanding of risks and combat associated criminal activities.
- **European competitiveness.** As noted by the Draghi report [83] on competitiveness, against the backdrop of the US and China technology race, innovations in the digital sphere are crucial for boosting European competitiveness.
- **Increased security awareness.** The current political agenda's emphasis on security, as indicated by the 2024 Niinistö report [84], and the broader wish of society for more security and safety are favourable factors for PETs.
- **Sovereignty over private interests.** Governments are increasingly seeking to stress security and sovereignty over the private corporate interests of companies, as can be seen in examples from other countries, like the Australian Assistance and Access Act[16].

Barriers

- **Legislation and geopolitical sensitivities.** In the fight against cybercrime, law enforcement and international cooperation may be hindered by geopolitical sensitivities and challenges posed by legislation (like the EU's Digital Markets Act or the EU AI Act). The diverging views of countries will also make cooperation more difficult in the area of law.
- ***Resource and talent limitations.*** Participants in the workshop questioned whether there was enough money and staff available to address challenges, taking into consideration the current understaffing in cybercrime teams as well as their issue with staff burnout. Shortages in raw materials (e.g. with chips production lagging behind) can impede progress.
- **Threats from the metaverse and dark web.** These complex and decentralised areas, primarily shaped by private entities and in some cases influenced by criminal organisations, are difficult to regulate and pose significant barriers.

Participants in the workshop also identified several other important factors, but they could not be easily identified as a single force, as these factors were highly nuanced. For example, the geo-location of data may be particularly useful for law enforcement in the future but may also pose a major privacy problem. Similarly, the impact of increased cyber hygiene or the weaponisation of AI is not clear. Legislation such as the EU's Digital Markets Act or the EU AI Act can also act as both a driver and a barrier to innovation. Overall, there is a clear tension between, on the one hand, the

[16] The Assistance and Access Act 2018 is a law enacted by the Australian government that empowers law enforcement and intelligence agencies to access encrypted communications and digital data. [98]

need for more privacy and freedom from mass surveillance, and on the other hand the need for a safer society.

5.1. Contextual factors according to the PESTEL methodology

A systemic analysis of contextual factors was carried out using the PESTEL (political, environmental, social, technological, economic, legal) methodology. The political domain, in this context, primarily refers to geopolitical factors. As legal (or regulatory) factors emerged as an important issue during the workshop discussions, the PESTEL approach was chosen as more appropriate than, for instance, a PESTEL framework (comprising political, environmental, social, technological, economic, legal)) which excludes legal/regulatory factors. The section below is based mainly on results from the workshop discussion on contextual factors with some post-workshop analysis and additional desk research conducted afterwards.

(Geo)political factors: the world in 'polycrisis'[17]

As noted by the 2024 Niinistö report [84], we are living in a more dangerous world. The intensifying competition among leading global actors using all instruments of power is further challenging the *status quo* of the rules-based international order. One of the key aspects of this rivalry is the US-China technology race, which is pivotal in shaping future global power dynamics. In this tech race, US leadership in cryptocurrencies and other digital innovations stands out as a significant strategic advantage. The ability to innovate and apply new technologies, especially in digital sectors, is now a crucial determinant of national strength. The most recent transatlantic developments in the areas of trade and other policies add even more uncertainty and ambiguity. It is not yet clear what cascading effects these developments could have on the digital technology sector. At the same time, it is not always easy to see which technologies are developing in other parts of the world. Overall, we are witnessing increasing security risks for the EU in the digital sphere. For example, the frequency and sophistication of nation-state cyber-attacks targeting critical infrastructure and exploiting vulnerabilities in global digital networks are only increasing. Deepfakes, especially those impersonating political leaders, pose an increasing threat to public trust and geopolitical stability, as they can be used to spread disinformation, manipulate public opinion or incite social unrest. A particular danger is posed by terrorist groups, which are increasingly using digital technologies for various malicious purposes, such as: (i) communication and recruitment; (ii) planning and coordinating attacks; (iii) weaponising emerging technologies (AI, drones, etc.); and (iv) using the dark web. Additionally, the workshop participants underscored the pervasive role of mass surveillance, particularly by authoritarian regimes, which makes use of advanced technologies such as AI and big data to monitor, control, and influence populations (for example via social scoring). These developments suggest a future in which digital warfare will intertwine with psychological and societal dimensions, making it harder to distinguish between physical and digital conflict zones.

Space remains another arena for both geopolitical rivalry and technological innovations. This has significant implications for privacy enhancing technologies (PETs) and security (for instance, the

[17] The term 'polycrisis' highlights interactions between crises through cascading effects; the phenomenon has five key characteristics: emergent harms, multiple causes, deep uncertainty, systemic context, and the need for new knowledge and action to address crisis interactions

growing use of drones, 6G mobile networks, interception of communication systems, etc.). The growing militarisation of space poses significant challenges to global security because of the increased risk it brings of cyber-attacks on space systems. For this reason, PETs are becoming crucial for secure data sharing and analysis in space-related applications. Participants in the workshop also noted the importance of new security threats stemming from 'mosaic' warfare[18], in which space acts as a critical enabler.

Given these trends, discussions about the need to balance security and privacy in the digital age continue to shape digital policy landscapes. European and international collaboration remains a key factor in fighting crime and increasing collaboration while ensuring safety for society. For this reason, all initiatives that can assist in the fight against digital crime are to be welcomed (these initiatives include e-evidence, cross-border access to electronic evidence [4], the UN Cyber-Crime Convention, and the creation of a G20 data space). However, the changing international order might make international cooperation for law enforcement harder. These trends also strengthen the need for Europe to increase its technological capabilities, ensure its cybersecurity, and foster innovation to retain or achieve leadership in critical technology sectors.

Economic factors: (lost) digital opportunities and rising costs/risks?

The digital economy was identified by participants in the workshop as one of the key drivers of PETs. According to the OECD Digital Economy Outlook 2024 [85], while the digital economy is no longer strictly confined to the information and communication technology (ICT) sector, this sector remains at its heart, underpinning digital innovation. Yet there is a lack of timely data on the performance of this vital sector, limiting policymakers' visibility. Some estimates suggest that the US holds about 35% of global ICT market share by sales revenues. [86]

Meanwhile, the European economy faces major challenges in competitiveness, as highlighted in the recent Draghi report [83]. The report argues that Europe largely missed out on the digital revolution led by the internet and the productivity gains it brought. In fact, the productivity gap between the EU and the US is largely explained by differences in the technology sector.

The report also noted Europe's underperformance in advanced technologies which are crucial for future growth. Currently, only 4 of the world's top 50 technology companies are European, and the EU's global position in tech is deteriorating: from 2013 to 2023, its share of global technology revenues dropped from 22% to 18%, while the US share rose from 30% to 38% [83]. To address this, the EU needs to close the innovation gap and focus on decarbonisation, competitiveness, and increasing security [83].

The workshop participants also highlighted the relevance of the European Digital Decade programme [87] as one of the enabling factors for PETs. The programme emphasises: (i) digitalising public services; (ii) investing in skills; (iii) transforming businesses through digital means; and (iv) ensuring secure and sustainable digital infrastructures (Table 2). This will help to accelerate the uptake of new technologies like AI, which remains low and sector-specific in Europe. In particular,

[18] Mosaic warfare represents the rapid and creative combination of small, cheap, flexible systems designed to conduct multi-domain manoeuvre against adversaries with precision strike capabilities that can quickly adapt to changing battlefield conditions

workshop participants emphasised the importance of advanced digital skills and the distribution of people with these skills across member-states, as well as the need for people to be more creative in the face of advances in digital technologies. It is worth noting the shortage of cybersecurity teams (and the high rates of burnout within these teams), especially due to rising cybercrime.

Table 2. Digital Decade targets for Europe 2030

Digitalisation of public services	**Skills**	**Digital transformation of businesses**	**Secure and sustainable digital infrastructures**
Key Public Services: 100% online **e-Health:** 100% of citizens have access to medical records online **Digital Identity:** 100% of citizens have access to digital ID	**ICT Specialists:** 20 million + gender convergence (i.e. 50% of these specialists should be women and 50% should be men) Basic digital skills: min. 80% of population	**Tech uptake:** 75% of EU companies using Cloud, AI, or Big Data **Innovators:** grow scale-ups & finance to double EU Unicorns **Late adopters:** more than 90% of SMEs to have reached at least a basic level of digital intensity	**Connectivity:** Gigabit for everyone **Cutting edge Semiconductors:** double EU share in global production **Data - Edge & Cloud:** 10 000 climate-neutral and highly secure edge nodes

Source: Europe's Digital Decade: digital targets for 2030

Cybercrime was one of the key topics addressed in the workshop discussions. According to market research company Cybersecurity Ventures, cybercrime is estimated to have cost the world USD 9.5 trillion in 2024. If it were a country, cybercrime would be the world's third largest economy after the US and China [88]. The 'weaponisation of AI' (including not just deepfakes but increasingly the use of AI-generated code and language) is a growing trend affecting geopolitics, economics, and society more broadly, as benign algorithms can be altered to disrupt economic and financial activities As AI-driven attacks become more common, companies need to implement autonomous response systems to defend against them. Participants in the workshop expressed concerns that companies currently rely on only a few cybersecurity vendors.

The workshop participants also discussed the emerging trend of business digital tools being used for malicious activities, including 'disinformation as a service' (DaaS). This tactic involves manipulating public opinion and disrupting organisations, and is significantly altering the cyber threat landscape. The implications of DaaS are far-reaching, extending beyond political interference to include reputational damage to organisations, often targeting high-level executives. This can have a profound impact on businesses, the economy, and ultimately, overall economic stability. Furthermore, workshop participants pointed out that the lack of economic incentives for adopting more privacy-preserving solutions is a significant concern, highlighting the need for a more comprehensive approach to addressing these emerging threats.

Social factors: changing teenagers' views as a precursor to broader changes

The workshop participants were quite unanimous in their opinions on – and drew particular attention to – the changing attitudes of young people to privacy in the digital space. Participants said that younger people have a deeper awareness of privacy online, but also have a different perception of privacy risks. This may be an indicator of broader changes in the attitudes and behaviour of society in the future. [89]

Several studies have been conducted on this issue, reporting that young adolescents' privacy behaviours, beliefs, and practices are multifaceted and complex, reflecting the trade-offs they must make between social connectedness and protecting their privacy. The behaviours of young people show a balance between protecting their privacy from corporations and potential predators, while sharing information to stay socially connected. Adolescents generally engage more in privacy-protecting behaviours related to their social interactions than they do in their interactions with corporations. Adolescents also heed warnings about online predators more strongly than risks related to corporate surveillance or their future reputation.

Research also suggests that there exists a 'privacy paradox': young people claim to be concerned about privacy, yet they release a great deal of personal information about themselves through social media. Unlike adults who seem to be concerned about online risks, adolescents share personal and sometimes intimate information on social networking sites and other online services, and are unaware of the online privacy policies of platforms. This makes them vulnerable to privacy violations and easy targets for online risks. In addition, adolescents between the ages of 13 and 17 are more likely than adults to respond favourably to online requests for data for commercial reasons [90]. Society does not have much control and influence over the views of young people so adjustments to their behaviour will be necessary in the future.

Building on their concerns for online privacy, workshop participants drew attention to the rise of immersive environments like the metaverse and how these environments add new dimensions to the challenges faced by younger generations. The metaverse, an interconnected virtual ecosystem blending Web 2.0 and Web 3.0 technologies, raises significant privacy concerns due to its reliance on extensive data collection and the real-time tracking of user behaviours, preferences, and interactions. Adolescents, who are already vulnerable to privacy violations on traditional platforms, may face even greater risks in these immersive spaces where personal, biometric, and behavioural data is intricately tied to their digital identities.

Technological factors: the importance of 'cyber hygiene' and post-quantum cryptography

Workshop participants also highlighted the need for more 'cyber hygiene' awareness in areas like: (i) supply-chain management in small and medium enterprises (SMEs); (ii) online research activities; and (iii) the digital transition in infrastructure and mobility systems. Cyber hygiene is a crucial aspect of ICT security, which involves maintaining a secure online environment by adhering to basic best practices in cybersecurity. These best practices include secure password management, avoiding suspicious links, turning on multi-factor authentication and regularly updating software [91]. Effective cyber hygiene practices can mitigate risks associated with cyber-attacks, increase the resilience of industries, and promote a safer online environment.

Cyber hygiene is not a completely novel concept, but it is an increasingly common topic of discussion in both scientific literature and business, particularly in response to the digital transformation brought about by the COVID-19 pandemic. Our increasing dependency on networked ICT in almost all industries, from transport to education, has highlighted the need for more robust daily cyber hygiene practices. However, traditional training programmes that focus on cybersecurity often lack sufficient emphasis on cyber hygiene, thereby leaving a gap that needs to be addressed for better security management.

Moreover, the application of AI to help increase cyber hygiene is still in its nascent stages, indicating the potential for further development and innovation in this field. Furthermore, understanding cyber

hygiene awareness varies according to different demographic factors such as gender, employment status, and education level, and it is critical to better understand the different cultures of cyber hygiene among different user groups. The development of tools like browser extensions that validate websites and promote safe browsing is another novel aspect of this trend. Better understanding and improving cyber hygiene practices in different cultural contexts, like in rural communities in developing countries, also offers pathways for a more secure online environment.

Another important issue raised by participants relates to quantum-resistant algorithms. Although it is still in the early stages of development, organisations must start considering post-quantum cryptography (PQC) to secure their data and systems. Organisations like the US National Institute of Standards and Technology (NIST) are already standardising post-quantum algorithms to ensure widespread adoption and interoperability. Robust frameworks are needed in this area.

Environmental factors: critical raw materials and the ICT impact on nature

During the workshop discussions, environmental factors affecting the uptake of PETs were primarily viewed as barriers, mainly due to their impact on nature. While it is challenging to accurately measure the direct impact of ICT on the environment, it is estimated that the digital sector currently accounts for up to 4% of global greenhouse gas (GHG) emissions. With rapid growth, the carbon footprint of the digital sector could rise by 60% by 2040. Although progress has recently been made in deploying a greater amount of renewable energy to offset rising electricity consumption [92], the impact of key emerging technologies, chief among them AI, is raising questions about our future energy needs. The rapid growth of AI presents significant energy challenges that have implications for global electricity consumption and environmental sustainability. Studies show that AI-related electricity consumption is projected to grow by up to 50% annually from 2023 to 2030. In addition, training large AI models can result in significant CO_2 emissions.

The increasing integration of digital technologies into other sectors of the economy further complicates the task of setting clear boundaries when evaluating the environmental footprint of the sector.

Critical raw materials (CRMs) were noted by workshop participants as another important factor to consider. This is because it is through physical devices, infrastructure and data centres that digital technologies must operate. The technology sector is becoming more 'resource-hungry', as these technologies are dependent on raw materials such as copper, gold and lithium, but also on much lesser-known metals such as indium, tantalum and gallium to manufacture the equipment that enables it to exist and develop. According to a JRC (2023) study, meeting the EU's ambitious policy goals for the twin transition and the defence/aerospace agenda will drive an unprecedented increase in strategic and raw materials demand in the run-up to 2030 and 2050 [93]. Currently, there are 34 CRMs identified in the EU, and they are mostly sourced outside the EU [94]. For certain CRMs, the EU is solely dependent on one country. For instance, China provides 100% of the EU's supply of heavy rare earth elements [95].

Legal and regulatory factors: balance between privacy and security

Current EU regulation, such as the EU's AI Act or the EU Digital Markets Act, was often identified by participants as playing an important role in the future development of PETs. However, workshop participants disagreed about the impact of this regulation. In some cases, the participants said the regulation could be considered as a driver or enabler promoting greater privacy in the digital space, while in other cases they could be considered as barriers, especially for law enforcement.

The right to privacy, recognised as a fundamental right, is addressed in both the Universal Declaration of Human Rights and the ECHR. This right is also explicitly enshrined in primary and secondary EU legislation, like the GDPR. Furthermore, the EU Digital Identity Framework Regulation [96] aims to put in place a comprehensive and secure digital identity ecosystem, including digital wallets, across the European Union, while the EU AI Act seeks to protect and enhance privacy by ensuring that AI systems are safe, respect fundamental rights, and align with the preferences for a safer society.

However, there are concerns that both: (i) non-EU countries, not to speak of malign actors, may ignore these regulations; and (ii) certain provisions of EU law could even hinder European law enforcement's understanding of technological developments abroad. For example, although the EU AI Act is expected to promote better cyber hygiene and benefit the exercise of fundamental rights, it may also restrict researchers, especially in the context of global competition, such as in the US-China tech race. For those in law enforcement, these restrictions can complicate fundamental research on how criminals might use AI, creating barriers that are exacerbated by other countries not sharing these self-imposed restrictions. The EU cannot impose its rules on non-EU countries, where differing approaches in this area may challenge the EU's understanding of their technological advancements.

On the other hand, EU initiatives like the E-Evidence Package [97] enable law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals, especially in the area of cross-border access to digital data. This ability to access digital evidence across borders has become of critical importance given the increasing criminal use of technology and the significant role that digital evidence plays in investigations, with around 85% of criminal cases now involving such data [40]. E-evidence includes emails, messaging app content, audiovisual material, and user account information, and law enforcement often encounters challenges in accessing e-evidence due to data-protection requirements, cross-border cooperation, the coexistence of multiple levels of regulation, etc.

Finally, workshop participants highlighted upcoming EU regulatory initiatives in this area, including proposed laws on child sexual abuse material (CSAM), which have ignited intense privacy debates. The legislation might require tech companies to use client-side scanning technology to scan user communications, including encrypted messages, for CSAM.

In summary, when we think about possible futures, it is obvious that we need to not only assess the technological possibilities for PET development but also look at the whole broad systemic picture of how significant political, social, economic and other factors may interact and how this will shape the future context for these possibilities.

6. Conclusions

There is a need to raise awareness of and continue promoting the adoption of (advanced) privacy enhancing technologies (PETs) as a solution to data privacy and security threats, given the increasing number of cybercrimes and broader security concerns. Due to their highly innovative nature, PETs as well as other enabling technologies tend to remain under the radar of the policy-makers. However, the development of effective regulations and strategies for data protection, emerging PETs, and other enabling technologies such as AI, requires a deeper understanding of how these technologies work.

This understanding is crucial for striking a balance between the need for security and privacy, as PETs can be used for both legitimate and malicious purposes. By gaining a better understanding of the opportunities and challenges presented by emerging PETs and related relevant key enabling technologies for law enforcement, we can harness their potential, mitigate their risks, and ultimately create a safer and more secure digital environment. This will contribute to greater public security in the future. For this purpose, better cooperation is needed between policy-makers, research institutions, service providers and law enforcement.

Further, we present some conclusions according to our research questions (see section 1). The authors acknowledge that the insights presented are based on the results of the participatory workshop and a limited number of interviews. For this reason, more in-depth research may be needed for broader findings. Therefore, the reflection points provided should be considered as provisional and incomplete.

6.1. Most promising privacy enhancing technologies

What are the most promising emerging privacy enhancing technologies for supporting Law Enforcement Agencies' operations in the future?

Based on the project results, the following PETs and key enabling technologies appear most promising for supporting law enforcement operations in the future:

- **Advanced privacy enhancing technologies**, such as fully homomorphic encryption (FHE), multi-party computation (MPC) and zero-knowledge proofs (ZKPs) enable computation on encrypted data. These technologies can be used in criminal investigations—for example, in the analysis of encrypted datasets for fraud detection—while preserving privacy and security.
- **Post-quantum technologies**, such as post-quantum cryptography (PQC) and quantum-key distribution (QKD) enable that sensitive data remains secure with the advent of quantum computers. This will also require adaptation of current digital forensic techniques.
- Technologies related **to identity protection and biometric security,** such as synthetic datasets that could be used to train predictive analytics models for crime detection without compromising the privacy of real suspects or victims.
- **Trusted execution environments** (TEEs) which provide opportunities to secure the handling of sensitive investigative data and ensure the privacy-compliant use of intelligence tools.

In addition to PETs, key enabling technologies such as AI have emerged as central to the future of law enforcement. AI could support complex investigative tasks, including revealing hidden identities,

predictive analytics, and digital forensics. In the context of preserving privacy, it is worth integrating core principles like explainable AI, machine unlearning, and privacy-preserving machine learning.

Other innovations with transformative potential include: advances in biometric security; the Internet of Behaviour (IoB), which analyses patterns from the IoT and social media to improve law enforcement strategies; drones and robotics (including the development of humanoid robots) and, for example, tiny solar-powered drones that open up new possibilities for surveillance, crisis response, and operational efficiency for law enforcement agencies; 6G networks with their integrated sensing capabilities, AI-driven network management, and satellite connectivity, which can provide richer data sources for investigations and security operations, enabling the real-time tracking and analysis of complex information.; and blockchain/ distributed ledger technology (DLT), which can serve a valuable tool for tracking and disrupting organised crime, particularly in cases where cryptocurrencies are used to launder money or finance illicit activities.

6.2. The key contextual factors

What are the key drivers, enablers and trends relevant for developing and adopting privacy enhancing technologies by law enforcement and criminal actors?

The workshop participants were unanimous in highlighting the importance of the following contextual factors, which are pulling the EU towards progress and innovation in the digital sphere: (i) the impact of regulatory initiatives such as the GDPR, the EU AI Act and the EU's Digital Markets Act; (ii) geopolitical and economic factors, such as the US-China technology race; (iii) US leadership in digital technologies; (iv) cryptocurrencies; and (v) the increased awareness of security issues in the light of rising cyber and other threats. The changing attitudes of younger generations towards privacy – a greater awareness of the concept combined with a changing understanding of risks – may be a precursor to future changes in public attitudes and behaviour.

Some factors could act as both a driver and a barrier at the same time. For example, regulatory measures such as the Digital Markets Act could potentially spur incumbent platforms to adopt more privacy-preserving solutions and allow interoperability. But, on the other hand, the Digital Markets Act could also be a barrier if incumbents find it very difficult to implement. The EU needs to catch up in digital technologies and boost its competitiveness while remaining vigilant about citizens' rights. Privacy concerns are currently driving the development and uptake of PETs. The workshop participants acknowledged the existing tension between the need to balance privacy while at the same time ensure societal security, especially in the face of increasing cyber threats against nation states. The use of deep fakes, often facilitated by automation, illustrates the need for detection and mitigation mechanisms.

Closer European and international collaboration help to both foster a common understanding of risks and combat associated criminal activities. This collaboration can be seen in initiatives such as data spaces (especially when PETs are included), regulations on e-Evidence and the UN Cyber-Crime Convention. International efforts to combat crime online are particularly necessary. However, current trends in the international arena with the world in a 'polycrisis' may hinder international cooperation and law enforcement efforts, especially in the fight against cybercrime. As was noted by participants, our efforts to regulate the digital sphere bring us many benefits, but many actors do not take our rules into consideration even though they retain access to European citizens. Areas such as the metaverse and dark web (as well as related threats), primarily shaped by private entities or in some cases influenced by criminal organisations, are difficult to regulate and pose significant barriers. Governments and law enforcement agencies may face challenges in keeping up

with developments in this area due to a shortage of resources, talent limitations, and problems of burnout in cybersecurity teams. With general levels of digital crime increasing, these are important issues to address.

6.3. Criminal threats and hindering law enforcement

What are the emerging privacy enhancing technologies and/or related technologies that could pose significant criminal threats or facilitate these threats in the future? What are the emerging PETs that could most hinder law enforcement work in the future?

Technologies are inherently value-neutral, they are tools that can be used for positive or negative purposes depending on the context and the actor's intent. In the hands of malicious actors, PETs can pose significant threats as they can be used to: (i) conceal traces of criminal and terrorist activities; and (ii) delete critical potential electronic evidence without the possibility of recovery. Generally, PETs can be abused for the purposes of: (i) secure communications in the context of planning criminal and terrorist activities; (ii) anonymising the identity of the relevant perpetrators; and (iii) encrypting potential digital evidence.

The following emerging PETs and/or related technologies that could pose significant criminal threats or hinder activities of law enforcement in the future are set out in the bullet points below.

— The increasing sophistication and accessibility of deepfake technology (as well as other synthetic content) could be used to create fake identities, manipulate digital evidence, and commit other types of cybercrime. This 'liar's dividend' will impose very high standards of evidence gathering and processing on law enforcement, complicating a significant amount of their work. As a result, agencies will need to adapt and develop new strategies to stay ahead of these emerging technologies.

— New encryption methods, such as FHE, could pose a challenge, as they allow computations to be performed on encrypted data, making it difficult for law enforcement agencies to access and analyse evidence. SMPC, which enables collaborative computation without exposing raw data, makes it harder for agencies to access evidence. Additionally, TEEs provide hardware-based security measures that could potentially conceal illicit activities from law enforcement.

— AI can be – and is already being – used by criminals to analyse and exploit large amounts of data, creating new opportunities for identity theft, phishing, and other types of cybercrime. The use of AI and ML can create sophisticated cyber-attacks, generate deepfakes, and conduct large-scale surveillance, making it harder for law enforcement agencies to track and access digital evidence.

— The emergence of quantum computing could potentially allow criminals to break current encryption methods, compromising the security of sensitive information. Law enforcement should also prepare for this, by the development and uptake of PQC to maintain the security of their systems.

— The IoB could be exploited by criminals to collect and analyse sensitive behavioural data, allowing them to refine their illicit activities and target vulnerable individuals and evade detection.

— There is an increase in the use of biometric security measures, such as facial recognition and fingerprint scanning. Vulnerabilities in these methods could be exploited by criminals to both: (i)

create fake identities and commit other types of cybercrime; and (ii) make it more difficult for law enforcement to access criminal data and communications channels. It could also potentially hinder agencies' ability to use biometric data for investigations.

— The use of DLT, such as blockchain, could be exploited by criminals to create secure and anonymous communication channels, facilitating the exchange of illicit goods and services.

— The development of secure communication protocols, such as end-to-end encrypted messaging apps, is being exploited by criminals to communicate securely and anonymously. Further advances in this technology will make it even more difficult for law enforcement to intercept and track these criminals' activities.

— 6G's enhanced capabilities, such as sensing technologies, AI-driven network management, and increased bandwidth, could be used by malicious actors to launch sophisticated cyber-attacks, generate deepfakes, and conduct large-scale surveillance. The distributed nature and mobility of data within 6G networks could make it harder to track and access digital evidence. In addition, the use of AI in 6G networks could create new attack vectors, such as manipulating AI decision-making processes to misdirect traffic or disrupt services. Additionally, 6G poses risks of tracking and profiling providing criminal opportunities.

6.4. Priorities for EU funding

What priorities could be considered for EU funding for skills and innovation in this area?

— The development of technical capabilities is a crucial aspect to consider for the EU funding prioritise. This would enable law enforcement agencies to detect, analyse, and disrupt the criminal abuse of emerging PETs. This funding could also help the development and sharing of relevant tools for the benefit of all EU law enforcement, such as via the Europol Tool Repository.

— Cybersecurity research and development, with a focus on areas such as cryptography, threat intelligence, and incident response. This will help to improve the security and resilience of law enforcement agencies' systems and networks, thereby ensuring they are better equipped to tackle the challenges posed by emerging technologies.

— Development of AI and ML expertise within law enforcement. This will enable them to effectively use these technologies for investigations, intelligence gathering, and threat assessment, ultimately strengthening their capabilities in these areas.

— Digital forensics and analytics, including by the development of tools and techniques for analysing and interpreting complex digital evidence. This is essential in today's digital landscape, where the ability to extract and analyse data from various sources is critical in aiding investigations and informing decision-making.

— Initiatives that promote interoperability and standardisation across different PETs, law enforcement agencies, and jurisdictions. This will help to ensure seamless communication and collaboration, which is vital in addressing the complexities of emerging technologies.

— Training and capacity-building programmes for law enforcement with a focus on emerging PETs, cybersecurity, AI and ML. This will ensure that law enforcement officials possess the necessary skills and knowledge to effectively address the challenges posed by these technologies. Moreover, it is essential that legislators and policy-makers working in areas

related to these topics are also upskilled, enabling them to properly legislate and regulate these technologies.

— Research into the ethical and societal implications of emerging PETs, ensuring that both their development and use align with EU values and respect human rights.

Public-private partnerships could be encouraged through EU funding, fostering collaboration between law enforcement agencies, industry, and academia to develop innovative solutions and share knowledge and expertise. This collaborative approach should address the full cycle, from fundamental research to the practical implementation of tools in the hands of law enforcement.

References

[1] U. v. d. Leyen, “Political Guidelines for the next European Commission 2024-2029,” 2024. [Online]. Available: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

[2] EUROPOL, “European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime,” Publications Office of the European Union, Luxembourg, 2025.

[3] EUROPOL, “Internet Organised Crime Threat Assessment,” Publications Office of the European Union, Luxembourg, 2025.

[4] European Commission, “E-evidence - cross-border access to electronic evidence,” [Online]. Available: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en. [Accessed 2025].

[5] European Commission, “Migration and Home Affairs,” 24 November 2024. [Online]. Available: https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en.

[6] The Royal Society, “From privacy to partnership - The role of privacy enhancing technologies in data governance and collaborative analysis,” 2023.

[7] G. Balston, M. Oswald, A. Harris and A. Janjeva, “Privacy and Intelligence - Implications of Emerging Privacy Enhancing Technologies for UK Surveillance Policy,” The Centre for Emerging Technology and Security, 2022.

[8] United Nations, “United Nations Guide on Privacy-Enhancing Technologies for Official Statistics,” New York, 2023.

[9] EUROPOL, “Europol Strategy. Delivering Security in Partnership,” 2023.

[10] European Council, “Council defines the EU’s crime-fighting priorities for the next years,” European Council, 2025. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2025/06/13/council-defines-eu-crime-fighting-priorities-for-next-years/.

[11] EUROPOL, “Innovation lab,” [Online]. Available: https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab.

[12] European Commission, “Joint Research Centre,” [Online]. Available: https://commission.europa.eu/about/departments-and-executive-agencies/joint-research-centre_en.

[13] European Commission, “EU Policy Lab - A collaborative and experimental space for innovative policymaking,” [Online]. Available: https://policy-lab.ec.europa.eu/index_en.

[14] European Commission, “Knowledge for policy - Technology Foresight,” European Commission, 2025. [Online]. Available: https://knowledge4policy.ec.europa.eu/tech-foresight_en.

[15] A. Mochan, J. Farinha, G. Bailey, L. Rodriguez and A. Polvora, “Securing the future - Horizon scanning for emerging technologies and breakthrough innovations in the field of digital and network security,” European Commission, Brussels, 2024.

[16] E. Störmer, L. Bontoux, M. Krzysztofowicz, E. Florescu, A.-K. Bock and F. Scapolo, “Foresight – Using Science and Evidence to Anticipate and Shape the Future,” *Science for Policy Handbook,* pp. 128-142, 2020.

[17] P. Rossel, “Early detection, warnings, weak signals and seeds of change: A turbulent domain of futures studies,” *Futures,* vol. 44, no. 3, pp. 229-239, 2012.

[18] B. L. van Veen and J. Roland Ortt, “Unifying weak signals definitions to improve construct understanding,” *Futures,* vol. 134, p. 102837, 2021.

[19] OECD, “Emerging privacy-enhancing technologies - Current regulatory and policy approaches,” *OECD Digital Economy Papers,* no. 351, 2023.

[20] ENISA, “Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies,” 2023.

[21] E. Curry, A. Metzger, S. Zillner, J.-C. Pazzaglia and A. G. Robles, Eds., The Elements of Big Data Value - Foundations of the Research and Innovation Ecosystem, Springer Cham, 2021.

[22] J. Domingo-Ferrer and A. Blanco-Justicia, “Privacy-Preserving Technologies,” in *The Ethics of Cybersecurity*, M. Christen, B. Gordijn and M. Loi, Eds., 2021, p. 279–297.

[23] L. Lundy-Bryan, “Privacy Enhancing Technologie - Part 2 - The Coming Age of Collaborative Computing,” 2021.

[24] Europen Commission, “What does data protection ‘by design’ and ‘by default’ mean?,” [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/rules-

business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

[25] C. Gressel, R. Overdorf, I. Hagenstedt, M. Karaboga, H. Lurtz and M. Raschke, “Privacy-Aware Eye Tracking: Challenges and Future Directions,” *IEEE Pervasive Computing,* vol. 22, no. 1, pp. 95 - 102, 2023.

[26] European Data Protection Supervisor, “Data Protection,” [Online]. Available: https://www.edps.europa.eu/data-protection/data-protection_en#:~:text=What%20is%20Privacy%3F,but%20also%20a%20social%20value..

[27] Council of Europe, “European Convention on Human Rights,” 1950. [Online]. Available: https://www.echr.coe.int/documents/d/echr/convention_ENG.

[28] European Union, “Official Journal of the European Communities,” 2000. [Online]. Available: https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[29] P. Blume, “Data Protection and Privacy - Basic Concepts in a Changing World,” *Scandinavian Studies in Law,* vol. 56, pp. 151-164, 2010.

[30] M. F. Dennedy, J. Fox and T. R. Finneran, The Privacy Engineer's Manifesto - Getting from Policy to Code to QA to Value, California: Apress Berkeley, 2014.

[31] European Commission, “What personal data is considered sensitive?,” [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.

[32] European Data Protection Supervisor, “Legislation,” [Online]. Available: https://www.edps.europa.eu/data-protection/data-protection/legislation.

[33] ENISA, “PETs controls matrix - A systematic approach for assessing online and mobile privacy tools,” 2016.

[34] Information Commissioner's Office - UK, “Privacy-enhancing technologies (PETs),” [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/#:~:text=This%20guidance%20discusses%20privacy-enhancing%20technologies%20%28PETs%29%20in%20detail.,understanding%20to%20help%20you%20apply%20P.

[35] Centre for Data Ethics and Innovation, “Privacy Enhancing Technologies Adoption Guide,” [Online]. Available: https://cdeiuk.github.io/pets-adoption-guide/.

[36] L. C. McDonnell, “Time To Tax Data? Why The Next Great Tax Frontier Could Be A Data Tax,” Forbes, 2024. [Online]. Available: https://www.forbes.com/sites/lauraclaytonmcdonnell/2024/04/17/time-to-tax-data-why-the-next-great-tax-frontier-could-be-a-data-tax/.

[37] Grand View Research, “Privacy Enhancing Technologies Market Size Report,” 2023.

[38] Information Commissioner's Office - UK, “Tackling barriers to privacy-enhancing technologies adoption - a PETs project report,” [Online]. Available: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tackling-barriers-to-privacy-enhancing-technologies-adoption/#Participant.

[39] EU Innovation Hub, “First Report on Encryption by the EU Innovation Hub for Internal Security,” Publications Office of the European Union, Luxembourg, 2024.

[40] European Council, “Better access to e-evidence to fight crime,” European Council, 2024. [Online]. Available: https://www.consilium.europa.eu/en/policies/e-evidence/.

[41] S. Penney and D. Gibbs, “Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter,” *McGill Law Journal,* vol. 63, no. 2, 2017.

[42] Y. Li, X. Yang, P. Sun, H. Qi and S. Lyu, “Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics,” in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Seattle, WA, USA, 2020.

[43] D. Coccomini, N. Messina, C. Gennaro and F. Falchi, “Combining EfficientNet and Vision Transformers for Video Deepfake Detection,” in *Image Analysis and Processing – ICIAP 2022*, Lecce, Italy, 2022.

[44] S. R. Ahmed, E. Sonuç, M. R. Ahmed and A. D. Duru, “Analysis Survey on Deepfake detection and Recognition with Convolutional Neural Networks,” in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2022.

[45] Y. Xu, K. Raja, L. Verdoliva and M. Pedersen, “Learning Pairwise Interaction for Generalizable DeepFake Detection,” in *2023 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW)*, Waikoloa, HI, USA, 2023.

[46] R. Hossain, “Decentralized VPN Services: The Future of Data Privacy Protection,” Linkedin, 2024. [Online]. Available: https://www.linkedin.com/pulse/decentralized-vpn-services-future-data-privacy-robiul-hossain-ioe7c/. [Accessed 21 11 2024].

[47] S. Chauhan and N. K. Panda, “Online Anonymity,” *Hacking Web Intelligence,* pp. 147-168, 2015.

[48] J. Wallen, “This new fully encrypted messenger app is serious about privacy,” ZDNET, 2024. [Online]. Available: https://www.zdnet.com/article/this-new-fully-encrypted-messenger-app-is-serious-about-privacy/. [Accessed 21 11 2024].

[49] D. Spooner, “What is the Internet of Behaviour? A Comprehensive Guide,” Scrums.com, 2024. [Online]. Available: https://www.scrums.com/blog/what-is-the-internet-of-behaviour-a-comprehensive-guide. [Accessed 21 11 2024].

[50] S. Midha, “The Future of Biometric Security: Beyond Passwords,” Medium, 2024. [Online]. Available: https://medium.com/@midhashivansh/the-future-of-biometric-security-beyond-passwords-4b0ddd8f4a23. [Accessed 21 11 2024].

[51] EUROPOL, “Biometric vulnerabilities - Ensuring future law enforcement preparedness,” Publications Office of the European Union, Luxembourg, 2025.

[52] P. Mohassel and Y. Zhang, “SecureML: A System for Scalable Privacy-Preserving Machine Learning,” in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2027.

[53] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal and K. Seth, “Practical Secure Aggregation for Privacy-Preserving Machine Learning,” in *2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, Texas, USA, 2017.

[54] Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang and H. Qi, “Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning,” in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, Paris, France, 2019.

[55] H. Lycklama, L. Burkhalter, A. Viand, N. Küchler and A. Hithnawi, “RoFL: Robustness of Secure Federated Learning,” in *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023.

[56] D. Fox, “This tiny solar-powered flyer weighs less than a paper plane,” nature, 2024. [Online]. Available: https://www.nature.com/articles/d41586-024-02316-6. [Accessed 25 11 2024].

[57] W. Shen, J. Peng, R. Ma, J. Wu, J. Li, Z. Liu, J. Leng, X. Yan and M. Qi, “Sunlight-powered sustained flight of an ultralight micro aerial vehicle,” *Nature,* vol. 631, p. 537–543, 2024.

[58] M. Sparkes, “Tiny solar-powered drones could stay in the air forever,” New Scientist, 2024. [Online]. Available: https://www.newscientist.com/article/2439277-tiny-solar-powered-drones-could-stay-in-the-air-forever/. [Accessed 25 11 2024].

[59] P. Gohel, P. Singh and M. Mohanty, “Explainable AI: current status and future directions,” *aRxIV,* 2021.

[60] Y. Cao and J. Yang, "Towards Making Systems Forget with Machine Unlearning," in *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, USA, 2015.

[61] M. Chen, Z. Zhang, T. Wang, M. Backes, M. Humbert and Y. Zhang, "When Machine Unlearning Jeopardizes Privacy," in *2021 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2021.

[62] Y. Liu, M. Fan, C. Chen, X. Liu, Z. Ma and L. Wang, "Backdoor Defense with Machine Unlearning," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, London, United Kingdom, 2022.

[63] H. Zhang, T. Nakamura, T. Isohara and K. Sakurai, "A Review on Machine Unlearning," *SN Computer Science,* vol. 4, p. 337, 2023.

[64] P. W. Grimm, M. R. Grossman and Gordon V. Cormack, "Artificial Intelligence as Evidence," *Northwestern journal of technology and intellectual property,* vol. 19, no. 1, 2021.

[65] EuropHPC Joint Undertaking, "The 'AI Factories' Amendment to the EuroHPC JU Regulation Enters Into Force," EuropHPC Joint Undertaking, 2024. [Online]. Available: https://eurohpc-ju.europa.eu/ai-factories-amendment-eurohpc-ju-regulation-enters-force-2024-07-09_en. [Accessed 25 11 2024].

[66] European Data Protection Supervisior, "Machine unlearning," European Data Protection Supervisior, 2025. [Online]. Available: https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/machine-unlearning_en.

[67] M. Kianpour and S.-F. Wen, "Timing Attacks on Machine Learning: State of the Art," in *2019 Intelligent Systems Conference (IntelliSys)*, London, United Kingdom, 2019.

[68] Y. Zhang, C. Yang, E. Y. Fu, Q. Jiang, C. Yan, S.-Y. Chau, G. Ngai, H.-V. Leong, X. Luo and W. Xu, "Understanding Impacts of Electromagnetic Signal Injection Attacks on Object Detection," *ArXiv,* 2024.

[69] R. S. S. Kumar, M. Nyström, J. Lambert, A. Marshall, M. Goertzel and A. Comissoneru, "Adversarial Machine Learning-Industry Perspectives," in *IEEE Symposium on Security and Privacy Workshops (SPW)*, 2020, 2020.

[70] I. Goodfellow, P. McDaniel and N. Papernot, "Making machine learning robust against adversarial inputs," *Communications of the ACM,* vol. 61, no. 7, pp. 56-66, 2018.

[71] I. Puddu, D. Lain, M. Schneider, E. Tretiakova, S. Matetic and S. Capkun, "TEEvil: Identity Lease via Trusted Execution Environments," *ArXiv,* 2019.

[72] X. Li, B. Zhao, G. Yang, T. Xiang, J. Weng and R. H. Deng, “A Survey of Secure Computation Using Trusted Execution Environments,” *ArXiv,* 2023.

[73] L. d’Aliberti, E. Gronberg and J. Kovba, “Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems,” *ArXiv,* 2024.

[74] “About the Confidential Computing Consortium,” The Linux Foundation, 2023. [Online]. Available: https://confidentialcomputing.io/about/. [Accessed 25 11 2024].

[75] EXFILES project, “TEE Security Study,” EXFILES project, 2023. [Online]. Available: https://exfiles.eu/wp-content/uploads/2022/07/EXFILES-D3.1-TEE-security-study-PU-M06.pdf. [Accessed 25 11 2024].

[76] M. Urwin, “Top 24 Humanoid Robots in Use Right Now,” Built In, 2024. [Online]. Available: https://builtin.com/robotics/humanoid-robots. [Accessed 25 11 2024].

[77] A. Chatzimichali, R. Harrison and D. Chrysostomou, “Toward privacy-sensitive human–robot interaction: Privacy terms and human–data interaction in the personal robot era,” *Paladyn, Journal of Behavioral Robotics,,* vol. 12, no. 1, pp. 160-174, 2020.

[78] B. C. Kok and H. Soh, “Trust in Robots: Challenges and Opportunities,” *Service and Interactive Robotics,* vol. 1, pp. 297-309, 2020.

[79] M. Simmler, “Responsibility gap or responsibility shift? The attribution ofcriminal responsibility in human–machine interaction,” *Information, Communication & Society,* vol. 27, no. 6, p. 1142–1162, 2024.

[80] The White House, “Executive Order on Strengthening and Promoting Innovation in the Nation’s Cybersecurity,” 16 01 2025. [Online]. Available: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/.

[81] Q. H. Abbasi, M. Weides, C. Li and M. A. Imran, “Dive into the Quantum Realm: Promise of Quantum Communication and What's Next!,” 2024. [Online]. Available: https://www.comsoc.org/publications/ctn/dive-quantum-realm-promise-quantum-communication-and-whats-next.

[82] S. Inayatullah, “The Futures Triangle: Origins and Iterations,” *World Futures Review,* vol. 15, no. 2-4, pp. 112-121, 2023.

[83] European Commission, “The future of European competitiveness: Report by Mario Draghi,” European Commission , 2024. [Online]. Available: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

[84] European Commission, “Safer together: A path towards a fully prepared Union,” [Online]. Available: https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en.

[85] OECD, “OECD Digital Economy Outlook 2024 (Volume 1) - Embracing the Technology Frontier,” OECD Publishing, Paris, 2024.

[86] Cognitive Market Research, “ICT Investment Market Report 2025 (Global Edition),” 2025.

[87] European Union, “Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030,” European Union, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dec/2022/2481/oj.

[88] S. Morgan, “Cybercrime To Cost The World $9.5 trillion USD annually in 2024,” Cybercrime Magazine, 2023. [Online]. Available: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

[89] B. T. E. I. L. D. L. Giovanni Vespoli, “The concept of privacy in the digital world according to teenagers,” 2024.

[90] S. Barth and M. D. d. Jong, “The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review,” *Telematics and Informatics,* vol. 34, no. 7, pp. 1038-1058, 2017.

[91] America's Cyber Defence Agency, “Cybersecurity Best Practices,” [Online]. Available: https://www.cisa.gov/topics/cybersecurity-best-practices#:~:text=Using%20strong%20passwords%2C%20updating%20your,drastically%20improve%20your%20online%20safety..

[92] Ericsson, “Ericsson Mobility Report,” Ericsson, 2024.

[93] C. Samuel, B. Silvia, B. Darina, A. D. Patricia, C. Alessandro, G. Konstantinos, G. Milan, I. Anca, K. Teodor, L. Cynthia, L. Lorcan, M. Giorgia, M. Thibaut, P. A. Angel and S. Julian, “Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU – A foresight study,” 2023.

[94] European Commission, “Critical Raw Materials Act,” [Online]. Available: https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en.

[95] European Council, “An EU critical raw materials act for the future of EU supply chains,” European Council, 2024. [Online]. Available: https://www.consilium.europa.eu/en/infographics/critical-raw-materials/.

[96] European Commission, “European Digital Identity (EUDI) Regulation,” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.

[97] European Union, “Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following..,” 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng.

[98] Australian Government - Department of Home Affairs, “The Assistance and Access Act 2018,” Australian Government - Department of Home Affairs, [Online]. Available: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption.

List of abbreviations and definitions

Abbreviations	Definitions
2PC	Two-Phase Commit
6G	The sixth generation of cellular network technology
AI	Artificial intelligence
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AR	Augmented reality
BCI	Brain-computer interfaces
CCC	Confidential Computing Consortium
CCPA	California Consumer Privacy Act of 2018
CEO	Chief Executive Officer
CNNs	Convolutional neural networks
CO_2	Carbon dioxide
CRM	Critical raw materials
CSAM	Child sexual abuse material
CSS	Client-side scanning
DaaS	Desktop as a Service or Data as a Service
Dapps	Decentralised Applications
DLT	Distributed ledger technology
EC	Encrypted computing

Abbreviations	Definitions
ECFR	European Charter of Fundamental Rights
ECHR	European Convention of Human Rights
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Union Agency for Cybersecurity
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FHE	Fully Homomorphic Encryption
FHME	Fully Homomorphic Message Encryption
FL	Federated learning
G20	Group of Twenty, a premier intergovernmental forum for international economic cooperation
GAN	Generative Adversarial Network
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
GHG	Global greenhouse gas
HE	Homomorphic encryption
HLG	High Level Group on access to data for law enforcement
HPC	High-Performance Computing
ICT	Information and communication technology

Abbreviations	Definitions
IoB	Internet of behaviour
IOCTA	Internet Organised Crime Threat Assessment by Europol
IoT	Internet of things
IP	Internet protocol
JRC	European Commission's Joint Research Centre
LEA(s)	Law enforcement agency(ies)
LEO	Low-earth-orbit Satellites
LLMs	Large language models
ML	Machine learning
MPC	Multi-party computation
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology of the United States
OECD	Organisation for Economic Cooperation and Development
PESTEL	Political, economic, social, technological, environmental, legal
PETs	Privacy enhancing technologies
PQC	Post-quantum cryptography
QKD	Quantum key distribution
RAN	Radio Access Network
SME	Small and Medium-sized Enterprise

Abbreviations	Definitions
SMPC	Secure multi-party computation
TEEs	Trusted execution environments
TOR	The Onion Router
TRL	Technology readiness level
UAV	Unmanned Aerial Vehicle
UK ICO	Information Commissioner's Office of the United Kingdom
UN	United Nations
US	United States of America
USD	United States dollar
VPN	Virtual private network
VR	Virtual reality
XAI	Explainable AI
ZKP	Zero-knowledge proofs

List of figures

List of tables

Annexes

Annex 1. Document sent to participants in advance to the workshop containing signals related with technologies and innovations, as well as with contextual factors

Instructions for the workshop and preparatory material

This document lists and summarizes signals on Privacy Enhancement Technologies (PETs) gathered for the upcoming horizon scanning workshop, scheduled for November 13, which you are invited to attend.

Horizon scanning is a foresight methodology aimed at the early identification of developments or events that are not yet widely on the radar of most experts, decision-makers, or the general public. It seeks future developments that remain on the fringes of current thinking and planning. In this exercise, we focus on novel ideas and unconventional interactions.

The signals in this document fall into two categories:

- A - technologies and innovations (solutions) in the area of privacy enhancement.
- B - contextual factors (drivers, enablers and barriers) relevant to the development and adoption of these technologies.

Various sources were utilized for this process, including reports, scientific articles, news items, patents, EU-funded projects, and conference proceedings. Some weak signals were proposed by experts invited to this exercise, while others were sourced directly by the project team through those kind of sources or via data and text mining techniques (marked as "TIM" in the source field).

The workshop will focus on emerging PETs that could be significant for the future activities of Europol and law enforcement agencies (LEAs). Consequently, the initial list of over 200 signals was reviewed and shortened based on the following research questions:

- What is the level of novelty of the technology?
- Which are the most promising emerging PETs for investigative support/operation of LEAs in future?
- Which techs could pose or facilitate major criminal threats/ inhibit the work of LEAs in future?

The contextual factors (organised through the STEEP framework dimensions) were selected based on their potential impact on PET's development and adoption.

The final list of signals is organized in twelve sub-clusters (see the table of contents on the next page).

Your role is essential in this exercise and includes some preparatory tasks for the workshop. To help achieve the workshop's goals, we invite you to follow these instructions:

- **Review the following pages. Scan through the list of signals. Consider which items seem most relevant to the research questions outlined above and whether there are any additional topics you'd like to discuss.**
- **View each item as raw material that you can combine with others to strengthen the signals. Think about possible connections and interrelations between items.**
- **If time is limited, simply familiarising yourself with the titles and technologies behind the signals will serve as useful preparation.**

Contents

Cluster A – Technologies and innovations

The signals related to technologies and innovations have been sub-clustered into six groups based on the types of technologies and the functionalities or capabilities they enable:

- Subcluster A1 - Distributed ledger technologies
- Subcluster A2 – Quantum and post-quantum
- Subcluster A3 – Internet of things and edge computing
- Subcluster A4 – Identity and deepfakes
- Subcluster A5 – Internet, browsing and VPNs
- Subcluster A6 – Encryption

Subcluster A1- Distributed ledger technologies

List of Signals

- 28 | After all the hype, blockchain supported cybersecurity and AI could be the way
- 39 | Quantum-resistant ledgers
- 47 | How Blockchains Can Help Solve AI's Deepfake Problem
- 113 | Blockchain integration into biometric domain
- 127 | Attribute based searchable encryption
- 129 | Blockchain 4 SAGIN
- 131 | Blockchain for secure cloud computing
- 132 | Blockchain interoperability
- 143 | Dual blockchain
- 160 | Quantum blockchain
- 162 | Redactable blockchain
- 164 | Secure decentralized finance
- 166 | Self sovereign identity

NUMBER | TITLE
28 | After all the hype, blockchain supported cybersecurity and AI could be the way
SUMMARY DESCRIPTION
Organizations are increasingly focusing on environmental, social, and governance (ESG) efforts and diversity, equity, and inclusion (DEI) commitments, alongside traditional business objectives. Blockchain technology is not a novelty. But after all the hype and speculation around crypto currencies and non-fungible tokens, it's emerging again as a key tool in enhancing digital trust, a crucial aspect in this shift. Its transparency and immutability can provide insights into the data used by AI, enhancing data integrity and security, and offering an audit trail. This technology also promises improved cybersecurity through decentralized architectures, which can reduce sensitive data storage by third parties and mitigate cyber risks. Blockchain enables trustless business models, addressing data credibility issues and building confidence among employees, customers, and industries. Amidst growing skepticism about digital information, decentralized, trustless systems suggest a collective approach to establishing trust and verifying authenticity, positioning society to rely less on individual arbitrators and more on collaborative verification.
SOURCE
Project team Tech Trends 2023 https://www2.deloitte.com/content/dam/insights/articles/us175897_tech-trends-2023/DI_tech-trends-2023.pdf

NUMBER | TITLE
39 | Quantum-resistant ledgers
SUMMARY DESCRIPTION
Distributed ledger technologies have encryption protocols but with the onset of quantum computing the need to implement post-quantum encryption will become crucial. This is what is being built today to secure against cryptographic threats especailly related to digital money.
SOURCE
Project team Science and Technology trends 2023 https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

NUMBER | TITLE

47 | How Blockchains Can Help Solve AI's Deepfake Problem

SUMMARY DESCRIPTION

AI-generated content creates a huge online disinformation threat. Blockchain can help verify and authenticate that what is being said is true. Harvard experts already predict that more than 90% of content online will be AI-generated in the future. To protect against threats such as deepfakes, it's crucial we get ahead of the issue and implement innovative solutions.
Public blockchains, collectively owned and operated by users, offer promising features like network security, transparency, and decentralization which can help against the issues deepfakes present.

SOURCE

Project team
CoinDesk
https://www.coindesk.com/opinion/2024/05/22/how-blockchains-can-help-solve-ais-deepfake-problem/

NUMBER | TITLE

113 | Blockchain integration into biometric domain

SUMMARY DESCRIPTION

The insecurities of centralized data storage have prompted the exploration of blockchain technology in the biometric domain. Blockchain's immutable ledger is being considered for storing encrypted biometric data, enhancing security and giving control back to the individual. Companies like Hyland Credentials and Bext Holdings are pioneering blockchain solutions that promise to revolutionize how facial data is stored and used, fostering trust in systems that handle personal identities.

SOURCE

Project team
The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch
https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/;
https://arxiv.org/pdf/2003.09262; https://arxiv.org/pdf/2302.10883

NUMBER | TITLE

127 | Attribute based searchable encryption

SUMMARY DESCRIPTION

Attribute-based searchable encryption (ABSE) is a sophisticated technology used to enhance the privacy and security of data shared across platforms, such as cloud services or blockchain networks. It allows fine-grained access control over encrypted data, enabling only authorized users to search and retrieve the data they require without compromising the overall data security. ABSE is particularly important in fields where sensitive information, such as medical records or personal health data, needs to be shared securely and efficiently. It is also applicable in other domains such as Industrial Internet of Things, vehicular networks, and cloud-assisted healthcare systems. This technology allows data storage in a distributed system, eliminating a single point of failure, and enables verification of data authenticity, ensuring data integrity and nonrepudiation. The novelty of the ABSE lies in its combination of data encryption, fine-grained access control, and efficient data searchability. Traditional encryption methods either secure data or allow for its searchable storage, but seldom both. ABSE also introduces the concept of attribute-based access, enabling more nuanced and flexible access control compared to the all-or-nothing approach of traditional methods. Furthermore, by integrating ABSE with blockchain technology, it decentralizes the data management, making it tamper-proof and verifiable. It also reduces the computational load on the user side by distributing the load across the network. Importantly, recent advancements have focused on addressing the challenges of computational overhead and storage efficiency, making ABSE more practical for devices with limited resources and storage capacity.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/MDM.2013.94 ; http://doi.org/10.1109/ICMCCE48743.2019.00188 ;
http://doi.org/10.1109/JIOT.2021.3063846 ; http://doi.org/10.1109/JAS.2021.1004003 ;
http://doi.org/10.1109/TCC.2021.3090519 ; http://doi.org/10.1109/ICC42927.2021.950096

NUMBER | TITLE

129 | Blockchain 4 SAGIN

SUMMARY DESCRIPTION

Blockchain 4 SAGIN is a technology that combines blockchain with Space-Air-Ground Integrated Networks (SAGIN) to enhance security and efficiency in a variety of applications, particularly in areas like Intelligent Transportation Systems (ITSs), Internet of Things (IoT), and vehicular ad-hoc networks (VANET). By integrating space and air nodes into the network, SAGIN can offer comprehensive traffic information and minimize transmission delay. Blockchain, with its decentralization and immutability features, is used to address security issues such as identity authentication, privacy protection, and data security. The technology uses a Hashchain-based identity verification scheme, Kafka algorithm for data backup, and tensor computing for a truthful incentive mechanism. The blockchain also assists in dynamic spectrum management, resource sharing, traffic offloading, and mobility management, among other tasks. The novelty of Blockchain 4 SAGIN lies in the integration of blockchain technology with SAGIN to address security issues in a comprehensive and efficient manner. The collaborative blockchain architecture proposed for SAGIN is new; each segment of SAGIN (space, air, and ground) maintains a specially designed blockchain, while inter-segment cooperation is enabled through blockchain collaboration. This innovative framework significantly improves upon existing technologies by ensuring security, reducing latency, and maximizing social welfare in a highly dynamic and heterogeneous network environment. The technology also introduces an incentive-based system to encourage participation and collaboration, and employs advanced algorithms like the Kafka algorithm and tensor computing to enhance performance and security.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/ICC.2019.8761821 ; http://doi.org/10.1109/SERVICES48979.2020.00060 ; http://doi.org/10.1109/MWC.001.2000134 ; http://doi.org/10.1109/JIOT.2021.3064357 ; http://doi.org/10.1109/COMST.2021.3131711 ; http://doi.org/10.1109/TITS.2022.31

NUMBER | TITLE

131 | Blockchain for secure cloud computing

SUMMARY DESCRIPTION

Blockchain for secure cloud computing is a technology that integrates the decentralized and tamper-proof nature of blockchain with cloud computing to enhance data security. It provides a robust solution to data integrity threats in cloud services by using a distributed network of cloud service providers (CSPs) which rely on Byzantine Fault Tolerance consensus. After computations, CSPs generate a master hash value for their database, which is stored in blockchain networks like Bitcoin or Ethereum for verification. This approach ensures data immutability, reducing the risk of data manipulation. Blockchain also enables a Controlled Access Mechanism and keeps a log of all operations on the data, which can be accessed by the owner anytime. Potential applications include IoT security, securing sensor networks, cyber security, and even criminal investigations. The novelty of integrating blockchain for secure cloud computing lies in its ability to overcome traditional cloud computing vulnerabilities, such as data manipulation, by decentralizing authority and ensuring data immutability. Unlike traditional systems where the CSP has ultimate control over data, this technology distributes the authority, reducing the risk of a single point of failure. It also provides a verifiable record of all operations on the data, enhancing transparency and trust. The use of public cryptocurrency networks for storing master hash values is a unique approach that reduces client financial costs and improves online performance. This technology also opens up new research opportunities in enhancing privacy and security in various fields such as IoT, sensor networks, and cyber security.

SOURCE

TIM
TIM analytics
http://doi.org/10.3390/sym9080164 ; http://doi.org/10.1109/ICSCAN.2018.8541258 ; http://doi.org/10.23919/ICACT48636.2020.9061435 ; http://doi.org/10.1016/j.matpr.2020.08.519 ; http://doi.org/10.1109/ACCESS.2021.3077123 ; http://doi.org/10.1007/978-3-030-5

NUMBER | TITLE

132 | Blockchain interoperability

SUMMARY DESCRIPTION

Blockchain interoperability is a technology that enables communication and data sharing across different blockchain networks and platforms. It addresses the challenge of data and information silos that exist due to the lack of interoperability in current blockchain networks. It can be implemented using frameworks like Blockchain Agnostic Interoperability Framework (BAILIF) or through the use of protocols such as the burn-to-claim or Inter Blockchain Communication (IBC) protocol. This technology adheres to the core principles of blockchain, such as decentralization, transparency, and trust. It has potential applications in various fields like energy trading, pharmaceutical drug supply chain management, and healthcare, where it can enable seamless data sharing, foster trustworthy relationships among stakeholders, and facilitate inter-microgrid transactions. The novelty of blockchain interoperability lies in its ability to overcome the limitations of existing blockchain networks that are typically isolated and heterogeneous, thereby creating disconnected value islands. This technology provides a solution to these issues by enabling blockchain interconnection, which improves interoperability and scalability. It also offers a solution to the challenge of guaranteeing the properties of ACID (Atomicity, Consistency, Isolation, Durability) across diverse blockchain systems. The development of frameworks and protocols for blockchain interoperability has also opened up new areas of research, with studies focusing on public connectors, blockchain of blockchains, and hybrid connectors. This technology is paving the way for a paradigm shift from closed blockchains to an open system where devices and users can interact with each other across blockchain boundaries.

SOURCE

TIM
TIM analytics
http://doi.org/10.1007/978-3-030-30429-4_1 ; http://doi.org/10.1109/ACCESS.2020.2999468 ; http://doi.org/10.1109/Blockchain50366.2020.00032 ; http://doi.org/10.1145/3471140 ; http://doi.org/10.1145/3582882 ; http://doi.org/10.1109/ISCON57294.2023.10112196

NUMBER | TITLE

143 | Dual blockchain

SUMMARY DESCRIPTION

Dual blockchain technology offers a solution for scalability and storage issues associated with conventional blockchain systems. By employing two interlinked chains, this approach increases the throughput of transactions and reduces storage dependencies. The dual-blockchain system uses a decentralized storage system such as IPFS to increase throughput and reduce storage liabilities. One chain handles the primary data, while the other stores references or additional information related to the first. This technology finds potential applications in various fields, including Internet of Things (IoT) information and reputation management, smart grid intelligent pricing systems, vehicular ad hoc networks (VANETs), agricultural data protection, electronic medical record (EMR) sharing, secure and anonymous data aggregation for fog-enabled smart grid, trust management in cloud computing, and distributed data management in large-scale Industrial Internet of Things (IIoT) networks. The novelty of dual blockchain technology lies in its potential to address the scalability issue inherent in single blockchain systems. By splitting the data between two chains, it can handle a significantly higher volume of transactions while maintaining security and reducing storage dependencies. Furthermore, the use of a decentralized storage system eliminates the need for every node in the network to store all of the transaction data, further increasing efficiency. Different consensus algorithms can be used for each chain, adding an additional layer of security. The technology also allows for fine-grained data aggregation and conditional privacy, which is not possible with traditional blockchain systems. This technology offers potential for numerous applications, from IoT to healthcare, demonstrating its versatility and adaptability.

SOURCE

TIM
TIM analytics
http://doi.org/10.1016/j.eng.2020.06.018 ; http://doi.org/10.1016/j.future.2020.12.007 ; http://doi.org/10.1016/j.cose.2021.102189 ; http://doi.org/10.1109/ICREST51555.2021.9331254 ; http://doi.org/10.1186/s13677-021-00247-5 ; http://doi.org/10.1109/WF-Io

NUMBER | TITLE

160 | Quantum blockchain

SUMMARY DESCRIPTION

Quantum blockchain leverages quantum computing and cryptographic principles to create a secure and efficient system for data management and transaction verification. It introduces quantum-resistant algorithms to ensure the integrity of digital signatures and encryption, effectively countering threats from quantum computers running Shor's and Grover's algorithms. Quantum blockchain incorporates concepts like quantum entropy, post-quantum key pairs, and quantum signatures to ensure secure information exchange and transaction verification. It also employs quantum detectable Byzantine agreement (DB to achieve data consensus and unconditionally secure protocols, enhancing the system's reliability and integrity. Applications of quantum blockchain are wide-ranging and include areas like smart cities, edge computing, online voting systems, and the IoT. The novelty in quantum blockchain technology lies in its ability to provide quantum resistance to existing blockchain networks. Compared to traditional blockchain protocols, which are vulnerable to quantum computing attacks, quantum blockchain offers increased security, scalability, and transparency. It uses quantum-resistant algorithms that can withstand attacks from quantum computers, making it a significant advancement in the field of security. Unlike conventional blockchains, quantum blockchains can harness quantum entropy to generate post-quantum key pairs, establish secure connections, and validate transactions using quantum signatures. Furthermore, it leverages the nonlocality of GHZ states to detect node honesty, providing improved scalability and practicality. This technology is thus a game-changer, offering a new level of security and efficiency in data management and consensus-building, especially in the era of quantum computing.

SOURCE

TIM
TIM analytics
http://doi.org/10.1016/bs.adcom.2018.03.003 ; http://doi.org/10.1109/ACCESS.2020.2968985 ; http://doi.org/10.1016/j.ipm.2021.102549 ; http://doi.org/10.1109/ICPC2T53885.2022.9776966 ; http://doi.org/10.1016/j.ins.2023.03.134 ; http://doi.org/10.1109/ISDFS

NUMBER | TITLE

162 | Redactable blockchain

SUMMARY DESCRIPTION

Redactable blockchain is an emerging technology that allows for the controlled modification of blockchain data. Unlike traditional blockchains, which are immutable once an object has been registered, redactable blockchains introduced the concept of policy-based chameleon hash (PCH) that permits the alteration of a blockchain object under specific policies. This technology offers a solution to issues such as the abuse of blockchain storage and legal obligations. It enables an individual with the right privileges to revise the blockchain without violating the overall integrity of the system. Potential applications are vast, including in the fields of data management, medical blockchain, and secure federated learning in Industrial Internet of Things (IIoT) settings. The novelty of redactable blockchain lies in its capability to break the traditional immutability of the blockchain in a controlled manner. This technology introduces the concept of blackbox accountability, which allows for the identification of responsible parties in case of misuse. It also reduces the reliance on fully trusted central authorities by allowing multiple authorities to issue rewriting privileges, thus decreasing vulnerability to various attacks. However, despite its innovative approach, this technology still faces challenges, including potential unscalabilities in large-scale implementations, and the need for stronger security and ideal scalability.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/EuroSP.2017.37 ; http://doi.org/10.1109/SP.2019.00039 ; http://doi.org/10.1145/3433210.3453091 ; http://doi.org/10.1007/978-3-662-64331-0_2 ; http://doi.org/10.1109/TIFS.2022.3156808 ; http://doi.org/10.1109/JIOT.2022.3162499 ; http

NUMBER | TITLE

164 | Secure decentralized finance

SUMMARY DESCRIPTION

Secure decentralized finance (DeFi) is a blockchain-based technology that allows financial transactions without the need for intermediaries, like banks. It is governed by Decentralized Autonomous Organizations (DAOs) via governance protocols, with governance tokens granting users voting rights. However, these tokens are often misused, leading to security vulnerabilities. DeFi platforms also face attacks, often causing significant financial losses. To address these, frameworks like the Clockwork Finance Framework (CFF) have been developed for formal verification and economic security analysis of DeFi smart contracts. Other strategies include stress-testing lending protocols to prevent financial meltdowns and developing mechanisms to detect profitable transactions across DeFi platforms. Despite the potential risks, this technology can facilitate a peer-to-peer financial paradigm and foster new developments in digital asset trading platforms. The novelty of secure DeFi lies in its decentralized structure, transparent transactions, and use of blockchain technology. Traditional financial systems are centralized, with intermediaries controlling transactions. In contrast, DeFi eliminates intermediaries and allows direct transactions between parties. However, this technology brings new challenges, such as the misuse of governance tokens and the vulnerability to attacks. The development of formal verification frameworks like the CFF and mechanisms for detecting profitable transactions represent innovative solutions exclusive to DeFi. Furthermore, the use of blockchain technology and the possibility of creating DeFi platforms that can autonomously manage financial transactions is a significant departure from established financial systems.

SOURCE

TIM

TIM analytics

http://doi.org/10.1109/CVCBT50464.2020.00005 ; http://doi.org/10.1109/SP40001.2021.00113 ; http://doi.org/10.1145/3491051 ; http://doi.org/10.1109/SP46214.2022.9833734 ; http://doi.org/10.1145/3548606.3559342 ; http://doi.org/10.1145/3570639 ; http://doi.

NUMBER | TITLE

166 | Self sovereign identity

SUMMARY DESCRIPTION

Self Sovereign Identity (SSI) is an emerging technology that allows individuals to control, access, and share their personal data. It is a decentralized digital identification system that is often linked with blockchain or Distributed Ledger Technology (DLT). SSI is based on the principle of granting individuals the right to self-manage their data, which is shared with services. It is user-centric and privacy-friendly, providing a more secure alternative to traditional user authentication processes like username and password, which are notorious for security breaches. Potential applications of SSI span across various sectors, including healthcare data-sharing, vehicular networks, smart cities, web services, and border politics and migration management. For instance, in healthcare, SSI can help reconcile patient data across various providers, while in vehicular networks, it can ensure confidentiality, authentication, and integrity of vehicle users' identity and their data. The novelty of SSI lies in its decentralized and user-centric approach to identity management, which contrasts with traditional centralized systems. The conventional systems are not only susceptible to security breaches but also limit user controls over their data. SSI, on the other hand, empowers individuals with control and ownership of their data, enhancing privacy and security. By leveraging DLT or blockchain technology, SSI offers a transparent, tamper-proof, and traceable system, which is particularly advantageous for application domains that demand high data integrity and security. Furthermore, SSI is adaptable to a wide range of applications, from smart cities to vehicular networks, indicating its versatility and potential for widespread adoption. Despite its promising prospects, SSI is still an embryonic technology with challenges to overcome, such as the need for a systematic proof system for IoT applications and the exploration of its full potential for web services.

SOURCE

TIM

TIM analytics

http://doi.org/10.1016/j.giq.2020.101493 ; http://doi.org/10.1080/14650045.2020.1823836 ; http://doi.org/10.1109/JIOT.2022.3145089 ; http://doi.org/10.1109/Blockchain55522.2022.00077 ; http://doi.org/10.1007/978-3-031-21229-1_34 ; http://doi.org/10.1109/D

Subcluster A2 – Quantum and post-quantum

List of Signals

- 14 | Blind quantum computing
- 15 | Quantum Random Number Generator
- 17 | Quantum entanglement makes quantum communication even more secure
- 25 | Secure network communication PoC with Quantum Key Distribution
- 32 | Laser-equipped Satellites for Secure Quantum Communications
- 33 | Multi-protocol quantum networks
- 34 | Quantum image encryption
- 35 | Quantum Elliptic curve cryptography
- 36 | Quantum communication for secure data exchange
- 38 | Quantum-resistant digital signatures
- 39 | Quantum-resistant ledgers
- 89 | Quantum-Safe VPNs
- 103 | Position-based quantum encryption
- 104 | Satellites for quantum communications
- 120 | Dilithium digital signature algorithms
- 121 | Biochemistry for arts and passwords protection
- 160 | Quantum blockchain
- 391 | Boeing to create first-ever quantum satellite communications technology
- 408 | New method to combine conventional internet with the quantum internet
- 437 | Quantum internet?
- 466 | Post-quantum cryptographic

NUMBER | TITLE
14 | Blind quantum computing
SUMMARY DESCRIPTION
The full power of next-generation quantum computing could soon be harnessed by millions of individuals and companies, thanks to a breakthrough guaranteeing security and privacy. This advance promises to unlock the transformative potential of cloud-based quantum computing. Quantum computing works in a fundamentally different way to conventional computing, is far more powerful and its applications could transform services in many areas like healthcare and financial services. The new study by researchers at Oxford University Physics shows for the first time that quantum computing in the cloud can be accessed in a scalable, practical way which will also give people complete security and privacy of data, plus the ability to verify its authenticity. Researchers used an approach dubbed "blind quantum computing," which connects two totally separate quantum computing entities - potentially an individual at home or in an office accessing a cloud server - in a completely secure way. This new method could be scaled up to large quantum computations.
SOURCE
Project team ScienceDaily https://www.sciencedaily.com/releases/2024/04/240411130238.htm

NUMBER | TITLE

15 | Quantum Random Number Generator

SUMMARY DESCRIPTION

Digital information exchange can be safer, cheaper and more environmentally friendly with the help of a new type of random number generator for encryption, called Quantum Random Number Generator, QRNG. The researchers from Linköping University, Sweden, behind the study believe that the new technology paves the way for a new type of quantum communication. To encrypt information, a random number generator is used, which can either be a computer programme or the hardware itself (considered to be the much safer option as randomness is controlled by physical processes). And the hardware method that provides the best randomness is based on quantum phenomena - what researchers call QRNG. With QRNG's, researchers say, it is possible to certify that a large amount of the generated bits is private and thus completely secure. And if the laws of quantum physics are true it should be impossible to eavesdrop without the recipient finding out. A new type of QRNG, that can be used for encryption, but also for betting and computer simulations. The new feature of the Linköping researchers' QRNG is the use of light emitting diodes made from the crystal-like material perovskite. Their random number generator is among the best produced and compares well with similar products. Thanks to the properties of perovskites, it has the potential to be cheaper and more environmentally friendly.

SOURCE

Project team
ScienceDaily
https://www.sciencedaily.com/releases/2023/09/230904104623.htm

NUMBER | TITLE

17 | Quantum entanglement makes quantum communication even more secure

SUMMARY DESCRIPTION

Three teams of researchers have demonstrated the ability to perform secure quantum communication without prior confirmation that the devices are foolproof. Called device-independent quantum key distribution, the method is based on quantum entanglement, a mysterious relationship between particles that links their properties even when separated over long distances.In everyday communication, such as the transmission of credit card numbers over the internet, a secret code, or key, is used to garble the information, so that it can be read only by someone else with the key. But there's a quandary: How can a distant sender and receiver share that key with one another while ensuring that no one else has intercepted it along the way?
Quantum physics provides a way to share keys by transmitting a series of quantum particles, such as particles of light called photons, and performing measurements on them. By comparing notes, the users can be sure that no one else has intercepted the key. Those secret keys, once established, can then be used to encrypt the sensitive intel

SOURCE

Project team
Science news
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.130.053602

NUMBER | TITLE

25 | Secure network communication PoC with Quantum Key Distribution

SUMMARY DESCRIPTION

A scalable quantum internet connection has been established in the port of Rotterdam. The trial setup demonstrated that the use of quantum technology prevents access to sensitive information. It is still not implemented at scale and expensive, but it looks the price is dropping already. The quantum internet is a theorized and much sought-after network of interconnected quantum computers that will one day allow people to send, compute, and receive information using quantum technology. The purpose of the quantum internet is not to replace the internet we know today, but to instead create a co-existent network that can be used to solve specific types of problems, such as analyzing financial risk, encrypting data, and studying the properties of materials.

SOURCE

Project team
Port of Rotterdam
https://www.portofrotterdam.com/en/news-and-press-releases/consortium-parties-first-world-build-scalable-quantum-internet-connection

NUMBER | TITLE

32 | Laser-equipped Satellites for Secure Quantum Communications

SUMMARY DESCRIPTION

Researchers at the Technical University of Munich (TUM), as part of the QUICK³ project, are aiming to develop new encryption methods for quantum cryptography that use physical laws to prevent message interception over long distances.

The main challenge in quantum cryptography is long-distance data transmission, as light signals in quantum cryptography cannot be repeatedly amplified like in traditional digital communication through fiber optics. This limits the transmission distance to only a few hundred kilometers.

The QUICK³ mission will use satellites to encode information into individual light particles for transmission. Physical laws ensure that any interception of the data will be immediately detected, regardless of technological advancements.

The team has tested each satellite component. The next step involves testing the entire system in space to see if the technology can withstand outer space conditions and how the system components interact. The satellite launch is planned for 2025.

SOURCE

Project team
Website
https://www.tum.de/en/news-and-events/all-news/press-releases/details/satellites-for-quantum-communications

NUMBER | TITLE

33 | Multi-protocol quantum networks

SUMMARY DESCRIPTION

In the initial stage of the quantum Internet, most of the practical quantum networks have been deployed relying on diverse individual quantum key distribution (QKD) protocols. However, this single-protocol paradigm cannot fulfill the heterogeneous requirements of the users, hence market-penetration of quantum networks is limited. Given the recent advances in QKD protocols, the next generation quantum networks are expected to support both legacy and emerging QKD protocols. These studies are contemplating the deployment of different segments of a QKD network, based on different protocols, and the orchestration of such heterogenous network. This will likely be the case when it will be about connecting the different national quantum communication infrastructures in Europe, and, in the future, when it will be about orchestrating networks based partially on discrete and partially on continuous variables.

SOURCE

Project team
IEEE Explore
https://ieeexplore.ieee.org/document/9852377%20;%20https://arxiv.org/abs/2311.12791

NUMBER | TITLE

34 | Quantum image encryption

SUMMARY DESCRIPTION

Quantum image encryption represents a novel approach to secure image processing harnessing the unique capabilities of quantum computing. It involves the use of algorithms that operate on quantum states to scramble and diffuse image data, rendering it incomprehensible without the correct encryption keys. Various strategies have been proposed, some utilizing chaos theory, quantum revolving gates, and the quantum version of Rubik's cube rotation. Others leverage quantum logistic maps, RSA encryption, and secure hash algorithms to generate encryption keys and manipulate image data. Quantum image encryption schemes have been shown to be highly secure, with strong resistance to various cryptographic attacks. In addition, they offer significant computational efficiency compared to classical counterparts, due to the inherent parallelism of quantum computing. These advances in quantum image encryption show great promise for secure image communication, enhancing privacy and data security in various fields such as telemedicine, surveillance, and remote sensing.

SOURCE

Project team
Signals for quantum workshop
https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574

NUMBER | TITLE

35 | Quantum Elliptic curve cryptography

SUMMARY DESCRIPTION

Quantum Elliptic Curve Cryptography (ECC) is a technology application in quantum computing that offers robust security measures for data encryption. Driven by advancements in cloud computing, ECC has emerged as a common practice in a range of fields including the Industrial Internet of Things, smart healthcare, and vehicular social networks. However, traditional public key protocols such as ECC are vulnerable to threats from large-scale quantum computers. Therefore, researchers are developing quantum-resistant algorithms to address these challenges. One notable development is the Isoga scheme, a post-quantum searchable encryption method that combats keyword guessing attacks. This scheme has been demonstrated to be more practical in a quantum environment regarding security, communication cost, and computational load. Another critical development is the lattice cryptography processor with configurable parameters, which offers significant energy savings and system area reduction. However, efficient and secure key agreement and session authentication protocols for IoT deployments are still needed, as existing protocols are either computationally expensive or do not offer the necessary robustness. Quantum ECC is also being developed to provide lightweight quantum-resistant solutions for 5G-enabled vehicular networks. In conclusion, while quantum ECC is an emerging technology with potential applications in various sectors, its development is still ongoing to address the challenges posed by the advent of quantum computers.

SOURCE

Project team
TIM signals for Quantum
https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574

NUMBER | TITLE

36 | Quantum communication for secure data exchange

SUMMARY DESCRIPTION

Quantum communication for secure data exchange is a rapidly advancing field in quantum technology, with significant potential for enhancing data security in various sectors. This technology utilizes quantum systems or classically chaotic systems to generate high-quality random sequences for secure data transfer and storage. Furthermore, semiconductor superlattices at room temperature offer a valuable nanotechnology option for generating these sequences. The development of user-friendly, fiber-coupled, single-photon sources operating at telecom wavelengths is another promising advancement in this field. These sources provide single photons on demand, maximizing data protection and transmission rate. Innovations in free-space optical communication, such as mid-infrared and solar-blind ultraviolet technologies, are also enhancing secure data transfer by reducing scattering losses and preventing remote eavesdropping. The applications of quantum communication for secure data exchange extend to healthcare cybersecurity, the Internet of Things (IoT), and even the Internet of Vehicles (IoV), where secure data transfer is essential. The use of Distributed Ledger Technology, like IOTA, ensures secure and private IoT data transmissions, while the Datagram Transport Layer Security (DTLS) protocol, enhanced by quantum protocol BB84, offers secure data transfer for IoT networks. Moreover, incorporating quantum technologies into sensor design can improve real-time data analytics and ensure secure wireless data transfer. DNA cryptography methods based on the NTRU cryptosystem and lightweight image encryption schemes based on quantum walks are also being explored to enhance data confidentiality. Overall, quantum communication for secure data exchange is a promising field with potential to reshape data security in various sectors.

SOURCE

Project team
Signals for Quantum
https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574

NUMBER | TITLE

38 | Quantum-resistant digital signatures

SUMMARY DESCRIPTION

Quantum-resistant digital signatures are cryptographic techniques designed to securely sign digital transactions even in the face of potential quantum computing attacks. As the development of quantum computers advances, traditional cryptographic methods, such as Elliptic Curve Digital Signature Algorithm (ECDSA), become vulnerable due to their reliance on integer factorization and discrete logarithms, which quantum computers can solve efficiently. Quantum-resistant signatures address this vulnerability, offering protection even if traditional methods are compromised. These signatures are critical in a range of applications such as securing Bitcoin transactions, Internet of Things (IoT) software updates, electronic information transmission in e-commerce, e-voting, and e-learning, as well as in securing the integrity of electronic documents in transport and logistics. Recent developments have focused on designing efficient quantum-resistant signatures using Multivariate Public Key Cryptography (MPKC), hash-based algorithms, and lattice ciphers. Implementation challenges, such as large key and signature sizes, are being addressed through innovative solutions like using application-specific blockchain structures and interplanetary file systems. Quantum-resistant signatures are also being incorporated into privacy-preserving data sharing schemes for medical information and payment channels for Bitcoin.

SOURCE

Project team
Signals for quantum
https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574

NUMBER | TITLE

39 | Quantum-resistant ledgers

SUMMARY DESCRIPTION

Distributed ledger technologies have encryption protocols but with the onset of quantum computing the need to implement post-quantum encryption will become crucial. This is what is being built today to secure against cryptographic threats especially related to digital money. The Quantum Resistant Ledger is a cryptocurrency designed to be secure against quantum computer attacks. It utilizes the eXtended Merkle Signature Scheme (XMSS), a hash-based, forward secure signature scheme with minimal security assumptions and reusable addresses, which has received NIST approval.

SOURCE

Project team
Science and Technology trends 2023
https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

NUMBER | TITLE

89 | Quantum-Safe VPNs

SUMMARY DESCRIPTION

Unlike traditional encryption methods, quantum computers can break into existing cryptographic algorithms without compromising data security. A quantum-safe VPN is a network security measure that uses Post Quantum Cryptography (PQC) to enhance encryption levels. PQC uses unique algorithms to encode data, which makes it more difficult for quantum computers to break encryption. A quantum-safe VPN can create an encrypted tunnel between the sender and receiver. Thus, it will safeguard the data.

SOURCE

Project team
The Future of VPN Technology: Emerging Trends & Innovations; Quantum-safe VPN to safeguard encrypted data https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html; https://www.tcs.com/insights/topics/cybersecurity-topic/article/quantum-safe-vpn

NUMBER | TITLE

103 | Position-based quantum encryption

SUMMARY DESCRIPTION

Using the laws of quantum physics, the researchers developed a new security protocol that uses a person's geographical location to guarantee that they are communicating with the right person. It is called position-based quantum encryption and it can be used to ensure that a person is speaking with an actual bank representative when the bank calls and asks a customer to make changes to their account. "Ask yourself, why do I trust an employee at the bank counter? Because they're in a bank. Their location creates trust. This explains the principle behind pposition-based cryptography, where physical location is used to identify oneself," explains postdoc Andreas Bluhm.The researchers highlight the fact that the new method is particularly handy because only a single quantum bit is needed for position verification.

SOURCE

Project team
Scientific advance leads to a new tool in the fight against hackers
https://www.sciencedaily.com/releases/2022/04/220428125430.htm

NUMBER | TITLE

104 | Satellites for quantum communications

SUMMARY DESCRIPTION

Modern quantum technologies have matured such that they can now be used in space applications, e.g., long-distance quantum communication. The researchers at the Technical University of Munich (TUM) are participating in an international research consortium to develop encryption methods that will apply physical laws to prevent the interception of messages. To safeguard communications over long distances, the QUICK space mission will deploy satellites. A new study proposes using satellite-based single photon sources as a means of secure transmission of information across vast distances. This research not only promises unhackable communication but also opens doors to probing fundamental laws of quantum mechanics and delving into quantum effects in gravity.

SOURCE

Project team
Satellites for quantum communications
https://www.sciencedaily.com/releases/2024/03/240313135442.htm;
https://www.advancedsciencenews.com/satellite-mission-sets-stage-for-unhackable-quantum-communication/

NUMBER | TITLE

120 | Dilithium digital signature algorithms

SUMMARY DESCRIPTION

Dilithium digital signature algorithms are a key component in the field of post-quantum cryptography (PQC), designed to mitigate cybersecurity threats posed by quantum computers. These algorithms work by replacing the deterministic, pseudo-random seed in PQC protocols with a fingerprint derived from the physical disorder of the embedded device, thus enhancing security and maintaining system integrity. This technology can be used to verify the origin and correctness of digital information sent to autonomous systems, from drones to IoT devices, ensuring that only authorized members can send instructions. Dilithium algorithms have also been integrated into secure enclaves in Intel SGX, a set of processor instructions that create hardware-protected secure environments in running programs.

SOURCE

Project team
IACR Transactions on Cryptographic Hardware and Embedded Systems

NUMBER | TITLE

121 | Biochemistry for arts and passwords protection

SUMMARY DESCRIPTION

A new molecular test method helps to prove the authenticity of works of art. The new method could also help to make passwords secure against quantum computers. Researchers at ETH Zurich have presented a cryptographic one-way function that works differently from today's and will also be secure in the future. Rather than processing the data using arithmetic operations, it is stored as a sequence of nucleotides -- the chemical building blocks of DNA. The system is based on true randomness, and since it's a physical system and not a digital one, it can't be decoded by an algorithm, not even by one that runs on a quantum computer.

SOURCE

Project team
Protecting art and passwords with biochemistry
https://www.sciencedaily.com/releases/2024/04/240408130730.htm

NUMBER | TITLE

160 | Quantum blockchain

SUMMARY DESCRIPTION

Quantum blockchain leverages quantum computing and cryptographic principles to create a secure and efficient system for data management and transaction verification. It introduces quantum-resistant algorithms to ensure the integrity of digital signatures and encryption, effectively countering threats from quantum computers running Shor's and Grover's algorithms. Quantum blockchain incorporates concepts like quantum entropy, post-quantum key pairs, and quantum signatures to ensure secure information exchange and transaction verification. It also employs quantum detectable Byzantine agreement (DB to achieve data consensus and unconditionally secure protocols, enhancing the system's reliability and integrity. Applications of quantum blockchain are wide-ranging and include areas like smart cities, edge computing, online voting systems, and the IoT. The novelty in quantum blockchain technology lies in its ability to provide quantum resistance to existing blockchain networks. Compared to traditional blockchain protocols, which are vulnerable to quantum computing attacks, quantum blockchain offers increased security, scalability, and transparency. It uses quantum-resistant algorithms that can withstand attacks from quantum computers, making it a significant advancement in the field of security. Unlike conventional blockchains, quantum blockchains can harness quantum entropy to generate post-quantum key pairs, establish secure connections, and validate transactions using quantum signatures. Furthermore, it leverages the nonlocality of GHZ states to detect node honesty, providing improved scalability and practicality. This technology is thus a game-changer, offering a new level of security and efficiency in data management and consensus-building, especially in the era of quantum computing.

SOURCE

TIM
TIM analytics
http://doi.org/10.1016/bs.adcom.2018.03.003 ; http://doi.org/10.1109/ACCESS.2020.2968985 ; http://doi.org/10.1016/j.ipm.2021.102549 ; http://doi.org/10.1109/ICPC2T53885.2022.9776966 ; http://doi.org/10.1016/j.ins.2023.03.134 ; http://doi.org/10.1109/ISDFS

NUMBER | TITLE

391 | Boeing to create first-ever quantum satellite communications technology

SUMMARY DESCRIPTION

Boeing plans to launch the Q4S mission in 2026, pioneering quantum satellite communications using entanglement swapping in space. This approach involves quantum teleportation, where particle information is transferred without moving the particle itself, potentially creating a secure, global quantum internet. The mission could advance quantum technology's applications in areas such as secure voting and blind quantum computing, where data is processed without revealing it. Boeing's Chief Engineer, Jay Lowell, highlights entanglement swapping as foundational for scaling quantum networks across long distances, overcoming current limitations of sensitivity and resolution in Earth and space data collection. The Q4S mission marks a significant step toward reliable, long-distance quantum networking, paving the way for more sophisticated space-based quantum communication systems.

SOURCE

Project team
Aerotime
https://www.aerotime.aero/articles/boeing-to-create-first-quantum-communications-technology

NUMBER | TITLE

408 | New method to combine conventional internet with the quantum internet

SUMMARY DESCRIPTION

Four researchers from the Institute of Photonics at Leibniz University Hannover have developed a new transmitter-receiver concept for transmitting entangled photons over an optical fiber.
This breakthrough could enable the next generation of telecommunications technology, the quantum Internet, to be routed via optical fibers.
The quantum Internet promises eavesdropping-proof encryption methods that even future quantum computers cannot decrypt, ensuring the security of critical infrastructure.

SOURCE

Project team
Physicists develop new method to combine conventional internet with the quantum internet
https://www.sciencedaily.com/releases/2024/08/240805134133.htm

NUMBER | TITLE

437 | Quantum internet?

SUMMARY DESCRIPTION

In the quest to build a quantum internet, scientists are putting quantum memories to the test.
Quantum memories are devices that store fragile information in the realm of the very small. They're an essential component for scientists' vision of quantum networks that could allow new types of communication, from ultra-secure messaging to linking up far-flung quantum computers. Such memories would help scientists establish quantum connections, or entanglement, throughout a network.

SOURCE

Project team
Two real-world tests of quantum memories bring a quantum internet closer to reality
https://www.sciencenews.org/article/quantum-physics-memories-internet

NUMBER | TITLE

466 | Post-quantum cryptographic

SUMMARY DESCRIPTION

Unlike quantum cryptography, which leverages quantum mechanics for secure communication, emerging privacy-enhancing technologies in the post-quantum cryptographic landscape focus on securing classical digital systems against quantum computer attacks. The most disruptive innovations stem from lattice-based cryptography and quantum-resistant algorithms that protect against potential quantum decryption, which threatens to break current cryptographic methods like RSA and ECC. Lattice-based systems are especially promising due to their high efficiency and scalability for resource-constrained environments, such as IoT devices. New standards (e.g., FIPS 203 and 204) emphasize the adoption of these techniques.
Kyber algorithms, particularly CRYSTALS-KYBER, leverage complex mathematical problems to secure transactions across fields from IoT to healthcare. Supersingular Isogeny Key Encapsulation (SIKE) further enhances post-quantum security with small key sizes and low-resource demands, making it suitable for embedded systems and offering a unique reliance on elliptic curve isogeny maps.
This shift toward post-quantum cryptography not only introduces quantum-resistant algorithms but also allows integration into existing infrastructures, minimizing transition risks. As the post-quantum era nears, these technologies represent a ground-breaking leap in cryptography, laying a foundation for secure, resilient digital ecosystems.

SOURCE

Project team
https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-post-quantum-cryptography-pqc;
https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-l

Subcluster A3 – Internet of things and edge computing

List of Signals

- 24 | IoT applications with Data Privacy-Enhancing Technologies
- 42 | Tiny solar-powered drones could stay in the air forever
- 63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges
- 65 | Privacy-Preserving Multiobjective Sanitization Model in 6G IoT Environments
- 92 | Edge Computing VPNs
- 111 | Edge Computing in Biometrics
- 125 | Adversarial defense
- 152 | Machine learning 4 intrusion detection
- 163 | Reflective intelligent surface 4 security
- 165 | Secure edge computing
- 396 | Towards Privacy in Decentralized IoT: A Blockchain-Based Dual Response DP Mechanism
- 411 | Internet of Behaviour (IoB)
- 448 | Humanoid robots

NUMBER | TITLE
24 | IoT applications with Data Privacy-Enhancing Technologies
SUMMARY DESCRIPTION
Internet of Things (IoT) devices have brought much efficiency and convenience to our daily life. However, the devices may collect a myriad of data from people without their consent. Controlling the large amount of data generated from the devices from being misused is critical to mitigate privacy risks. Therefore, privacy protection on personal data has become an important factor in the development of the IoT. For potential improvements certain solutions are being proposed: blockchain technologies are being applied in PETs in IoT (access control, auditing, and data storage), holistic privacy preservation, adhering the right to be forgotten, realising right to data portability, designing PETs in IoT with the differential privacy, applications of fully homomorphic encryption in PETs, improvements in performance and efficiency.
SOURCE
Project team IEEE Xplore https://ieeexplore.ieee.org/document/8515008

NUMBER | TITLE
42 | Tiny solar-powered drones could stay in the air forever
SUMMARY DESCRIPTION
A drone weighing just 4 grams is the smallest solar-powered aerial vehicle to fly yet, thanks to its unusual electrostatic motor and tiny solar panels that produce extremely high voltages. Although the hummingbird-sized prototype only operated for an hour, its makers say their approach could result in insect-sized drones that can stay in the air indefinitely. Tiny drones are an attractive solution to a range of communications, spying and search-and-rescue problems, but they are hampered by poor battery life, while solar-powered versions struggle to generate enough power to sustain themselves. Researchers from China developed a simple circuit that scales up the voltage produced by solar panels to between 6000 and 9000 volts. Rather than using an electromagnetic motor like those in electric cars, quadcopters and various robots, they used an electrostatic propulsion system to power a 10-centimetre rotor.
SOURCE
Project team New Scientist https://www.newscientist.com/article/2439277-tiny-solar-powered-drones-could-stay-in-the-air-forever

NUMBER | TITLE

63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges

SUMMARY DESCRIPTION

Sixth-generation (6G) mobile networks will have to cope with diverse threats on a space-air-ground integrated network environment, novel technologies, and an accessible user information explosion. However, for now, security and privacy issues for 6G remain largely in concept. This survey provides a systematic overview of security and privacy issues based on prospective technologies for 6G in the physical, connection, and service layers, as well as through lessons learned from the failures of existing security architectures and state-of-the-art defenses. Two key lessons learned are as follows. First, other than inheriting vulnerabilities from the previous generations, 6G has new threat vectors from new radio technologies, such as the exposed location of radio stripes in ultra-massive MIMO systems at Terahertz bands and attacks against pervasive intelligence. Second, physical layer protection, deep network slicing, quantum-safe communications, artificial intelligence (AI) security, platform-agnostic security, real-time adaptive security, and novel data protection mechanisms such as distributed ledgers and differential privacy are the top promising techniques to mitigate the attack magnitude and personal data breaches substantially.

SOURCE

Project team
Professional association
https://ieeexplore.ieee.org/document/9524814

NUMBER | TITLE

65 | Privacy-Preserving Multiobjective Sanitization Model in 6G IoT Environments

SUMMARY DESCRIPTION

The next revolution of the smart industry relies on the emergence of the Industrial Internet of Things (IoT) and 5G/6G technology. The properties of such sophisticated communication technologies will change our perspective of information and communication by enabling seamless connectivity and bring closer entities, data, and “things.” Terahertz-based 6G networks promise the best speed and reliability, but they will face new man-in-the-middle attacks. In such critical and high-sensitive environments, the security of data and privacy of information still a big challenge. Without privacy-preserving considerations, the configuration state may be attacked or modified, thus causing security problems and damage to data. In this article, motivated by the need to secure 6G IoT networks, an ant colony optimization (ACO) approach is presented by adopting multiple objectives as well as using transaction deletion to secure confidential and sensitive information. Each ant in the population is represented as a set of possible deletion transactions for hiding sensitive information. We utilize the use of a prelarge concept to assist in the reduction of multiple database scans in the evaluation progress. We then also adopt external solutions to maintain discovered Pareto solutions, thus improving effectiveness to find optimized solutions. Experiments are conducted comparing our methodology to state-of-the-art bioinspired particle swarm optimization (PSO) as well as genetic algorithm (GA). Our strong results clearly show that the designed approach achieves fewer side effects while maintaining low computational cost overall

SOURCE

Project team
Professional association
https://ieeexplore.ieee.org/document/9234523

NUMBER | TITLE

92 | Edge Computing VPNs

SUMMARY DESCRIPTION

In simple words, edge computing involves processing data closer to the source – such as IoT devices, sensors, or mobile devices. Usually, such devices have limited resources as well as unstable connections. In this sense, edge computing VPNs prioritize speed and minimize latency. All while establishing secure connections with unreliable networks. The use cases of such technology are genuinely futuristic. For example, they are integral to autonomous vehicles, smart cities, and industrial automation.

SOURCE

Project team
The Future of VPN Technology: Emerging Trends & Innovations
https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html

NUMBER | TITLE
111 | Edge Computing in Biometrics
SUMMARY DESCRIPTION
Edge computing brings processing power closer to the data source, allowing for faster analysis and response, a critical factor in biometrics. With edge AI, facial authentication can be performed locally on a device, offering improved privacy and performance. Devices with edge computing capabilities are less reliant on cloud servers, reducing latency and the risk of a data breach. This trend dovetails with the rising demand for on-device processing in biometric systems.
SOURCE
Project team The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/

NUMBER | TITLE
125 | Adversarial defense
SUMMARY DESCRIPTION
Adversarial Defense is a technology in the field of security that focuses on enhancing the robustness of machine learning and deep learning systems against adversarial attacks. These attacks typically involve introducing small, often imperceptible, modifications to input data (such as images, text, or sounds) in order to deceive machine learning models, causing them to misclassify. In the context of Internet of Things (IoT) and Android applications, adversarial defense techniques can be used to detect and neutralize malicious Android apps. This is achieved through the use of graph-based classification, generative adversarial networks, and other machine learning algorithms. Similarly, in the realm of air transportation communication, adversarial defense can bolster the reliability of communication jamming recognition models. Adversarial defense technology also finds application in autonomous driving, where it helps to improve the robustness of deep visual detectors. The novelty of adversarial defense lies in its ability to provide robustness against adversarial attacks in a variety of application domains. Unlike traditional security methods that may not effectively mitigate the vulnerabilities of deep learning systems, adversarial defense offers a more resilient approach. Techniques such as Stochastic Activation Pruning (SAP) that prune and scale activations within neural networks, and FaceGuard, a self-supervised adversarial defense framework that automatically detects and purifies adversarial faces, represent significant advancements in this area. However, despite these innovations, the technology still faces challenges, especially in terms of its robustness against adaptive attacks. Hence, continuous research and development are needed to further improve the efficacy of adversarial defense technology.
SOURCE
TIM TIM analytics http://doi.org/10.1016/j.eng.2019.12.012 ; http://doi.org/10.1109/TEM.2021.3059664 ; http://doi.org/10.1109/JIOT.2022.3188583 ; http://doi.org/10.1109/IV51971.2022.9827222 ; http://doi.org/10.1007/978-3-031-20096-0_31 ; http://doi.org/10.1109/FG57933.2023

NUMBER | TITLE

152 | Machine learning 4 intrusion detection

SUMMARY DESCRIPTION

Machine learning for intrusion detection involves the use of advanced computational algorithms to identify anomalies or malicious activity in network systems, thereby enhancing cybersecurity. This technology utilizes machine learning and deep learning to analyze large amounts of data, identify patterns, and predict potential intrusions. It includes methods such as Principal Component Analysis for dimension reduction, Random Oversampling for data imbalance, and hybrid models for higher detection rates. Additionally, techniques like Stacking Feature Embedding based on clustering results and XGBoost for feature selection are used for efficient pre-processing. Quantum machine learning may also be employed to improve capacity and learning efficiency. The technology can be applied in various network environments including the Industrial Internet of Things (IIoT), where it can help to detect and update models on network intrusions and attacks in real time. The novelty of machine learning for intrusion detection lies in its ability to handle large and imbalanced datasets, its high accuracy rates, and its adaptability to different network environments and attack scenarios. The development of hybrid models combining machine learning and deep learning, as well as the use of quantum machine learning algorithms, represents a significant advancement over traditional intrusion detection methods. Moreover, the technology's adaptability to real-world networks and its potential to be deployed in resource-constrained environments like IIoT further underscore its innovative aspects. Despite its novelty, there is a recognized need for more practical deployment and evaluation methodologies, as well as for addressing issues related to adversarial attacks and the vulnerability of deep neural networks.

SOURCE

TIM
TIM analytics
http://doi.org/10.1007/978-3-030-72802-1_9 ; http://doi.org/10.1109/SP.2010.25 ;
http://doi.org/10.1109/ICIT52682.2021.9491770 ; http://doi.org/10.1109/JIOT.2022.3172393 ;
http://doi.org/10.1016/j.jisa.2022.103405 ; http://doi.org/10.1109/COMST.2022.32337

NUMBER | TITLE

163 | Reflective intelligent surface 4 security

SUMMARY DESCRIPTION

Reflective Intelligent Surface for Security (RIS4Securit) is a novel technology that enhances security in wireless communications by manipulating electromagnetic waves in a programmable manner. This technology utilizes Reconfigurable Intelligent Surfaces (RIS) and Rate-Splitting Multiple Access (RSM strategies to improve security in the physical layer of communication systems. RIS4Securit aims to maximize the secrecy rate of the system, offering protection against eavesdropping and jamming attacks by optimizing the beamforming and phase shifts of the RIS. Potential applications include enhancing security in Internet-of-Things (IoT), wireless networks, unmanned aerial vehicles, and ground targets, among others. The novelty of RIS4Securit lies in its integration of RIS and RSMA, a departure from traditional methods of security and interference management in wireless communication systems. Unlike traditional methods, RIS4Securit offers numerous benefits including enhanced spectral, energy, and computation efficiency, flexibility in coping with any interference levels, and robustness to inaccurate channel state information. Furthermore, it outperforms established technologies in terms of its resilience to mixed-critical quality of service and reliability under short channel codes and low latency. The STAR-RIS (Simultaneously Transmitting and Reflecting Reconfigurable Intelligent Surface) variant of RIS4Securit, for instance, has shown to significantly outperform conventional RIS in terms of long-term security rate maximization.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/TII.2023.3292968 ; http://doi.org/10.1109/COMST.2021.3123267 ;
http://doi.org/10.1109/MWC.018.2100717 ; http://doi.org/10.1109/TVT.2022.3213334 ;
http://doi.org/10.1109/COMST.2022.3225859 ; http://doi.org/10.1016/j.dt.2022.12.010 ;

NUMBER | TITLE

165 | Secure edge computing

SUMMARY DESCRIPTION

Secure edge computing is a technology that aims to enhance data security and privacy in the field of Internet of Things (IoT). This technology enables data processing at or near the source of data, allowing for efficient computation offloading, real-time analytics, and privacy-preserving interactions between IoT applications and cloud servers. Notably, secure edge computing systems such as Intelligent Trusted and Secure Edge Computing (ITEC) incorporate mechanisms for detecting and managing potential malware attacks from untrusted third-party IoT applications. Other novel configurations include the use of reconfigurable intelligent surface (RIS)-assisted frameworks, blockchain technologies, and homomorphic cryptosystem-based models for secure data processing. These systems have found applications in diverse areas including healthcare, vehicular networks, and surveillance, where they help to mitigate security risks and ensure data integrity. Compared with traditional cloud computing, secure edge computing introduces novel approaches to handling the security challenges posed by the proliferation of IoT devices. Its application in fields such as healthcare and vehicular networks represents a significant advancement over established technologies. The use of intelligent systems like ITEC, which pre-identify malicious behaviors and embed delay strategies for threat analysis, is a fresh approach to IoT security. Similarly, the development of RIS-assisted secure mobile edge computing (MEC) networks, blockchain-integrated aerial computing networks, and homomorphic cryptosystem-based secure data processing models represent new methodologies for enhancing task offloading security and privacy-preserving computation offloading. Therefore, secure edge computing represents a significant step forward in the field of IoT security, offering innovative solutions to the challenges posed by the proliferation of IoT devices and applications.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/SEC.2018.00060 ; http://doi.org/10.1109/TVT.2019.2912227 ; http://doi.org/10.1109/JIOT.2021.3065970 ; http://doi.org/10.1109/TSC.2022.3155447 ; http://doi.org/10.1109/TVT.2022.3162044 ; http://doi.org/10.1109/TII.2023.3245681 ; http

NUMBER | TITLE

396 | Towards Privacy in Decentralized IoT: A Blockchain-Based Dual Response DP Mechanism

SUMMARY DESCRIPTION

A novel blockchain-based dual response differential privacy (DP) mechanism addresses privacy challenges in decentralized IoT environments, where collusion attacks are a key vulnerability. Traditional DP methods struggle in these settings due to the lack of synchronized privacy budget tracking and query history sharing across nodes, enabling adversaries to extract sensitive data through excessive querying. This new dual response mechanism introduces both direct and indirect strategies for responding to external queries, optimizing privacy without sacrificing data utility. By synchronizing query history and privacy budget usage across the blockchain, the mechanism mitigates privacy risks effectively. Performance assessments using metrics like Relative Error (RE), Mean Square Error (MSE), and privacy budget consumption confirm the mechanism's adaptability and robust privacy preservation within decentralized IoT networks.

SOURCE

Project team
Zhang K, Tsai P-W, Tian J, et al.
https://www.sciopen.com/article/10.26599/BDMA.2024.9020023

NUMBER | TITLE
411 | Internet of Behaviour (IoB)
SUMMARY DESCRIPTION
The aim of IoB is to address how data collected can be interpreted from a human psychological and sociological perspective and how to use this understanding to influence or change human behaviour for various purposes, ranging from commercial interests to public policies.The Internet of Behaviour (IoB) represents a convergence of multiple disciplines: technology, data analytics, and behavioural psychology. It's an emerging field that extends beyond the data collection capabilities of the Internet of Things (IoT) to delve into the realm of behavioural science. IoB is increasingly becoming a cornerstone in our digital world. The Internet of Behaviour (IoB) extends its reach by collecting and analysing data from a wide array of sources, including IoT devices, social media platforms, and websites. This comprehensive scope of data collection raises significant ethical, security, and privacy concerns that must be addressed meticulously.IoB data, encompassing sensitive information like bank codes and personal habits, present lucrative targets for cybercriminals. Risks include potential cyber-attacks, identity theft, ransomware, money laundering, and sophisticated phishing attempts.
SOURCE
Project team What is the Internet of Behaviour? A Comprehensive Guide https://www.sovtech.com/blog/what-is-the-internet-of-behaviour-a-comprehensive-guide

NUMBER | TITLE
448 | Humanoid robots
SUMMARY DESCRIPTION
Humanoid robots are robots that resemble and act like humans. Typically engineered to imitate authentic human expressions, interactions and movements, these robots are often outfitted with an array of cameras, sensors and AI and machine learning technologies. Humanoid robots could be used in different kinds of tasks and services for eg. in healthcare, production and customer services.
SOURCE
Experts https://builtin.com/robotics/humanoid-robots

Subcluster A4 – Identity and deepfakes

List of Signals

- 22 | Biometric Security
- 27 | Privacylens camera turns people in images into stick figures
- 31 | Clothing to trick facial recognition cameras
- 44 | Digital identity – enabling secure collaboration with blockchain technology
- 47 | How Blockchains Can Help Solve AI's Deepfake Problem
- 53 | What is Synthetic Data? Use Cases & Benefits in 2024
- 56 | AI 'deepfake' faces detected using astronomy methods
- 97 | New Digital Identity models for travels
- 98 | Verifiable Credentials
- 99 | Selective disclosure
- 106 | Multimodal Authentication
- 108 | DPGazeSynth
- 109 | 3D Facial Authentication
- 110 | Biometrics for Contactless Transactions / payments
- 111 | Edge Computing in Biometrics
- 112 | Liveness detection
- 113 | Blockchain integration into biometric domain
- 114 | Biometric Continous Authentication
- 115 | Attribute-based credentials
- 122 | Voice conversion methods
- 137 | Decentralized identity
- 138 | Deepfake detection
- 153 | Machine unlearning
- 154 | Masked face recognition
- 159 | Privacy-preserving machine learning
- 166 | Self sovereign identity
- 394 | Face privacy protection scheme by security-enhanced encryption structure and nonlinear dynamics
- 407 | WebXR allowing for the creation of digital nation-states
- 410 | digital identity wallet
- 413 | Generative Adversarial Network
- 444 | Adverserial wearables
- 446 | SecureNed
- 448 | Humanoid robots

NUMBER | TITLE

22 | Biometric Security

SUMMARY DESCRIPTION

Biometric security is a cutting-edge technology that leverages unique physiological or behavioral characteristics to verify and authenticate an individual's identity. It goes beyond traditional forms of authentication like passwords or smart cards and brings a whole new level of security to the table. It's being used already but future developments in the areas of voice recognition, facial recognition systems, fingerprint scanning (e.g. enhancement through ultrasonic sensors that capture more detailed information about the ridges and pores on our fingertips), gait analysis (measuring how someone walks), vein patterns under the skin.

SOURCE

Project team
Biometric Security: The Future of Identity Authentication
https://medium.com/@analyticsemergingindia/biometric-security-the-future-of-identity-authentication-070fa916b455

NUMBER | TITLE

27 | Privacylens camera turns people in images into stick figures

SUMMARY DESCRIPTION

Engineers at the University of Michigan (U-M) have found a way to preserve privacy without sacrificing security or the capabilities of a multitude of smart devices designed to make our lives easier. They've developed a new camera dubbed PrivacyLens that can mask a person's identity by turning them into a stick figure, before it gets sent anywhere. The PrivacyLens consists of a standard video camera and a heat-sensing camera – to identify the presence of a person from their body temperature. Onboard electronics then remove the person from the video and replace them with an animated stick figure that mimics their actual movements. The processing to achieve this takes place on the camera, so in theory, no identifiable images are transmitted to the cloud.

SOURCE

Project team
New Atlas
https://newatlas.com/technology/privacylens-camera-stick-figure

NUMBER | TITLE

31 | Clothing to trick facial recognition cameras

SUMMARY DESCRIPTION

Many options for helping people outsmart facial-recognition involve wearing a mask, but the Italian fashion startup Cap-able aims to do the same thing without the need to cover your face. A $400 sweater tricks facial-recognition cameras into thinking you're a zebra or a giraffe to protect your privacy. It uses animal-based patterns to deceive facial-recognition software. Being identified as an animal often stops facial-recognition software from starting to begin analyzing, collecting, and storing your biometric data, the company says.

SOURCE

Project team
Website
https://www.businessinsider.com/facial-recognition-cameras-sweater-protect-privacy-data-trick-fool-clothes-2023-2

NUMBER | TITLE

44 | Digital identity – enabling secure collaboration with blockchain technology

SUMMARY DESCRIPTION

Self-sovereign identities (SSI) are digital identities that are managed in a decentralized manner. This technology allows users to self-manage their digital identities without depending on third-party providers to store and centrally manage the data. Bosch Research is part of the IDunion consortium initiated by the German Federal Ministry of Economics. Policymakers and industry are working together to establish an open digital ecosystem for decentralized identity management so that people, companies and machines can interact safely and reliably in the Internet of Things based on artificial intelligence (AIoT). Already today, companies can use SSI for their corporate identity and master data management.

SOURCE

Project team
Bosh
https://www.bosch.com/stories/self-sovereign-identities/

NUMBER | TITLE
47 | How Blockchains Can Help Solve AI's Deepfake Problem
SUMMARY DESCRIPTION
AI-generated content creates a huge online disinformation threat. Blockchain can help verify and authenticate that what is being said is true. Harvard experts already predict that more than 90% of content online will be AI-generated in the future. To protect against threats such as deepfakes, it's crucial we get ahead of the issue and implement innovative solutions. Public blockchains, collectively owned and operated by users, offer promising features like network security, transparency, and decentralization which can help against the issues deepfakes present.
SOURCE
Project team CoinDesk https://www.coindesk.com/opinion/2024/05/22/how-blockchains-can-help-solve-ais-deepfake-problem/

NUMBER | TITLE
53 | What is Synthetic Data? Use Cases & Benefits in 2024
SUMMARY DESCRIPTION
Developing successful AI and ML models requires access to large amounts of high-quality data. However, collecting such data is challenging because it requires access to sensitive customer data such as Personally Identifiable Information (PII) or Personal Health Information (PHI). Collecting and using sensitive data raises privacy concerns and leaves businesses vulnerable to data breaches. Furthermore, some types of data are costly to collect, or they are rare (e.g. bank fraud). As a result, businesses are turning to data-centric approaches to AI/ML development, including synthetic data to solve these problems. Generating synthetic data is inexpensive compared to collecting large datasets and can support AI/deep learning model development or software testing without compromising customer privacy. It's estimated that by the end of 2024, 60% of the data used to develop AI and analytics projects will be synthetically generated.
SOURCE
Project team AIMultiple https://research.aimultiple.com/synthetic-data/

NUMBER | TITLE
56 | AI 'deepfake' faces detected using astronomy methods
SUMMARY DESCRIPTION
Advances in artificial intelligence (AI) are making it increasingly difficult to tell the difference between genuine images, videos and audio and those that have been created by algorithms. Deepfakes substitute the features of one person or environment with another, and can make it seem as though individuals said or did things that they did not. Analysing reflections of light in the eyes can help to determine an image's authenticity. By analysing images of faces using methods that are usually used to survey distant galaxies, astronomers can measure how a person's eyes reflect light, which can reveal telltale signs of image manipulation.
SOURCE
Project team Nature https://www.nature.com/articles/d41586-024-02364-y

NUMBER | TITLE

97 | New Digital Identity models for travels

SUMMARY DESCRIPTION

The report outlines three identity models that, they argue, will play a fundamental role in the future of secure and seamless travel.
1) ICAO released the Digital Travel Credential (DTC) that presents an opportunity to accelerate seamless travel using a global standard with a clearly defined ICAO governance. This virtual credential is an exact representation of the ePassport, containing the holder's facial image, biographical data, and security features. Once generated, DTC can be securely stored on the holder's device and shared with travel service providers (e.g., border agencies) ahead of travel to provide required information.
2)The International Organization for Standardization (ISO) is developing mobile driving license (mDL) standard that is gaining a lot of traction, especially in the US, where the number of states offering mDLs is rapidly growing due to increasing demand for contactless forms of digital ID. This mDL specification supports privacy-preserving techniques like selective disclosure where only required information and not the whole credential is shared.
3) W3C standards for decentralized (or self-sovereign) identity and verifiable credentials (VCs) re-envision the way we share, access, control, and manage our online personal information. Decentralized digital identity gives individuals full control of their digital identities and has privacy by design at its core. With the right governance and trust frameworks in place, this new wave of digital identity credentials could be accepted across sectors and borders, support a wide variety of interactions, and help move towards a fully digital travel experience.

SOURCE

Project team
Digital identity models: What's next for secure and seamless travel?
https://www.weforum.org/agenda/2023/05/emerging-digital-identity-models-secure-and-seamless-travel/

NUMBER | TITLE

98 | Verifiable Credentials

SUMMARY DESCRIPTION

Verifiable Credentials are a digital, cryptographically secured version of both paper and digital credentials that people can present to organizations that need them for verification. In the Verifiable Credentials ecosystem, there is an issuer, holder, and verifier.One of the main benefits of Verifiable Credentials is that issuing organizations can generate fraud-proof digital credentials and verifying organizations can instantly check the authenticity of those credentials. Individuals have full ownership and control of their data while preserving privacy as well as providing improved security.There are a growing number of use cases where Verifiable Credentials can be used in a variety of sectors including supply chain, education, and finance. Verifiable Credentials, blockchain, and decentralized identifiers work together to create Verifiable Credential system

SOURCE

Project team
Verifiable Credentials: The Ultimate Guide 2024
https://www.dock.io/post/verifiable-credentials#how-does-a-verifiable-credential-work

NUMBER | TITLE

99 | Selective disclosure

SUMMARY DESCRIPTION

Digital credentials represent digital versions of physical credentials. They are the cornerstone of digital identity on the Internet. In order to enhance privacy, different authors implement selective disclosure in digital credentials (e.g. anonymous credentials, attribute-based credentials and the relatively new verifiable credentials), allowing users to disclose only the claims or attributes they want. With selective disclosure, access to data is limited, especially to personal data. Selective disclosure represents a mechanism for preserving privacy for individuals and organizations. It can be seen as a privacy design pattern that enhances privacy and security.

SOURCE

Project team
Selective disclosure in digital credentials: A review
https://www.sciencedirect.com/science/article/pii/S2405959524000614#d1e1791

NUMBER | TITLE

106 | Multimodal Authentication

SUMMARY DESCRIPTION

While fingerprint biometrics remain popular, we'll see increased adoption of multi-factor authentication (MFA) using combinations of facial recognition, voice analysis, iris scans and even gait recognition. This offers enhanced security and caters to individual preferences.Multimodal biometric authentication utilizes a process called fusion to combine data from various modalities.

SOURCE

Project team
10 Biometric Trends to Watch in 2024
https://blog.hidglobal.com/2024/01/10-biometric-trends-watch-2024; https://www.oloid.ai/blog/beyond-fingerprints-the-power-of-multimodal-biometric-authentication/

NUMBER | TITLE

108 | DPGazeSynth

SUMMARY DESCRIPTION

As spatial computing devices increasingly integrate eye-tracking technology to enhance virtual reality (VR) experiences, the imperative to protect sensitive eye-tracking data against privacy risks, such as user re-identification, has become more pressing. Existing privacy-preserving mechanisms face challenges in balancing the dual demands of privacy and utility in the context of VR applications. This paper presents DPGazeSynth, a novel framework designed to fortify privacy protections while ensuring the utility of eye-tracking data. DPGazeSynth addresses the unique requirements of gaze path synthesis, especially the differentiation between fixations and saccades. Our approach introduces a semi-synthetic method based on the Markov Chain model to accurately maintain data correlations for analytical tasks. We demonstrate that DPGazeSynth provides robust differential privacy guarantees, and our comprehensive experiments on two real-world datasets validate its effectiveness in safeguarding against re-identification attacks.

SOURCE

Project team
DPGazeSynth: Enhancing eye-tracking virtual reality privacy with differentially private data synthesis
https://doi.org/10.1016/j.ins.2024.120720

NUMBER | TITLE

109 | 3D Facial Authentication

SUMMARY DESCRIPTION

While conventional 2D authentication methods have been widely implemented, 3D facial authentication is quickly gaining ground for its superior accuracy and security. This technology maps the contours of a face in three dimensions, which not only makes it more challenging for potential spoofing but also allows for authentication even in low light or extreme angles. Many smartphones are already integrating systems like Apple's Face ID, but expect this trend to spill over into sectors like finance, border control, and healthcare, where the precision of authentication is a top priority. Sometimes it is linked to 3D liveness detection.

SOURCE

Project team
The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch
https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/; https://facia.ai/blog/3d-face-recognition/

NUMBER | TITLE

110 | Biometrics for Contactless Transactions / payments

SUMMARY DESCRIPTION

Contactless facial authentication is poised to revolutionize retail, healthcare, and travel, where fast and touchless operations are in demand. Companies like Mastercard and Alipay are already piloting systems that link your face to payment verification, streamlining the check-out process. Security is bolstered by advanced liveness detection and integration with secure element chips, ensuring that your payments are tied to no one but you.

The incorporation of biometrics into contactless payments is just the beginning. As technology continues to evolve, we can expect to see further advancements in this field.One such advancement is the use of multi-factor authentication, combining biometric data with other forms of verification, such as a PIN or a one-time password. This multi-layered approach will create even stronger security measures, making it even more challenging for fraudsters to access sensitive payment information.

Furthermore, the emergence of artificial intelligence (AI) and machine learning (ML) will revolutionize the field of biometrics and contactless payments. These technologies have the potential to improve the accuracy and efficiency of biometric authentication, making it even more reliable and seamless.

SOURCE

Project team

The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/; https://alicebiometrics.com/en/biometrics-contactless-payments/

NUMBER | TITLE

111 | Edge Computing in Biometrics

SUMMARY DESCRIPTION

Edge computing brings processing power closer to the data source, allowing for faster analysis and response, a critical factor in biometrics. With edge AI, facial authentication can be performed locally on a device, offering improved privacy and performance. Devices with edge computing capabilities are less reliant on cloud servers, reducing latency and the risk of a data breach. This trend dovetails with the rising demand for on-device processing in biometric systems.

SOURCE

Project team

The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/

NUMBER | TITLE

112 | Liveness detection

SUMMARY DESCRIPTION

Liveness detection is a technique where an algorithm securely detects whether the source of a biometric sample comes from a fake representation or is a live human being. The biometric sample is a facial photo taken by a user. The algorithm is able to recognize a live person from presentation attacks, for example, masks, photos, or videos. There are active, passive and hybrid (or semi-passive) liveness detection technologies. In the first case, liveness is being detected by prompting a user to perform a simple task like watching a moving object on a screen or performing some simple movement with one's head. In the second, liveness detection running in the background of the biometric facial verification process.The future sees more advanced systems using techniques like eye tracking and blinking pattern analysis.

SOURCE

Project team

The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/; https://www.innovatrics.com/glossary/liveness-detection/

NUMBER | TITLE
113 | Blockchain integration into biometric domain
SUMMARY DESCRIPTION
The insecurities of centralized data storage have prompted the exploration of blockchain technology in the biometric domain. Blockchain's immutable ledger is being considered for storing encrypted biometric data, enhancing security and giving control back to the individual. Companies like Hyland Credentials and Bext Holdings are pioneering blockchain solutions that promise to revolutionize how facial data is stored and used, fostering trust in systems that handle personal identities.
SOURCE
Project team The Future of Facial Authentication & Biometrics: 8 Emerging Trends to Watch https://bioconnect.com/2024/04/18/the-future-of-facial-authentication-biometrics-8-emerging-trends-to-watch/; https://arxiv.org/pdf/2003.09262; https://arxiv.org/pdf/2302.10883

NUMBER | TITLE
114 | Biometric Continous Authentication
SUMMARY DESCRIPTION
Authentication usually relies on statical processes like the use of passwords, cards, or any biometric trait of the person. The main aim is to verify the identity of users at the beginning of the delivery of a service or at the entrance of a specific area. Contrasting with this approach, continuous authentication aims at repeating this verification throughout a specific time frame during the delivery of an electronic service or during the presence of a person in a certain area. Biometric continuous authentication is a type of continuous authentication that verifies a user identity by using biometric traits or behaviours. Examples include facial images, typing, screen tapping, walking patterns or voice. Applications of biometric continuous authentication can be seen in banking services, identification of stolen mobile devices or authentication on smart home devices.
SOURCE
Project team Biometric Continuous Authentication https://www.edps.europa.eu/press-publications/publications/techsonar/biometric-continuous-authentication_en

NUMBER | TITLE
115 | Attribute-based credentials
SUMMARY DESCRIPTION
Privacy-preserving ABCs enable identity management providing data minimization. Anonymous credentials refer to a type of certification that allows users to prove certain properties without revealing all their personal attributes. These credentials provide stronger privacy properties compared to traditional credentials by enabling selective disclosure and unlinkability of different uses of the credential. Despite the latest efforts to foster the adoption of privacy-enhancing Attribute-Based Credential (p-ABC) systems in electronic services, those systems are not yet broadly adopted. The main reasons behind this are performance efficiency issues, lack of interoperability with standards, and the centralized architectural scheme that relies on a unique Identity Provider (IdP) for credential issuance.
SOURCE
Project team Simply tell me how -- On Trustworthiness and Technology Acceptance of Attribute-Based Credentials https://arxiv.org/abs/2308.06555; https://blog.dock.io/anonymous-credentials/; https://www.sciencedirect.com/science/article/pii/S2214212621001824; https://www.sciencedirect.com/topics/computer-science/anonymous-credential

NUMBER | TITLE
122 | Voice conversion methods
SUMMARY DESCRIPTION
Voice conversion is a process where the essence of a speaker's identity is seamlessly transferred to another speaker, all while preserving the content of their speech. This usage is accomplished using algorithms that blend speech processing techniques, such as speech analysis, speaker classification, and vocoding. The cutting-edge voice conversion technology is characterized by deep neural networks that effectively separate a speaker's voice from their linguistic content.
SOURCE
Project team Overview of Voice Conversion Methods Based on Deep Learning https://www.mdpi.com/2076-3417/13/5/3100

NUMBER | TITLE
137 | Decentralized identity
SUMMARY DESCRIPTION
Decentralized identity is an innovative technology in the security field that leverages blockchain and artificial intelligence to address challenges in data privacy, authentication, and data sharing, especially in edge applications. It enables users and devices to have full control over their data, providing a means to build and prove their identity. This technology uses Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to authenticate and verify identities, making it a viable solution for managing identities across a vast digital landscape. It has potential applications in various sectors, including IoT, edge computing, AI, cloud computing, and even sustainable material production. Its use could help create a more secure, private, and decentralized internet. The novelty of decentralized identity lies in its user-centric approach and the employment of blockchain technology. Unlike traditional identity management systems that rely on a centralized authority, decentralized identity gives control back to the users, addressing privacy and security concerns associated with large-scale data storage. It uses blockchain's immutable and transparent nature to ensure data integrity and verifiability, which is a considerable improvement over traditional systems. Moreover, it provides a solution to device authentication and data sharing difficulties in edge applications, offering a more secure and efficient way to manage identities in an increasingly digitally connected world.
SOURCE
TIM TIM analytics http://doi.org/10.1109/ISSE49799.2020.9272223 ; http://doi.org/10.1109/SP40001.2021.00038 ; http://doi.org/10.1109/SPW54247.2022.9833873 ; http://doi.org/10.1016/j.compag.2022.107544 ; http://doi.org/10.1007/s10586-022-03921-8 ; http://doi.org/10.1109/JIO

NUMBER | TITLE

138 | Deepfake detection

SUMMARY DESCRIPTION

Deepfake detection technology leverages advanced machine learning models to identify falsified images or videos, a byproduct of the rapid advancements in deep generative models and deepfake techniques. Deepfake detection primarily utilizes Convolutional Neural Networks (CNNs), but recent studies have combined Vision Transformers with EfficientNet B0 for enhanced performance. Other innovative methods include the use of rational augmented CNNs for real-time facial reconstruction, noise-based models focusing on forensic noise traces left by deepfake videos, and watermarking facial identity features as anti-deepfake labels. The technology has also been applied to deepfake text detection, aiming to differentiate between human and machine-generated text. The novelty of deepfake detection lies in its ability to adapt and evolve with the increasing sophistication of deepfake generation. Traditional CNN-based detection methods are being augmented with Vision Transfomers for improved results. To tackle challenges posed by the 'Implicit Identity Leakage' phenomenon, ID-unaware Deepfake Detection Models have been proposed. NoiseDF, a noise-based deepfake detection model, utilizes underlying forensic noise traces for detection. Moreover, a novel method embedding watermarks into facial identity features has been introduced as a safeguard against malicious deepfake tampering. The Multi-Channel Xception Attention Pairwise Interaction (MCX-API) method showcases enhanced generalization ability across different deepfake generation types. Furthermore, the person-of-interest (POI) deepfake detector, trained exclusively on real talking-face video, exhibits high generalization ability and robustness against various manipulation methods and quality levels. This continuous innovation underscores the ongoing development in the field of deepfake detection technology.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/CVPR42600.2020.00327 ; http://doi.org/10.1007/s13204-021-02072-3 ; http://doi.org/10.1007/978-3-031-06433-3_19 ; http://doi.org/10.1109/HORA55278.2022.9799858 ; http://doi.org/10.1109/WACVW58289.2023.00074 ; http://doi.org/10.1109/W

NUMBER | TITLE

153 | Machine unlearning

SUMMARY DESCRIPTION

Machine unlearning is a technology that involves removing or 'unlearning' certain data from a machine learning (ML) model, with the aim of enhancing privacy and security. This process could be crucial in situations where data owners want their information forgotten, or when an anomaly detector needs to forget injected data to regain security. It can also be used to remove noise and incorrect entries for improved system usability. This technology can deal with single or multiple classes of data, and its process can be scaled to large datasets and generalized to different deep networks. The unlearning process is achieved by manipulating the model weights with an error-maximizing noise matrix learned for the class to be unlearned using the original model. The technology can also be used to erase backdoors injected into ML models, thus defending against backdoor injection attacks. Moreover, it can be utilized for reverting policies in machine learning-based access control systems and addressing potential vulnerabilities. The novelty of machine unlearning technology lies in its ability to efficiently and effectively 'unlearn' specific data from ML models without retraining the model from scratch or accessing the full training data. This marks a departure from traditional methods that required substantial computational resources or access to original training data, making it a more practical and scalable solution. Furthermore, the technology introduces a new approach to privacy and security by providing a means to erase data in response to new privacy risks or security threats. However, it's important to note that while machine unlearning is designed to enhance privacy, it may leave some imprint of the data in the ML model, potentially creating unintended privacy risks. Therefore, ongoing research is crucial to mitigate these risks and improve privacy protection in practical implementations of this technology.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/SP.2015.35 ; http://doi.org/10.1145/3460120.3484756 ; http://doi.org/10.1109/INFOCOM48880.2022.9796974 ; http://doi.org/10.1145/3548606.3559352 ; http://doi.org/10.1109/TIFS.2023.3265506 ; http://doi.org/10.1007/s42979-023-01767-4 ;

NUMBER | TITLE

154 | Masked face recognition

SUMMARY DESCRIPTION

Masked face recognition is a technology that leverages machine learning and image processing techniques to identify or verify individuals even when their faces are partially obstructed by masks. This technology has become more significant due to the widespread use of face masks during the COVID-19 pandemic. Several methods, including Principal Component Analysis (PC, convolutional neural networks, support vector machines, and others, have been developed to improve the accuracy of masked face recognition. The technology can be applied in various sectors such as security, healthcare, and education, where it can be used in video surveillance equipment, to detect proper mask-wearing, for identity verification in automatic border control gates, secure login to electronic devices, and marking students' attendance. Masked face recognition is a novel extension of conventional face recognition methods. Unlike traditional techniques which struggle with occlusions like masks, new developments in this field aim to maintain high recognition accuracy even when faces are partially covered. What makes it new is the application of advanced algorithms and machine learning models, such as PCA, convolutional neural networks, and support vector machines, specifically designed to handle the challenges presented by mask occlusion. The technology also offers potential solutions to address new societal challenges brought about by the COVID-19 pandemic, such as ensuring proper mask usage and maintaining contactless identity verification systems. However, the novelty is still limited as the technology is in its early stages of development, with many algorithms and models undergoing testing and evaluation.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/ICASERT.2019.8934543 ; http://doi.org/10.1109/STI47673.2019.9068044 ; http://doi.org/10.1109/IJCB52358.2021.9484337 ; http://doi.org/10.1007/s11760-021-02050-w ; http://doi.org/10.1109/FG52635.2021.9666792 ; http://doi.org/10.1007/9

NUMBER | TITLE

159 | Privacy-preserving machine learning

SUMMARY DESCRIPTION

Privacy-preserving machine learning is a technology that enables the training of predictive models on large amounts of data while maintaining the privacy of the data contributors. It employs techniques such as Federated Learning (FL), two-party computation (2PC), and differential privacy to ensure that the local training data is kept confidential even when used to build shared models. The technology is particularly relevant in fields where privacy is paramount, such as healthcare, education, and finance. It can also be used to enhance efficiency and accuracy in deep learning implementations, enable secure summation of user-held data vectors, and aid in disease diagnosis in agriculture by identifying and classifying disease patterns. The novelty of privacy-preserving machine learning lies in its ability to maintain data privacy while allowing for collaborative model training. Unlike traditional machine learning approaches that require data to be centralized, this technology enables decentralized learning, reducing the risk of privacy breaches. It also incorporates mechanisms to protect against targeted attacks, a challenge that most existing technologies have not adequately addressed. Furthermore, it introduces innovative frameworks, such as the multi-task discriminator in Generative adversarial networks (GANs), to enhance privacy. Additionally, it presents solutions for privacy-preserving linear and logistic regressions that are significantly faster than existing implementations. By integrating the hardware latency of the cryptographic building block into the neural architecture search loss function, it also enhances energy efficiency and reduces latency in deep learning. The technology also enables the training of neural networks in a privacy-preserving manner, a feature that has not been implemented before.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/SP.2017.12 ; http://doi.org/10.1145/3133956.3133982 ; http://doi.org/10.1109/INFOCOM.2019.8737416 ; http://doi.org/10.1109/FOCS52979.2021.00096 ; http://doi.org/10.1109/SP46215.2023.10179400 ; http://doi.org/10.1109/INCET57972.2023.

NUMBER | TITLE

166 | Self sovereign identity

SUMMARY DESCRIPTION

Self Sovereign Identity (SSI) is an emerging technology that allows individuals to control, access, and share their personal data. It is a decentralized digital identification system that is often linked with blockchain or Distributed Ledger Technology (DLT). SSI is based on the principle of granting individuals the right to self-manage their data, which is shared with services. It is user-centric and privacy-friendly, providing a more secure alternative to traditional user authentication processes like username and password, which are notorious for security breaches. Potential applications of SSI span across various sectors, including healthcare data-sharing, vehicular networks, smart cities, web services, and border politics and migration management. For instance, in healthcare, SSI can help reconcile patient data across various providers, while in vehicular networks, it can ensure confidentiality, authentication, and integrity of vehicle users' identity and their data. The novelty of SSI lies in its decentralized and user-centric approach to identity management, which contrasts with traditional centralized systems. The conventional systems are not only susceptible to security breaches but also limit user controls over their data. SSI, on the other hand, empowers individuals with control and ownership of their data, enhancing privacy and security. By leveraging DLT or blockchain technology, SSI offers a transparent, tamper-proof, and traceable system, which is particularly advantageous for application domains that demand high data integrity and security. Furthermore, SSI is adaptable to a wide range of applications, from smart cities to vehicular networks, indicating its versatility and potential for widespread adoption. Despite its promising prospects, SSI is still an embryonic technology with challenges to overcome, such as the need for a systematic proof system for IoT applications and the exploration of its full potential for web services.

SOURCE

TIM
TIM analytics
http://doi.org/10.1016/j.giq.2020.101493 ; http://doi.org/10.1080/14650045.2020.1823836 ; http://doi.org/10.1109/JIOT.2022.3145089 ; http://doi.org/10.1109/Blockchain55522.2022.00077 ; http://doi.org/10.1007/978-3-031-21229-1_34 ; http://doi.org/10.1109/D

NUMBER | TITLE

394 | Face privacy protection scheme by security-enhanced encryption structure and nonlinear dynamics

SUMMARY DESCRIPTION

A new face privacy protection scheme enhances secure communication by integrating face detection with a chaotic partition permutation technique. Using edge detection to identify facial features as encryption objects, this method generates a secret key based on the image's hash value, feeding it into a chaotic system to produce pseudo-random sequences. Two chaotic systems enable multiple encryption steps, with the initial key derived from both image hash functions and external parameters. Experimental results show this approach provides robust encryption and withstands typical attack methods, making it a promising solution for privacy protection in secure facial data transmission.

SOURCE

Project team
Science Direct
https://www.sciencedirect.com/science/article/pii/S258900422401993X

NUMBER | TITLE

407 | WebXR allowing for the creation of digital nation-states

SUMMARY DESCRIPTION

A new system with unified login and WebXR could become the bedrock of a new generation of digital engagement. WebXR (Web application programming interface) is set to transform how users, developers, and creators engage with virtual environments. It offers a frictionless, universal platform where anyone with a device that supports a web browser — whether that's a PC, mobile phone, or VR headset — can seamlessly engage in immersive experiences through a simple URL. This could also open up opportunities for building digital sovereignty. The nation-state model is built on the concept of unified governance — centralised rules and structures that create consistency and a sense of identity for its citizens and users. Similarly, in the world of digital platforms, a unified login system serves as the foundation for building digital sovereignty. Just as a unified national ID allows citizens to access services and engage with their government, a unified login system allows users to access a broad range of services within a digital ecosystem with one credential.

The benefits of such a system are manifold. Firstly, it removes the friction associated with managing multiple accounts across various services. Users gain immediate access to multiple areas of a platform, with a consistent experience across devices. Digital sovereignty is a step toward breaking down the barriers that have traditionally limited people to operating within physical borders or disconnected digital ecosystems. When a user can move effortlessly through multiple virtual worlds with a single identity, the potential for building thriving, borderless communities becomes immense. 'WebXR is valued as one of the most promising technologies for universal access to virtual and augmented reality. It gives developers the ability to reach audiences they couldn't previously access, on any device, without needing to convince them to install an app," notes Tony Parisi, a thought leader in immersive technologies.

SOURCE

Project team

The Nation-state Playbook: How a Unified Login System and WebXR Can Shape the Future of Digital Communities https://medium.com/@bennydoda83/the-nation-state-playbook-how-a-unified-login-system-and-webxr-can-shape-the-future-of-digital-cdbfa59ec59f

NUMBER | TITLE

410 | digital identity wallet

SUMMARY DESCRIPTION

The EU Digital Identity Wallet is a collaboration between the EU institutions and the Member States. Together, they are working across two main streams of work to make EU Digital Identity Wallets a reality that can be used by citizens, residents, and businesses across Europe. EU Digital Identity Wallets will enable users to access online services, store and share digital documents, and create binding signatures. EU Digital Identity Wallets are the European Union's response to the challenges of digital identification. Every EU Member State will offer its own wallet app, built to the same specifications, to all citizens, residents and businesses in the next few years. Each version of the wallet will be interoperable and will work wherever you are in Europe. With this, the digital documents digital documents will be:

Secure: Strong cryptographic encryption keeps your data safe.

Privacy-preserving: Private by design; only necessary information is shared.

Cross-border: Many digital documents will be accepted wherever you are in Europe.

SOURCE

Project team

A digital ID and personal digital wallet https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

NUMBER | TITLE

413 | Generative Adversarial Network

SUMMARY DESCRIPTION

Among the various deepfake creation methods, Generative Adversarial Network (GAN) is a technology that has shown remarkable results, creating manipulations that are difficult to distinguish from original content. GANs are machine learning (ML) models in which two neural networks - a generator and a discriminator - compete with each other to make predictions that are as accurate as possible or, in the case of deepfake generation, to produce the most realistic result. In addition to the question of content manipulation, there is also the concern that deepfake content could promote disinformation and have a negative impact on people's opinions, with potential political and social consequences. Nude or otherwise offensive depictions of people, hoaxes and financial fraud can also be produced through video manipulation. Additionally, the ability to impersonate other people, by swapping faces in photos and videos, increases the risk of unauthorised access to services or premises.

SOURCE

Project team
TechSonar 2023-2024 report
https://www.edps.europa.eu/system/files/2023-12/23-12-04_techsonar_23-24_en.pdf

NUMBER | TITLE

444 | Adverserial wearables

SUMMARY DESCRIPTION

This innovative t-shirt, designed to block facial recognition technology, offers a novel approach to personal privacy in a digital age where surveillance is ubiquitous. Created by a team of Italian researchers, the garment features complex patterns that disrupt AI algorithms, effectively preventing facial recognition software from identifying the wearer. This visually unique design marks a significant step in counter-surveillance fashion, blending functionality with aesthetics to protect individual privacy in public spaces. As privacy concerns grow, this anti-surveillance clothing could pioneer new trends in wearable technology, giving individuals a creative and effective tool to maintain their anonymity.

SOURCE

Experts
https://www.dazeddigital.com/science-tech/article/49183/1/this-t-shirt-blocks-facial-recognition-technology

NUMBER | TITLE

446 | SecureNed

SUMMARY DESCRIPTION

The SecureNed application is based on the Privacy Enhancing Technology MPC with Secret Sharing. While this technology is already known, the wider adoption of this technology, specifically in the cybersecurity domain, could/should receive more attention. SecureNed enables organizations to securely share information about cybersecurity incidents; the receiving organization (NCSC - the Dutch National Cyber Security Centre) is not able to identify and link incidents to organizations, but is able to perform analyses and overviews based on the information submitted. This helps to mitigate hesitations from organizations to report cyber incidents - no company wants to have their cyber incidents leaked to the public, while they understand how important it is to actually report.

SOURCE

Experts
https://mpc.cs.berkeley.edu/posts/Crypto-SecureNed/

NUMBER | TITLE

448 | Humanoid robots

SUMMARY DESCRIPTION

Humanoid robots are robots that resemble and act like humans. Typically engineered to imitate authentic human expressions, interactions and movements, these robots are often outfitted with an array of cameras, sensors and AI and machine learning technologies. Humanoid robots could be used in different kinds of tasks and services for eg. in healthcare, production and customer services.

SOURCE

Experts
https://builtin.com/robotics/humanoid-robots

Subcluster A5 – Internet, browsing and VPNs

List of Signals

- 57 | Enhancing detection of suspicious phishing attacks with an optimal feature vectorization algorithm and supervised machine learning
- 63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges
- 77 | Oblivious proxies
- 82 | The Onion Router (TOR)
- 85 | Simple PIR and Double PIR
- 88 | AI integration into VPN
- 89 | Quantum-Safe VPNs
- 90 | Decentralised VPNs
- 91 | Multi-cloud VPNs
- 93 | Zero Trust Network Access (ZTNA)
- 105 | Mix network
- 107 | Limited disclosure technology
- 116 | DC Network
- 142 | DNS-over-HTTPS
- 388 | Anti-detect browser
- 393 | A bidirectional reversible and multilevel location privacy protection method based on attribute encryption
- 398 | Chrome switching to NIST-approved ML-KEM quantum encryption
- 401 | Unveiling the Dark Web: How Privacy Coins Fuel the Trade of Criminal Material Online
- 407 | WebXR allowing for the creation of digital nation-states
- 408 | New method to combine conventional internet with the quantum internet
- 409 | New security protocol shields data from attackers during cloud-based computation
- 411 | Internet of Behaviour (IoB)
- 415 | Session - new fully encrypted messenger app is serious about privacy
- 417 | Anti-tracking tools
- 418 | I2P Network
- 421 | Solid
- 426 | ASMesh
- 446 | SecureNed

NUMBER | TITLE
57 | Enhancing detection of suspicious phishing attacks with an optimal feature vectorization algorithm and supervised machine learning
SUMMARY DESCRIPTION
The dynamic and sophisticated nature of phishing attacks, coupled with the relatively weak anti-phishing tools, has made phishing detection a pressing challenge. In light of this, new gaps have emerged in phishing detection, including the challenges and pitfalls of existing phishing detection techniques. To bridge these gaps, this study aims to develop a more robust, effective, sophisticated, and reliable solution for phishing detection through the optimal feature vectorization algorithm (OFVA) and supervised machine learning (SML) classifiers.
SOURCE
Project team Frontiers in computer science https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1428013/full

NUMBER | TITLE

63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges

SUMMARY DESCRIPTION

Sixth-generation (6G) mobile networks will have to cope with diverse threats on a space-air-ground integrated network environment, novel technologies, and an accessible user information explosion. However, for now, security and privacy issues for 6G remain largely in concept. This survey provides a systematic overview of security and privacy issues based on prospective technologies for 6G in the physical, connection, and service layers, as well as through lessons learned from the failures of existing security architectures and state-of-the-art defenses. Two key lessons learned are as follows. First, other than inheriting vulnerabilities from the previous generations, 6G has new threat vectors from new radio technologies, such as the exposed location of radio stripes in ultra-massive MIMO systems at Terahertz bands and attacks against pervasive intelligence. Second, physical layer protection, deep network slicing, quantum-safe communications, artificial intelligence (AI) security, platform-agnostic security, real-time adaptive security, and novel data protection mechanisms such as distributed ledgers and differential privacy are the top promising techniques to mitigate the attack magnitude and personal data breaches substantially.

SOURCE

Project team
Professional association
https://ieeexplore.ieee.org/document/9524814

NUMBER | TITLE

77 | Oblivious proxies

SUMMARY DESCRIPTION

Oblivious proxies divide data up between two entities. Their goal is to allow the user of an app or website to communicate with a company's servers without the company learning who they are. But all communication over the internet uses an identifier known as an IP address, which can aid in the identification of an individual or household. Let's say the same ice cream shop wants to allow the users of their app to vote on a new flavor to introduce. To encourage true honesty in the votes, the ice cream shop needs to ensure it can't identify the votes users cast. Using an oblivious proxy, the app can encrypt a user's vote so it's only readable by the ice cream shop, then send it to a trustworthy third party. The trustworthy third party can then forward the encrypted vote along, with the user's IP address removed, at which point the ice cream shop can decrypt and view the vote without knowing who sent it (the winner was Proxy Road).

SOURCE

Project team
Keeping Your Privacy Enhancing Technology (PET) Promises
https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/keeping-your-privacy-enhancing-technology-pet-promises

NUMBER | TITLE

82 | The Onion Router (TOR)

SUMMARY DESCRIPTION

An onion router is a software and open network that allows users to access the internet anonymously. It uses layered encryption to send data packets through multiple nodes in the network, removing one layer of encryption at each node. This ensures that the data remains encrypted while the sender's identity is protected. The onion routing process in Tor makes it a popular method for maintaining online anonymity.

SOURCE

Project team
Science Direct
https://www.sciencedirect.com/topics/computer-science/onion-router

NUMBER | TITLE

85 | Simple PIR and Double PIR

SUMMARY DESCRIPTION

Searching the internet can reveal information a user would rather keep private. New research enables users to search for information without revealing their queries, based on a method that is 30 times faster than comparable prior techniques. Moreover, it is driven by a simple algorithm that would be easier to implement than the more complicated approaches from previous work.Their technique could enable private communication by preventing a messaging app from knowing what users are saying or who they are talking to. It could also be used to fetch relevant online ads without advertising servers learning a users' interests.

MIT researchers developed a protocol, known as Simple PIR, in which the server performs much of the underlying cryptographic work in advance, before a client even sends a query. This preprocessing step produces a data structure that holds compressed information about the database contents, and which the client downloads before sending a query.In a sense, this data structure is like a hint for the client about what is in the database.To reduce the size of the hint, the researchers developed a second technique, known as Double PIR, that basically involves running the Simple PIR scheme twice. This produces a much more compact hint that is fixed in size for any database.

SOURCE

Project team

A faster way to preserve privacy online

https://news.mit.edu/2022/online-information-user-data-privacy-1207

NUMBER | TITLE

88 | AI integration into VPN

SUMMARY DESCRIPTION

With AI disrupting every industry in 2024, VPNs are not the exception. In fact, AI-driven functionalities are set to revolutionize the industry. Take, for instance, machine learning algorithms that already optimize routing, reduce latency, and dynamically allocate resources. In such a sense, AI can predict server loads and route traffic efficiently. And this is only the tip of the iceberg, as AI can also perform behavioral analysis and adaptive encryption to enhance VPN performance..

SOURCE

Project team

The Future of VPN Technology: Emerging Trends & Innovations

https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html

NUMBER | TITLE

89 | Quantum-Safe VPNs

SUMMARY DESCRIPTION

Unlike traditional encryption methods, quantum computers can break into existing cryptographic algorithms without compromising data security. A quantum-safe VPN is a network security measure that uses Post Quantum Cryptography (PQC) to enhance encryption levels. PQC uses unique algorithms to encode data, which makes it more difficult for quantum computers to break encryption. A quantum-safe VPN can create an encrypted tunnel between the sender and receiver. Thus, it will safeguard the data.

SOURCE

Project team

The Future of VPN Technology: Emerging Trends & Innovations; Quantum-safe VPN to safeguard encrypted data

https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html; https://www.tcs.com/insights/topics/cybersecurity-topic/article/quantum-safe-vpn

NUMBER | TITLE
90 | Decentralised VPNs
SUMMARY DESCRIPTION
Classical VPNs rely on centralized servers. While decentralized VPNs operate through distributed network nodes, often used in the blockchain. Furthermore, decentralized VPNs provide an array of benefits. First, it is improved security as such technology reduces the risk of a single point of failure. Second, it is a user-operated node, meaning individuals contribute their idle bandwidth and become a part of the network. The key components of a decentralized VPN include: Blockchain Technology; Smart Contracts; Encryption.
SOURCE
Project team The Future of VPN Technology: Emerging Trends & Innovations; Decentralized VPN Services: The Future of Data Privacy Protection https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html; https://www.linkedin.com/pulse/decentralized-vpn-services-future-data-privacy-robiul-hossain-ioe7c/

NUMBER | TITLE
91 | Multi-cloud VPNs
SUMMARY DESCRIPTION
Thanks to the pandemic, there has been a shift to remote work involving large-scale clout migrations that combine infrastructure for scalability, cost-effectiveness, and flexibility. As a vivid example, large organizations continue to adopt up-to-cloud strategies from diverse providers, including AWS, Azure, Google Cloud, and others. Thus, cloud communication has become paramount. Enterprises realized they needed to have seamless connectivity across platforms without compromising security. As such, multi-cloud VPNs support various cloud-native protocols, making the technology versatile and adaptable.
SOURCE
Project team The Future of VPN Technology: Emerging Trends & Innovations https://www.cybersecurityintelligence.com/blog/the-future-of-vpn-technology-emerging-trends-and-innovations-7572.html

NUMBER | TITLE
93 | Zero Trust Network Access (ZTNA)
SUMMARY DESCRIPTION
This model assumes that no one, whether inside or outside the organization, can be trusted by default. It enforces strict access controls and verifies every user, device, and application attempting to connect to the network. ZTNA solutions provide organizations with granular access controls (users are only granted access to the specific resources they need to perform their job, reducing the attack surface and limiting lateral movement for potential attackers); Continuous Verification (ZTNA solutions continuously verify the trustworthiness of users and devices throughout their session); Application-Centric Security (ZTNA focuses on securing applications rather than the network itself); Simplicity and Scalability (Implementing ZTNA can be more straightforward and scalable compared to managing and maintaining complex VPN configurations. It aligns well with modern workforces that are increasingly remote and mobile.). While VPNs grant access to an entire network, ZTNA - only to specific services or applications. Related area - secure access services edge concept.
SOURCE
Project team Rethinking Network Security: Why Zero Trust is the Future, and VPNs are the Past https://www.bdo.com/insights/digital/rethinking-network-security-why-zero-trust-is-the-future-and-vpns-are-the-past; https://greenmethod.net/blogs/the-future-of-zero-trust-network-access/

NUMBER | TITLE
105 | Mix network
SUMMARY DESCRIPTION
Mix network is a routing protocol that enhances user communication privacy over the internet. As a privacy-enhancing technology, it is designed to route and obfuscate messages, so the destination and source would be unknown. This is achieved by mixing and routing the messages through many servers called 'mix nodes' or 'mixers'. These servers receive encrypted data, then mix them with other bathes of incoming messages, finally forwarding them in random order. Due to the procedure, it is challenging to trace the sender or destination of these messages. It could be used for email communications, anonymous messaging, file sharing, financial transactions, anonymous web browsing.
SOURCE
Project team Mix network https://nordvpn.com/cybersecurity/glossary/mix-network/

NUMBER | TITLE
107 | Limited disclosure technology
SUMMARY DESCRIPTION
Limited disclosure technology is designed to protect individuals' privacy by allowing them to share only enough personal information with service providers to complete an interaction or transaction. The technology is also designed to limit tracking and correlation of users' interactions with these third parties. Limited disclosure uses cryptographic techniques and allows users to retrieve data that is vetted by a provider, to transmit that data to a relying party, and have these relying parties trust the authenticity and integrity of the data.
SOURCE
Project team Limited Disclosure Technology https://www.gartner.com/en/information-technology/glossary/limited-disclosure-technology

NUMBER | TITLE
116 | DC Network
SUMMARY DESCRIPTION
David Chaum's DC (Dining Cryptographer) network protocol is an anonymous communication protocol, which, even though it cannot be easily used in practice, is still very interesting from a scientific perspective. It provides unconditional sender anonymity, recipient anonymity, and unobservability, even if we assume a global adversary who can observe all communication in the network. Hence, it can guarantee the strongest anonymity properties of all known anonymous communication protocols. DC nets are based on binary superposed sending
SOURCE
Project team Computer and Information Security Handbook, Ch. 43- Privacy-Enhancing Technologies https://www.sciencedirect.com/science/article/pii/B978012394397200043X#s0060; https://arxiv.org/pdf/2103.17091; https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_194

NUMBER | TITLE

142 | DNS-over-HTTPS

SUMMARY DESCRIPTION

DNS-over-HTTPS (DoH) is a protocol designed to enhance the privacy and security of Internet users by encrypting Domain Name System (DNS) traffic, preventing eavesdropping and data manipulation. This is achieved by transmitting DNS data over the HyperText Transfer Protocol Secure (HTTPS), which thwarts potential attacks such as Man-in-the-Middle (MitM). Despite its potential benefits, DoH also poses challenges as it could hinder network administrators from detecting suspicious network traffic produced by malware and malicious tools. To address these issues, machine learning techniques and explainable AI solutions are being implemented to detect and classify DoH attacks, as well as identify malicious DoH traffic and tunneling activities. The novelty of DoH lies in its encryption of DNS traffic, a significant departure from traditional DNS protocols that have been vulnerable to various security issues. While efforts to secure DNS traffic have previously been made (e.g., DNS over TLS), DoH offers additional advantages by leveraging the secure and widely adopted HTTPS protocol. However, it's also worth noting that encryption does not completely prevent traffic analysis or DNS-based censorship. Even so, emerging technologies like DNS over QUIC (DoQ) promise to further enhance encrypted DNS with reduced latency. The integration of machine learning methods for detecting malicious DoH traffic and for classifying DoH attacks signifies another innovative approach in this field. Despite these advancements, the technology is still evolving and ongoing research is needed to address its potential drawbacks and enhance its effectiveness.

SOURCE

TIM
TIM analytics
http://doi.org/10.14722/ndss.2020.24301 ; http://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00026 ; http://doi.org/10.1007/978-3-030-98785-5_24 ; http://doi.org/10.1109/TIFS.2022.3183390 ; http://doi.org/10.1145/3517745.3561445 ; http://doi.

NUMBER | TITLE

388 | Anti-detect browser

SUMMARY DESCRIPTION

An anti-detection browser is a special type that transfers your data to the websites in a modified form. Such browsers send a completely different set of parameters about your device and location to the website (browser version, IP, language and much more). This artificially generated data set is called a browser fingerprint.
Thus, the service helps you remain anonymous and bypass some restrictions on ad platforms linked to account authenticity. As a rule, these tools are helpful when dealing with Facebook and other advertising platforms.

SOURCE

Project team
What is an anti-detect browser and why is it necessary for affiliate marketers?
https://richads.com/blog/what-is/anti-detect-browser/; https://multilogin.com/antidetect/glossary/anti-fingerprint-browser/

NUMBER | TITLE

393 | A bidirectional reversible and multilevel location privacy protection method based on attribute encryption

SUMMARY DESCRIPTION

A new bidirectional, reversible, and multilevel location privacy protection method using attribute-based encryption offers a sophisticated alternative to traditional privacy approaches like k-anonymity. Unlike rigid, all-or-nothing standards, this method enables flexible, layered privacy control tailored to user trust levels. By encrypting data with an access structure tree and adding hierarchical dummy information, users can adjust anonymization granularity as needed, allowing controlled de-anonymization. The attribute-based access control system manages decryption keys based on user attributes, streamlining key generation and distribution. This approach significantly enhances location data utility while preserving privacy, as demonstrated in tests where it effectively balances privacy with data quality, a challenge for existing methods.

SOURCE

Project team
National University of Sciences and Technology
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0309990

NUMBER | TITLE

398 | Chrome switching to NIST-approved ML-KEM quantum encryption

SUMMARY DESCRIPTION

Google is enhancing Chrome's post-quantum security by transitioning to the NIST-approved ML-KEM (Module Lattice Key Encapsulation Mechanism) for TLS encryption, replacing the experimental Kyber system. This switch aims to bolster protection against potential quantum computer attacks and to prevent store-now-decrypt-later threats. Unlike Kyber, ML-KEM is fully standardized, receiving NIST endorsement in August 2024. Although the technical differences between Kyber and ML-KEM are minor, they are incompatible, necessitating the change. Google's shift also addresses the efficiency challenge: post-quantum cryptographic exchanges like Kyber significantly increase data sizes, risking network performance. Chrome 131, set for release on November 6, 2024, will exclusively support ML-KEM. Server operators are encouraged to offer dual support temporarily to aid the transition, while a DNS-based IETF proposal could streamline algorithm selection in future. Users on Chrome's development channels can access ML-KEM ahead of the official rollout.

SOURCE

Project team
Bleeping Computer
https://www.bleepingcomputer.com/news/security/chrome-switching-to-nist-approved-ml-kem-quantum-encryption/

NUMBER | TITLE

401 | Unveiling the Dark Web: How Privacy Coins Fuel the Trade of Criminal Material Online

SUMMARY DESCRIPTION

Privacy coins like Monero are increasingly implicated in the dark web's criminal economy, particularly in child sexual abuse material (CSAM) trade, according to Chainalysis's 2024 Crypto Crime Report. While Bitcoin is still commonly used for CSAM purchases, Monero's privacy features make it popular among vendors for laundering and concealing funds post-transaction. The report highlights Monero's use via instant exchangers—non-custodial, anonymous platforms that enable fast crypto exchanges without KYC verification, aiding CSAM vendors in hiding transaction trails.

Regulators have pressured exchanges like Binance to delist privacy coins, citing risks of money laundering and insufficient KYC and AML protections. However, blockchain analysis has also been a crime-fighting tool: in 2019, law enforcement leveraged Chainalysis to dismantle a major CSAM site, leading to arrests and victim rescues. The report underscores the dual nature of crypto: a tool for both privacy-focused crime and law enforcement breakthroughs.

SOURCE

Project team
Cryptonews
https://cryptonews.com/news/unveiling-the-dark-web-how-privacy-coins-fuel-the-trade-of-criminal-material-online/

NUMBER | TITLE

407 | WebXR allowing for the creation of digital nation-states

SUMMARY DESCRIPTION

A new system with unified login and WebXR could become the bedrock of a new generation of digital engagement. WebXR (Web application programming interface) is set to transform how users, developers, and creators engage with virtual environments. It offers a frictionless, universal platform where anyone with a device that supports a web browser — whether that's a PC, mobile phone, or VR headset — can seamlessly engage in immersive experiences through a simple URL. This could also open up opportunities for building digital sovereignty. The nation-state model is built on the concept of unified governance — centralised rules and structures that create consistency and a sense of identity for its citizens and users. Similarly, in the world of digital platforms, a unified login system serves as the foundation for building digital sovereignty. Just as a unified national ID allows citizens to access services and engage with their government, a unified login system allows users to access a broad range of services within a digital ecosystem with one credential.

The benefits of such a system are manifold. Firstly, it removes the friction associated with managing multiple accounts across various services. Users gain immediate access to multiple areas of a platform, with a consistent experience across devices. Digital sovereignty is a step toward breaking down the barriers that have traditionally limited people to operating within physical borders or disconnected digital ecosystems. When a user can move effortlessly through multiple virtual worlds with a single identity, the potential for building thriving, borderless communities becomes immense. 'WebXR is valued as one of the most promising technologies for universal access to virtual and augmented reality. It gives developers the ability to reach audiences they couldn't previously access, on any device, without needing to convince them to install an app," notes Tony Parisi, a thought leader in immersive technologies.

SOURCE

Project team

The Nation-state Playbook: How a Unified Login System and WebXR Can Shape the Future of Digital Communities
https://medium.com/@bennydoda83/the-nation-state-playbook-how-a-unified-login-system-and-webxr-can-shape-the-future-of-digital-cdbfa59ec59f

NUMBER | TITLE

408 | New method to combine conventional internet with the quantum internet

SUMMARY DESCRIPTION

Four researchers from the Institute of Photonics at Leibniz University Hannover have developed a new transmitter-receiver concept for transmitting entangled photons over an optical fiber. This breakthrough could enable the next generation of telecommunications technology, the quantum Internet, to be routed via optical fibers. The quantum Internet promises eavesdropping-proof encryption methods that even future quantum computers cannot decrypt, ensuring the security of critical infrastructure.

SOURCE

Project team

Physicists develop new method to combine conventional internet with the quantum internet
https://www.sciencedaily.com/releases/2024/08/240805134133.htm

NUMBER | TITLE

409 | New security protocol shields data from attackers during cloud-based computation

SUMMARY DESCRIPTION

Researchers developed a technique guaranteeing that data remain secure during multiparty, cloud-based computation. This method, which leverages the quantum properties of light, could enable organizations like hospitals or financial companies to use deep learning to securely analyze confidential patient or customer data.

SOURCE

Project team

New security protocol shields data from attackers during cloud-based computation
https://www.sciencedaily.com/releases/2024/10/241001142659.htm

NUMBER | TITLE

411 | Internet of Behaviour (IoB)

SUMMARY DESCRIPTION

The aim of IoB is to address how data collected can be interpreted from a human psychological and sociological perspective and how to use this understanding to influence or change human behaviour for various purposes, ranging from commercial interests to public policies.The Internet of Behaviour (IoB) represents a convergence of multiple disciplines: technology, data analytics, and behavioural psychology. It's an emerging field that extends beyond the data collection capabilities of the Internet of Things (IoT) to delve into the realm of behavioural science. IoB is increasingly becoming a cornerstone in our digital world. The Internet of Behaviour (IoB) extends its reach by collecting and analysing data from a wide array of sources, including IoT devices, social media platforms, and websites. This comprehensive scope of data collection raises significant ethical, security, and privacy concerns that must be addressed meticulously.IoB data, encompassing sensitive information like bank codes and personal habits, present lucrative targets for cybercriminals. Risks include potential cyber-attacks, identity theft, ransomware, money laundering, and sophisticated phishing attempts.

SOURCE

Project team
What is the Internet of Behaviour? A Comprehensive Guide
https://www.sovtech.com/blog/what-is-the-internet-of-behaviour-a-comprehensive-guide

NUMBER | TITLE

415 | Session - new fully encrypted messenger app is serious about privacy

SUMMARY DESCRIPTION

Session is an end-to-end encrypted messenger that minimizes sensitive metadata, designed and built for people who want absolute privacy and freedom from any form of surveillance. With Session, there's no phone number, account name, or footprint to be had. Session uses an onion routing network to ensure you leave no trace, so it's simply impossible for anyone to create a profile based on metadata or account information. All accounts are completely anonymous, and zero data is collected, which means there's absolutely nothing to leak.

SOURCE

Project team
This new fully encrypted messenger app is serious about privacy
https://www.zdnet.com/article/this-new-fully-encrypted-messenger-app-is-serious-about-privacy/;
https://getsession.org/

NUMBER | TITLE

417 | Anti-tracking tools

SUMMARY DESCRIPTION

Websites track your behavior to sell to advertisers — and scammers. Anti-tracking and ad blocking tools can help increase your online privacy and safety. Here are some of the benefits of blocking tracking software online: Hides your browsing history from websites; Stops companies from tracking your personal information; Prevents you from receiving personalized ads; Can help keep you safe from identity theft; Protects you from data brokers. The 8 Best Anti-Tracking Software Providers in 2024

- Aura
- Total Adblock Plus
- DuckDuckGo
- uBlock Origin
- Ghostery
- Brave browser
- AVG AntiTrack
- Privacy Badger

SOURCE

Project team
The 8 Best Anti-Tracking Software for Online Privacy (2024)
https://www.aura.com/learn/best-anti-tracking-software

NUMBER | TITLE

418 | I2P Network

SUMMARY DESCRIPTION

I2P (known as the Invisible Internet Project - founded in 2003) is a low-latency network layer that runs on a distributed network of computers across the globe. It is primarily built into applications such as email, Internet Relay Chat (IRC) and file sharing. I2P works by automatically making each client in the network a node, through which data and traffic are routed. These nodes are responsible for providing encrypted, one-way connections to and from other computers within the network. I2P is an enclosed network that runs within the Internet infrastructure (referred to as the clearnet in this paradigm). Unlike VPNs and Tor, which are inherently “outproxy” networks designed for anonymous and private communication with the Internet, I2P is designed as a peer-to-peer network. This means it has very little to no communication with the Internet. It also means each node in I2P is not identified with an Internet Protocol (IP) address, but with a cryptographic identifier. A node in the I2P network can be either a server that hosts a darknet service (similar to a website on the Internet), or a client who accesses the servers and services hosted by other nodes. Each client/server in I2P is automatically a relay node. Whether data is routed through a specific node is normally bandwidth dependent.

SOURCE

Project team
Introduction to Tor and I2P
https://tlu.tarilabs.com/protocols/intro-to-tor-and-i2p#what-is-i2p

NUMBER | TITLE

421 | Solid

SUMMARY DESCRIPTION

Solid is an open standard for structuring data, digital identities, and applications on the Web.
Solid aims to support the creation of the Web as Sir Tim Berners-Lee originally envisioned it when he invented the Web at CERN in 1989. Tim sometimes refers to Solid as “the web - take 3” — or Web3.0 — because Solid integrates a new layer of standards into the Web we already have. The goal of Solid is for people to have more agency over their data. Solid is a specification that lets people store their data securely in decentralized data stores called Pods. Pods are like secure personal web servers for your data.
Entities control access to the data in their Pod. Entities decide what data to share and with whom (be those individuals, organizations, applications, etc.), and can revoke access at any time.

SOURCE

Project team
Solid
https://solidproject.org/about; https://www.cmswire.com/digital-experience/what-is-solid-project-a-detailed-exploration/

NUMBER | TITLE

426 | ASMesh

SUMMARY DESCRIPTION

The majority of secure messengers have single, centralized service providers that relay ciphertexts between users to enable asynchronous communication. However, in some scenarios such as mass protests in censored networks, relying on a centralized provider is fatal. Mesh messengers attempt to solve this problem by building ad hoc networks in which user clients perform the ciphertext-relaying task. Yet, recent analyses of widely deployed mesh messengers discover severe security weaknesses (Albrecht et al. CT-RSA'21 & USENIX Security'22).
To support the design of secure mesh messengers, we provide a new, more complete security model for mesh messaging. Our model captures forward and post-compromise security, as well as forward and post-compromise anonymity, both of which are especially important in this setting. We also identify novel, stronger confidentiality goals that can be achieved due to the special characteristics of mesh networks (e.g., delayed communication, distributed network and adversary).
Finally, we develop a new protocol, called ASMesh, that provably satisfies these security goals. For this, we revisit Signal's Double Ratchet and propose non-trivial enhancements. On top of that, we add a mechanism that provides forward and post-compromise anonymity. Thus, our protocol efficiently provides strong confidentiality and anonymity under past and future user corruptions. Most of our results are also applicable to traditional messaging. We prove security of our protocols and evaluate their performance in simulated mesh networks. Finally, we develop a proof of concept implementation.

SOURCE

Project team
ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet
https://dl.acm.org/doi/10.1145/3576915.3616615

NUMBER | TITLE
446 | SecureNed
SUMMARY DESCRIPTION
The SecureNed application is based on the Privacy Enhancing Technology MPC with Secret Sharing. While this technology is already known, the wider adoption of this technology, specifically in the cybersecurity domain, could/should receive more attention. SecureNed enables organizations to securely share information about cybersecurity incidents; the receiving organization (NCSC - the Dutch National Cyber Security Centre) is not able to identify and link incidents to organizations, but is able to perform analyses and overviews based on the information submitted. This helps to mitigate hesitations from organizations to report cyber incidents - no company wants to have their cyber incidents leaked to the public, while they understand how important it is to actually report.
SOURCE
Experts https://mpc.cs.berkeley.edu/posts/Crypto-SecureNed/

Subcluster A6 – Encryption

List of Signals

- 16 | PrivDNN
- 20 | Honey encryption
- 38 | Quantum-resistant digital signatures
- 71 | Zero Knowledge Proof System
- 73 | Private Set Intersection
- 76 | Differential Privacy
- 81 | Trusted Execution Environments
- 84 | PAC privacy
- 85 | Simple PIR and Double PIR
- 86 | Keyed Cryptographic Hashing
- 116 | DC Network
- 125 | Adversarial defence
- 127 | Attribute based searchable encryption
- 133 | Colour image encryption algorithm
- 153 | Machine unlearning
- 159 | Privacy-preserving machine learning
- 419 | AI TRISM
- 422 | Verifiable computing
- 425 | End-to-End Encrypted Cloud Storage
- 429 | Data privacy vault
- 445 | Secure LLM querying
- 447 | Ma3tch
- 449 | New cryptographic primitives
- 450 | Indistinguishability obfuscation
- 453 | Privacy Enhancing Technologies in Data Spaces
- 458 | Secure Multi-Party Computation
- 460 | Federated learning methodologies
- 462 | Confidential Computing

NUMBER | TITLE
16 | PrivDNN
SUMMARY DESCRIPTION
Researchers from the University of Kansas present a novel solution to privacy-preserving deep learning, namely, PrivDNN, which (1) offloads the computation to the user side by sharing an encrypted deep learning model with them, (2) significantly improves the efficiency of DNN evaluation using partial DNN encryption, (3) ensures model accuracy and model privacy using a core neuron selection and encryption scheme. Experimental results show that PrivDNN reduces privacy-preserving DNN inference time and memory requirement by up to 97% while maintaining model performance and privacy.
SOURCE
Project team Proceedings on Privacy Enhancing Technologies https://petsymposium.org/popets/2024/popets-2024-0089.pdf

NUMBER | TITLE

20 | Honey encryption

SUMMARY DESCRIPTION

One of the emerging encryption mechanisms used against brute force attacks is honey encryption, which deceives the attacker into believing that he or she has hacked the codebase.
A brute force attack relies on repeated decryption with randomly generated keys. What honey encryption does is that it produces ciphertext, which, on decryption with the wrong key, yields a plausible looking yet incorrect plaintext encryption keys. This will make it harder for the attacker to know if he/she has guessed correctly or not.
Ari Juels from Cornell Institute and Thomas Ristenpart from the University of Wisconsin developed honey encryption in 2014. The honey encryption mechanism is used to protect private data in real-world applications like credit card transactions and text messaging.
Recent implementations have seen its application in protection of cloud storage and big data, offering a deceptive layer of security that confounds potential attackers with misleading data.

SOURCE

Project team
Concentric AI
https://concentric.ai/advances-in-encryption-technology/
https://www.iacr.org/archive/eurocrypt2014/84410181/84410181.pdf

NUMBER | TITLE

38 | Quantum-resistant digital signatures

SUMMARY DESCRIPTION

Quantum-resistant digital signatures are cryptographic techniques designed to securely sign digital transactions even in the face of potential quantum computing attacks. As the development of quantum computers advances, traditional cryptographic methods, such as Elliptic Curve Digital Signature Algorithm (ECDSA), become vulnerable due to their reliance on integer factorization and discrete logarithms, which quantum computers can solve efficiently. Quantum-resistant signatures address this vulnerability, offering protection even if traditional methods are compromised. These signatures are critical in a range of applications such as securing Bitcoin transactions, Internet of Things (IoT) software updates, electronic information transmission in e-commerce, e-voting, and e-learning, as well as in securing the integrity of electronic documents in transport and logistics. Recent developments have focused on designing efficient quantum-resistant signatures using Multivariate Public Key Cryptography (MPKC), hash-based algorithms, and lattice ciphers. Implementation challenges, such as large key and signature sizes, are being addressed through innovative solutions like using application-specific blockchain structures and interplanetary file systems. Quantum-resistant signatures are also being incorporated into privacy-preserving data sharing schemes for medical information and payment channels for Bitcoin.

SOURCE

Project team
Signals for quantum
https://www.timanalytics.eu/TimTechPublic/dashboard/index.jsp#/space/s_2261?ds=303574

NUMBER | TITLE

71 | Zero Knowledge Proof System

SUMMARY DESCRIPTION

Zero Knowledge Proof (ZKP) is a method that allows the owner of sensitive data to prove a statement about this data without having to reveal it. It is cryptographic algorithms which allows a prover to convince a distrusting verifier that a certain statement is true. It is an increasingly common way privacy is achieved on public blockchain networks. ZKP can be used as part of a 'zero-trust' framework which assumes that every person and device, both internal and external to the network, could be a threat due to malicious behavior or simple incompetence. To mitigate threats, zero-trust systems require users and devices to be authenticated, authorized, and continuously validated before access to resources is granted.

SOURCE

Project team
https://eprint.iacr.org/2023/122.pdf

NUMBER | TITLE

73 | Private Set Intersection

SUMMARY DESCRIPTION

Private Set Intersection (PSI) allows two (or more) distrusting parties with respective input sets S1 and S2 to securely learn their intersection, i.e. S1 ∩ S2, without revealing the non-intersecting elements to the other party.For example, if party 1 has S1 = {a, b, d} and party 2 has S2 = {b, c, e} then both parties will learn that they have b in common in their sets. At the same time, party 2 will not learn that party 1 also had a, d in its input set and vice-versa for c, e. Highly efficient PSI protocols have been developed recently and some, such as the one developed by Chen et al. found applications in industry.

SOURCE

Project team
SoK: Privacy-Enhancing Technologies in Finance
https://eprint.iacr.org/2023/122.pdf

NUMBER | TITLE

76 | Differential Privacy

SUMMARY DESCRIPTION

Differential privacy is a state-of-the-art definition of privacy used when analyzing large data sets. It guarantees that adversaries cannot discover an individual within the protected data set by comparing the data with other data sets. In this context, an adversary is a person or organization attempting to glean information about specific individuals within a data set. No matter the adversary, differential privacy is achieved using mathematics, artificial intelligence, intelligent control, machine learning, and other technologies. It is a technique to compute add noise to outcomes of algorithms such that leakage about the inputs of the computation is minimized. The level of the noise is calibrated such that mathematical guarantees about the privacy of the inputs can be given.

SOURCE

Project team
SoK: Privacy-Enhancing Technologies in Finance
https://eprint.iacr.org/2023/122.pdf

NUMBER | TITLE

81 | Trusted Execution Environments

SUMMARY DESCRIPTION

A TEE is an isolated compute space, separate from its host instance, that relies on hardware-based encryption to protect both data in memory and application-level code. Entities outside a TEE, including the host instance, are unable to see or alter the code or data used during execution. A program running inside a TEE is cryptographically attested to be the program that is intended to run. (Mé nétrey et al., 2022) Figure 6 shows how a TEE could be deployed to ensure that data sent to a model is neither seen nor tampered with during inference.Using a TEE ensures that systems are protected from external compute providers, which is of great concern to system owners. Using a TEE also provides guarantees to system users, ensuring that their data is not logged or stored in ways outside of its intended use.

SOURCE

Project team
ArXiv
https://arxiv.org/html/2404.03509v1#S3

NUMBER | TITLE

84 | PAC privacy

SUMMARY DESCRIPTION

One means of preventing sensitive information to be disclosed or intercepted by a malicious agent is to add some noise, or more generic randomness, to it. MIT researchers have developed a technique that enables the user to potentially add the smallest amount of noise possible, while still ensuring the sensitive data are protected. The researchers created a new privacy metric, which they call Probably Approximately Correct (PAC) Privacy, and built a framework based on this metric that can automatically determine the minimal amount of noise that needs to be added. Moreover, this framework does not need knowledge of the inner workings of a model or its training process, which makes it easier to use for different types of models and applications.In several cases, the researchers show that the amount of noise required to protect sensitive data from adversaries is far less with PAC Privacy than with other approaches. This could help engineers create machine-learning models that provably hide training data, while maintaining accuracy in real-world settings.

SOURCE

Project team
A new way to look at data privacy
https://news.mit.edu/2023/new-way-look-data-privacy-0714

NUMBER | TITLE

85 | Simple PIR and Double PIR

SUMMARY DESCRIPTION

Searching the internet can reveal information a user would rather keep private. New research enables users to search for information without revealing their queries, based on a method that is 30 times faster than comparable prior techniques. Moreover, it is driven by a simple algorithm that would be easier to implement than the more complicated approaches from previous work.Their technique could enable private communication by preventing a messaging app from knowing what users are saying or who they are talking to. It could also be used to fetch relevant online ads without advertising servers learning a users' interests.

MIT researchers developed a protocol, known as Simple PIR, in which the server performs much of the underlying cryptographic work in advance, before a client even sends a query. This preprocessing step produces a data structure that holds compressed information about the database contents, and which the client downloads before sending a query.In a sense, this data structure is like a hint for the client about what is in the database.To reduce the size of the hint, the researchers developed a second technique, known as Double PIR, that basically involves running the Simple PIR scheme twice. This produces a much more compact hint that is fixed in size for any database.

SOURCE

Project team
A faster way to preserve privacy online
https://news.mit.edu/2022/online-information-user-data-privacy-1207

NUMBER | TITLE

86 | Keyed Cryptographic Hashing

SUMMARY DESCRIPTION

A keyed hash function (also known as a hash message authentication code, or HMAC) is an algorithm that uses a cryptographic key and a cryptographic hash function to produce a message authentication code that is keyed and hashed. In general HMAC is used to verify the integrity and authenticity of data by computing a fixed-size hash value based on a secret key and input data.

Unlike traditional cryptographic hash functions that generate a hash value solely based on the input data, keyed hashing incorporates a secret key or salt value into the hashing process, making it resistant to tampering and unauthorised modification. The key serves as a shared secret between the sender and receiver, ensuring that only parties possessing the key can compute or verify the hash value.

SOURCE

Project team
Privacy Technologies for Financial Intelligence
https://arxiv.org/pdf/2408.09935

NUMBER | TITLE
116 | DC Network
SUMMARY DESCRIPTION
David Chaum's DC (Dining Cryptographer) network protocol is an anonymous communication protocol, which, even though it cannot be easily used in practice, is still very interesting from a scientific perspective. It provides unconditional sender anonymity, recipient anonymity, and unobservability, even if we assume a global adversary who can observe all communication in the network. Hence, it can guarantee the strongest anonymity properties of all known anonymous communication protocols. DC nets are based on binary superposed sending
SOURCE
Project team Computer and Information Security Handbook, Ch. 43- Privacy-Enhancing Technologies https://www.sciencedirect.com/science/article/pii/B978012394397200043X#s0060; https://arxiv.org/pdf/2103.17091; https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_194

NUMBER | TITLE
125 | Adversarial defense
SUMMARY DESCRIPTION
Adversarial Defense is a technology in the field of security that focuses on enhancing the robustness of machine learning and deep learning systems against adversarial attacks. These attacks typically involve introducing small, often imperceptible, modifications to input data (such as images, text, or sounds) in order to deceive machine learning models, causing them to misclassify. In the context of Internet of Things (IoT) and Android applications, adversarial defense techniques can be used to detect and neutralize malicious Android apps. This is achieved through the use of graph-based classification, generative adversarial networks, and other machine learning algorithms. Similarly, in the realm of air transportation communication, adversarial defense can bolster the reliability of communication jamming recognition models. Adversarial defense technology also finds application in autonomous driving, where it helps to improve the robustness of deep visual detectors. The novelty of adversarial defense lies in its ability to provide robustness against adversarial attacks in a variety of application domains. Unlike traditional security methods that may not effectively mitigate the vulnerabilities of deep learning systems, adversarial defense offers a more resilient approach. Techniques such as Stochastic Activation Pruning (SAP) that prune and scale activations within neural networks, and FaceGuard, a self-supervised adversarial defense framework that automatically detects and purifies adversarial faces, represent significant advancements in this area. However, despite these innovations, the technology still faces challenges, especially in terms of its robustness against adaptive attacks. Hence, continuous research and development are needed to further improve the efficacy of adversarial defense technology.
SOURCE
TIM TIM analytics http://doi.org/10.1016/j.eng.2019.12.012 ; http://doi.org/10.1109/TEM.2021.3059664 ; http://doi.org/10.1109/JIOT.2022.3188583 ; http://doi.org/10.1109/IV51971.2022.9827222 ; http://doi.org/10.1007/978-3-031-20096-0_31 ; http://doi.org/10.1109/FG57933.2023

NUMBER | TITLE

127 | Attribute based searchable encryption

SUMMARY DESCRIPTION

Attribute-based searchable encryption (ABSE) is a sophisticated technology used to enhance the privacy and security of data shared across platforms, such as cloud services or blockchain networks. It allows fine-grained access control over encrypted data, enabling only authorized users to search and retrieve the data they require without compromising the overall data security. ABSE is particularly important in fields where sensitive information, such as medical records or personal health data, needs to be shared securely and efficiently. It is also applicable in other domains such as Industrial Internet of Things, vehicular networks, and cloud-assisted healthcare systems. This technology allows data storage in a distributed system, eliminating a single point of failure, and enables verification of data authenticity, ensuring data integrity and nonrepudiation. The novelty of the ABSE lies in its combination of data encryption, fine-grained access control, and efficient data searchability. Traditional encryption methods either secure data or allow for its searchable storage, but seldom both. ABSE also introduces the concept of attribute-based access, enabling more nuanced and flexible access control compared to the all-or-nothing approach of traditional methods. Furthermore, by integrating ABSE with blockchain technology, it decentralizes the data management, making it tamper-proof and verifiable. It also reduces the computational load on the user side by distributing the load across the network. Importantly, recent advancements have focused on addressing the challenges of computational overhead and storage efficiency, making ABSE more practical for devices with limited resources and storage capacity.

SOURCE

TIM
TIM analytics
http://doi.org/10.1109/MDM.2013.94 ; http://doi.org/10.1109/ICMCCE48743.2019.00188 ; http://doi.org/10.1109/JIOT.2021.3063846 ; http://doi.org/10.1109/JAS.2021.1004003 ; http://doi.org/10.1109/TCC.2021.3090519 ; http://doi.org/10.1109/ICC42927.2021.950096

NUMBER | TITLE

133 | Color image encryption algorithm

SUMMARY DESCRIPTION

The Color Image Encryption Algorithm is a security technology that utilizes complex properties of chaotic systems, particularly hyper-chaotic systems, to protect digital images. The algorithm is designed on a permutation-diffusion structure, transmitting key information through hyper-chaotic synchronization technology. It uses the hash value of the plaintext image to generate the initial key and a hyper-chaotic sequence to implement pixel- and bit-level permutation operations. Some versions of the technology employ Latin squares, DNA sequence operations, and multi-scroll hyperchaotic systems to enhance security. The algorithm can effectively resist various attacks, including exhaustive, statistical, and differential attacks. Potential applications include secure image communication fields and multimedia transmission over unsecured channels. The novelty of the Color Image Encryption Algorithm lies in its use of hyper-chaotic systems, which exhibit pseudo randomness and extreme sensitivity, making them ideal for image encryption. Novel techniques such as the incorporation of tri-valued memristors, Latin squares, DNA sequence operations, and multi-scroll hyperchaotic systems add unique layers of security. Some versions of the algorithm also make use of advanced concepts like gene theory and chaos theory to improve encryption security. Compared to existing technologies, this algorithm provides a higher level of security by resisting a broader range of attacks and by utilizing the inherent connections of orthogonal Latin squares and color images to reduce redundancy and improve efficiency.

SOURCE

TIM
TIM analytics
http://doi.org/10.1016/j.jss.2011.08.017 ; http://doi.org/10.1007/s11071-021-06472-6 ; http://doi.org/10.1016/j.optlastec.2021.107753 ; http://doi.org/10.1016/j.vlsi.2022.10.002 ; http://doi.org/10.1016/j.ijleo.2023.170590 ; http://doi.org/10.3390/math110

NUMBER | TITLE

153 | Machine unlearning

SUMMARY DESCRIPTION

Machine unlearning is a technology that involves removing or 'unlearning' certain data from a machine learning (ML) model, with the aim of enhancing privacy and security. This process could be crucial in situations where data owners want their information forgotten, or when an anomaly detector needs to forget injected data to regain security. It can also be used to remove noise and incorrect entries for improved system usability. This technology can deal with single or multiple classes of data, and its process can be scaled to large datasets and generalized to different deep networks. The unlearning process is achieved by manipulating the model weights with an error-maximizing noise matrix learned for the class to be unlearned using the original model. The technology can also be used to erase backdoors injected into ML models, thus defending against backdoor injection attacks. Moreover, it can be utilized for reverting policies in machine learning-based access control systems and addressing potential vulnerabilities. The novelty of machine unlearning technology lies in its ability to efficiently and effectively 'unlearn' specific data from ML models without retraining the model from scratch or accessing the full training data. This marks a departure from traditional methods that required substantial computational resources or access to original training data, making it a more practical and scalable solution. Furthermore, the technology introduces a new approach to privacy and security by providing a means to erase data in response to new privacy risks or security threats. However, it's important to note that while machine unlearning is designed to enhance privacy, it may leave some imprint of the data in the ML model, potentially creating unintended privacy risks. Therefore, ongoing research is crucial to mitigate these risks and improve privacy protection in practical implementations of this technology.

SOURCE

TIM

TIM analytics

http://doi.org/10.1109/SP.2015.35 ; http://doi.org/10.1145/3460120.3484756 ; http://doi.org/10.1109/INFOCOM48880.2022.9796974 ; http://doi.org/10.1145/3548606.3559352 ; http://doi.org/10.1109/TIFS.2023.3265506 ; http://doi.org/10.1007/s42979-023-01767-4 ;

NUMBER | TITLE

159 | Privacy-preserving machine learning

SUMMARY DESCRIPTION

Privacy-preserving machine learning is a technology that enables the training of predictive models on large amounts of data while maintaining the privacy of the data contributors. It employs techniques such as Federated Learning (FL), two-party computation (2PC), and differential privacy to ensure that the local training data is kept confidential even when used to build shared models. The technology is particularly relevant in fields where privacy is paramount, such as healthcare, education, and finance. It can also be used to enhance efficiency and accuracy in deep learning implementations, enable secure summation of user-held data vectors, and aid in disease diagnosis in agriculture by identifying and classifying disease patterns. The novelty of privacy-preserving machine learning lies in its ability to maintain data privacy while allowing for collaborative model training. Unlike traditional machine learning approaches that require data to be centralized, this technology enables decentralized learning, reducing the risk of privacy breaches. It also incorporates mechanisms to protect against targeted attacks, a challenge that most existing technologies have not adequately addressed. Furthermore, it introduces innovative frameworks, such as the multi-task discriminator in Generative adversarial networks (GANs), to enhance privacy. Additionally, it presents solutions for privacy-preserving linear and logistic regressions that are significantly faster than existing implementations. By integrating the hardware latency of the cryptographic building block into the neural architecture search loss function, it also enhances energy efficiency and reduces latency in deep learning. The technology also enables the training of neural networks in a privacy-preserving manner, a feature that has not been implemented before.

SOURCE

TIM

TIM analytics

http://doi.org/10.1109/SP.2017.12 ; http://doi.org/10.1145/3133956.3133982 ; http://doi.org/10.1109/INFOCOM.2019.8737416 ; http://doi.org/10.1109/FOCS52979.2021.00096 ; http://doi.org/10.1109/SP46215.2023.10179400 ; http://doi.org/10.1109/INCET57972.2023.

NUMBER | TITLE
419 | AI TRISM
SUMMARY DESCRIPTION
Generative AI has sparked extensive interest in artificial intelligence pilots, but organizations often don't consider the risks until AI models or applications are already in production or use. A comprehensive AI trust, risk, security management (TRiSM) program helps you integrate much-needed governance upfront, and proactively ensure AI systems are compliant, fair, reliable and protect data privacy.
SOURCE
Project team Tackling Trust, Risk and Security in AI Models https://www.gartner.com/en/articles/what-it-takes-to-make-ai-safe-and-effective

NUMBER | TITLE
422 | Verifiable computing
SUMMARY DESCRIPTION
Verifiable computing enables a computer to offload a computation of a function to others, perhaps untrusted clients, while maintaining verifiable results (i.e. a kind of verifiable outsourcing). Trusting Execution Environments (TEE) can be considered a type of verifiable computing that requires specific hardware. An ideal verifiable computing environment would be one completely software-based that doesn't require specific hardware. The most likely route to practice software-based verifiable computing is using FHE or probabilistically checkable proofs, but today constructions are too costly.
SOURCE
Project team PETs https://docsend.com/view/db577xmkswv9ujap?submissionGuid=650e684f-93eb-4cee-99e8-12a92d5d88a0

NUMBER | TITLE
425 | End-to-End Encrypted Cloud Storage
SUMMARY DESCRIPTION
End-to-end encryption is rapidly becoming the accepted security goal for personal data. In this article, authors examine consumer cloud storage systems, focusing in particular on those systems that attempt to provide end-to-end security for customer data. We survey the security guarantees of current service providers and the issues they face, discuss open research questions, and highlight the challenges that impede the deployment of end-to-end secure cloud storage.
SOURCE
Project team End-to-End Encrypted Cloud Storage https://ieeexplore.ieee.org/document/10488835

NUMBER | TITLE
429 | Data privacy vault
SUMMARY DESCRIPTION
A data privacy vault is a technology that isolates, secures, and tightly controls access to manage, monitor, and use sensitive data. Innovative companies increasingly adopt data privacy vaults that isolate, protect, monitor, and manage sensitive user data and accommodate region-specific compliance through data localization. Data privacy vaults employ a zero-trust approach to manage sensitive data access tightly, ensuring that user accounts or processes cannot access such data unless access control regulations explicitly permit it. This gives you control over all visibility and its timing, location, continuation, and format to guarantee compliance.
SOURCE
Project team How to Address Generative AI Data Privacy Concerns? https://www.scalefocus.com/blog/how-to-address-generative-ai-data-privacy-concerns; https://www.ciodive.com/spons/the-data-privacy-vault-safeguarding-against-pii-data-breaches/729322/

NUMBER | TITLE
445 | Secure LLM querying
SUMMARY DESCRIPTION
Besides other concerns, one potential information leak when using (remotely operated) LLMs (Large Language Models) could be that the queries submitted to the system could be leaked. Those queries may contain sensitive information. A Privacy Enhancing Technology based on Secret Sharing has been introduced by the Dutch startup Roseman Labs, which enables a user to securely query an LLM: the query is encrypted and cannot be decrypted by anybody, yet the system can infer the answer while staying in the encrypted domain. Such applications are already available for other types of data processing but for the application in LLMs this has not been shown before.
SOURCE
Experts https://rosemanlabs.com/en/blogs/the-future-of-secure-multi-party-computation-tpmpc-2024

NUMBER | TITLE
447 | Ma3tch
SUMMARY DESCRIPTION
The Ma3tch technology (based on Bloom filters) itself is already available some time, but wide application is lagging behind. The first deployment is in FCInet (Financial Crime Intelligence) that links various collaborating FIUs (Financial Intelligence Units) of different countries. The idea is that an FIU could check with other FIUs whether a specific suspect is also being investigated by other countries - but doing this without uncovering the identity of the suspect. No FIU learns which suspects are being queried, no FIU learns which suspects are in the databases of the other FIUs - only when two suspects match, the two FIUs receive an indication and can contact each other for further exchange of information, all while respecting their own legislations. Some other, experimental, deployments of this technology are currently being tested in the Netherlands. The technology itself is stable (TRL9) but the application context is usually complex because of legal considerations.
SOURCE
Experts https://www.fcinet.org/

NUMBER | TITLE
449 | New cryptographic primitives
SUMMARY DESCRIPTION
"The cryptographic community is showing interest in new primitives based on mathematical problems that have not yet received sufficient attention. We can expect changes in the post-quantum context that involves different mathematical problems, but the impact will only be felt in the long term, at least 5 to 10 years in the future. In addition, we can assume that researchers will find new flaws in these new primitives as well."
SOURCE
Experts https://www.enisa.europa.eu/publications/cryptographic-products-and-services-market-analysis/@@download/fullReport

NUMBER | TITLE
450 | Indistinguishability obfuscation
SUMMARY DESCRIPTION
Indistinguishability Obfuscation (iO) is a cryptographic technique that transforms a program or circuit into a version that is functionally equivalent but obscured in such a way that it becomes impossible to distinguish between two different programs with identical functionality. From a technological perspective, iO ensures that no adversary can gain any additional information about the program's internal workings, even if they have access to the obfuscated version.
SOURCE
Experts https://www.enisa.europa.eu/publications/cryptographic-products-and-services-market-analysis/@@download/fullReport

NUMBER | TITLE

453 | Privacy Enhancing Technologies in Data Spaces

SUMMARY DESCRIPTION

Data Spaces are an approach towards trusted data sharing where the trust stems from a governance framework which is supported by technological means. PETs on the other hand derive trust from mathematical principles and do not have to rely on governance and agreements. The novel aspect is to combine the two approaches in such a way that PETs can be easily used in the context of Data Spaces. For this, the Data Spaces architectures and standards need to be further elaborated, and PETs need to be adapted in such a way that they can be deployed within a Data Space, preferably in an automatic way.

SOURCE

Experts
https://bdva.eu/download/92/publications/5196/leveraging-the-benefits-of-combining-data-spaces-and-privacy-enhancing-technologies.pdf

NUMBER | TITLE

458 | Secure Multi-Party Computation

SUMMARY DESCRIPTION

Secure Multi-Party Computation (SMPC) enables multiple parties to compute a function jointly over private data without revealing individual inputs, supporting privacy-preserving collaboration. Recent advancements in post-quantum cryptography are enhancing SMPC protocols to withstand quantum attacks, ensuring long-term data security. SMPC's integration with cloud services marks a disruptive development, enabling secure computations across multi-cloud environments. This allows businesses to leverage scalable cloud power without compromising privacy, with emerging secure cloud-based SMPC services offering accessible solutions for diverse industries. Practical applications have expanded with performance improvements, reducing computational and communication overhead, making SMPC feasible for real-world, high-demand contexts. Particularly valuable in finance, healthcare, and secure voting, SMPC also provides resilience against malicious actors, maintaining security as long as a majority adhere to protocol. As privacy regulations tighten, SMPC's ability to secure collaborative data use across distributed systems positions it as essential to modern cryptographic infrastructure, offering a foundation for secure, decentralized data processing in a variety of high-stakes fields.

SOURCE

Project team
https://www.marketsandmarkets.com/ResearchInsight/emerging-trends-in-secure-multiparty-computation-market.asp
https://www.tno.nl/en/technology-science/technologies/secure-multi-party-computation/
https://research.aimultiple.com/secure-multi-party-computat

NUMBER | TITLE

460 | Federated learning methodologies

SUMMARY DESCRIPTION

Federated Learning (FL) empowers decentralized data collaboration for machine learning without sharing raw data, enhancing privacy. Advanced techniques like Multi-Input Functional Proxy Re-Encryption (MI-FPRE) secure federated training by mitigating leakage risks associated with shared parameters. Asynchronous Federated Learning (AFL) enables continuous, decentralized model updates across diverse devices in dynamic networks, overcoming latency and dropout issues. AFL's asynchronous processing marks a departure from traditional synchronous FL, providing robust real-time applications like Internet of Vehicles (IoV).
Decentralized Federated Learning (DFL) eliminates reliance on central servers, addressing issues like communication bottlenecks and data heterogeneity, while remaining resilient against adversarial attacks. Meanwhile, Federated Reinforcement Learning (FRL) integrates advanced reinforcement techniques, offering adaptive, privacy-preserving training for high-stakes environments such as autonomous driving and ultra-dense networks.
Vertical Federated Learning (VFL) supports secure, cross-organization collaboration by enabling joint model training on shared samples with distinct feature sets, though it introduces privacy challenges related to inference attacks. Each variant contributes to expanding FL's applications in privacy-critical domains like healthcare, telecommunications, and AIoT, paving the way for secure, scalable data sharing in increasingly regulated and distributed data landscapes.

SOURCE

Project team
https://ieeexplore.ieee.org/document/10446283
https://www.techtarget.com/healthtechanalytics/feature/How-Architectural-Privacy-Enhancing-Tools-Support-Health-Analytics; https://theodi.cdn.ngo/media/documents/ODI_Federated-learning_-an-introduction--Consid

NUMBER | TITLE

462 | Confidential Computing

SUMMARY DESCRIPTION

Confidential Computing represents a significant evolution in data security by protecting data in use, in addition to data at rest and in transit. This is achieved through Trusted Execution Environments (TEEs), which create isolated "enclaves" within hardware, preventing unauthorized access even from privileged system levels. These secure enclaves maintain data confidentiality and integrity throughout processing, a novel approach that contrasts with traditional methods limited to encrypting data at rest or in transit.

Confidential computing's introduction of Realms establishes a dedicated physical address space, enhancing protection by eliminating the need to trust the host OS, hypervisor, or privileged software. Additionally, the technology incorporates advanced verification methods to confirm data security and detect unauthorized access, and addresses side-channel attack vulnerabilities—a persistent issue in previous security models.

By integrating with platforms like NVIDIA GPUs and Microsoft Azure, confidential computing enables secure, privacy-preserving AI model training and inference, benefiting sectors like healthcare, finance, and government. This technology promises a transformative shift in cloud and multiparty data processing, offering robust security that aligns with the growing demand for data privacy in increasingly regulated environments.

SOURCE

Project team

https://www.technologyreview.com/2024/07/12/1094838/unlocking-secure-private-ai-with-confidential-computing/

http://doi.org/10.1109/SEED51797.2021.00025 ; http://doi.org/10.1145/3485447.3512244 ; http://doi.org/10.1145/3548606.3560627 ; http://doi.org/10.

Cluster B – Contextual factors (drivers, enablers, and barriers)

The signals related to contextual factors cover various topics concerning drivers, enablers, and barriers for technology development and adoption. These signals have been sub-clustered using the STEEP framework[1], with each signal attributed to the dimension it most strongly connects with. A sixth group includes signals relevant to at least three of the five dimensions. The subclustering is organised as follows:

- Subcluster B1 – Social
- Subcluster B2 – Technological
- Subcluster B3 – Economical
- Subcluster B4 – Environmental
- Subcluster B5 - Political/policy
- Subcluster B6 - Relevant for 2+ dimensions

[1] What is STEEP Analysis, How-To Guide and Examples

Subcluster B1 – Social

List of Signals

- 18 | Washington DC police start using drones alongside police officers
- 389 | Teenagers views on privacy
- 390 | Early adolescents perspectives and behaviours regarding digital privacy
- 399 | Telegram Quietly Updates FAQ Page As Pavel Durov Says Rapid Growth Made It Easier For 'Criminals To Abuse Our Platform'
- 411 | Internet of Behaviour (IoB)
- 414 | The Best Private Messaging Apps for 2024
- 441 | Post-cyberpunk
- 442 | Crypto-anarchy
- 469 | Strava, the exercise app filled with security holes
- 470 | Crypto-anarchists and cryptoeconomics
- 478 | Rising burnout of cybersecurity teams

NUMBER | TITLE
18 | Washington DC police start using drones alongside police officers
SUMMARY DESCRIPTION
Washington DC police will start using drones to respond alongside officers to some calls, including barricade situations and large-scale public gatherings, bolstering a broader government effort that has increased video surveillance of the District.
SOURCE
Project team Website https://www.washingtonpost.com/dc-md-va/2024/06/24/dc-police-drones-surveillance/

NUMBER | TITLE
389 | Teenagers views on privacy
SUMMARY DESCRIPTION
Current literature suggests that adolescents are only partially aware of the concept of online privacy and the implications of sharing personal information and data in different online contexts. Research also suggest that there exists a 'privacy paradox': young people claim to be concerned about privacy, yet they provide a great deal of personal information through social media. Unlike adults who seem to be concerned about online risks, adolescents share personal and sometimes intimate information on social networking sites, provide personal information online, and are unaware of the online privacy policies of platforms. This makes them vulnerable to privacy violations and easy targets for online risks.In addition, adolescents between the ages of 13 and 17 are more likely than adults to provide online data collection practices for commercial reasons. A recent study based on survey of nearly 600 participans show that the analysis of the partici- pants' narratives reveals that adolescents place a high value on the general concept of privacy, which is maintained by moving into the online context. Online privacy is primarily defined as a reflection of the online self. It is also related to a theme of digital safe, as well as human right and ability to surf the web safely and the emotional correlates. In general, the study revealed that students show a deep awareness of the topic under study.
SOURCE
Project team The concept of privacy in the digital world according to teenagers https://doi.org/10.1007/s10389-024-02242-x

NUMBER | TITLE

390 | Early adolescents perspectives and behaviours regarding digital privacy

SUMMARY DESCRIPTION

Using a survey of youth aged 11-14 years information was collected about youth privacy practices. Researchers found that young adolescents' privacy behaviors, beliefs, and practices are multifaceted and complex, reflecting the trade-offs they must make between social connectedness and protecting their privacy. Key findings:
- Adolescents reported more proximal (e.g., not sharing passwords with known others) than distal (e.g., restricting data collection from websites and apps) privacy-protecting behaviors.
- Adolescents were more likely to endorse prescriptive messages regarding risks associated with potential online predators more strongly than risks about corporations and data collection practices.
- While younger adolescents (11- and 12-year-olds) reported fewer total privacy-protecting behaviors than older adolescents (13- and 14-year-olds), they engaged more frequently in privacy-protecting behaviors related to their social relationships.
- Proximal privacy-protecting behaviors were more relaxed with age, compared to distal privacy-protecting behaviors, which increased with age.
- Our findings suggest that issues of digital privacy, especially corporate surveillance, are complex for early adolescents to understand and emotionally navigate.

SOURCE

Project team
Early Adolescents' Perspectives on Digital Privacy
https://wip.mitpress.mit.edu/pub/early-adolescents-perspectives-on-digital-privacy/release/1

NUMBER | TITLE

399 | Telegram Quietly Updates FAQ Page As Pavel Durov Says Rapid Growth Made It Easier For 'Criminals To Abuse Our Platform'

SUMMARY DESCRIPTION

Telegram CEO Pavel Durov addressed criticisms of the platform's moderation, acknowledging that rapid user growth has facilitated misuse by criminals. Responding to calls for improved moderation, Durov emphasized that Telegram takes down millions of harmful posts daily but admitted the platform's abrupt increase to 950 million users has posed challenges. Following criticism, Telegram updated its FAQ page to clarify its reporting process, allowing users to flag illegal content with a few taps, marking a shift from its previous stance on private chats. Users can now report messages for various reasons, including spam, violence, or personal data. Additionally, users can email links for takedown requests to abuse@telegram.org. Durov reiterated Telegram's commitment to balancing privacy and security, even if it means exiting countries where regulatory expectations conflict with the platform's policies.

SOURCE

Project team
Forbes
https://www.forbes.com/sites/siladityaray/2024/09/06/telegram-quietly-updates-faq-page-as-pavel-durov-says-rapid-growth-made-it-easier-for-criminals-to-abuse-our-platform/

NUMBER | TITLE

411 | Internet of Behaviour (IoB)

SUMMARY DESCRIPTION

The aim of IoB is to address how data collected can be interpreted from a human psychological and sociological perspective and how to use this understanding to influence or change human behaviour for various purposes, ranging from commercial interests to public policies.The Internet of Behaviour (IoB) represents a convergence of multiple disciplines: technology, data analytics, and behavioural psychology. It's an emerging field that extends beyond the data collection capabilities of the Internet of Things (IoT) to delve into the realm of behavioural science. IoB is increasingly becoming a cornerstone in our digital world. The Internet of Behaviour (IoB) extends its reach by collecting and analysing data from a wide array of sources, including IoT devices, social media platforms, and websites. This comprehensive scope of data collection raises significant ethical, security, and privacy concerns that must be addressed meticulously.IoB data, encompassing sensitive information like bank codes and personal habits, present lucrative targets for cybercriminals. Risks include potential cyber-attacks, identity theft, ransomware, money laundering, and sophisticated phishing attempts.

SOURCE

Project team
What is the Internet of Behaviour? A Comprehensive Guide
https://www.sovtech.com/blog/what-is-the-internet-of-behaviour-a-comprehensive-guide

NUMBER | TITLE

414 | The Best Private Messaging Apps for 2024

SUMMARY DESCRIPTION

A significant majority (63%) of social media users now express a preference for private messaging apps for sending messages or recommendations to people in their circle, as opposed to posting publicly on social media. However, the information that is shared on those apps (photos, videos, etc.) is also a big business that can be used in identity theft schemes, scams driven by generative AI deep fake technology, or good old-fashioned blackmail. Thus, it is recommended to communicate via a secure private messenger. Signal is our top pick overall, thanks to its uncompromising privacy, but there are other good options with privacy-focused E2EE messaging services: WhatsApp, Telegram, Session, Briar. There are currently 2 bln people in the world using WhatsApp, but it was recently banned in China. There are also certain new features added to these apps to keep the users intact and boost their privacy, for instance Disappearing or self-destructing messages for chats, instant messages, photos, videos, and other media sharing that hides or deletes the message when read. This feature is now available in most used apps (Snapchat, WhatsApp, Signal, Telegram, Messenger, Instagram).

SOURCE

Project team
The Best Private Messaging Apps for 2024
https://www.pcmag.com/picks/best-secure-messaging-apps; https://www.fronetics.com/report-internet-users-prefer-private-messaging-apps-to-shared-content/; https://www.airdroid.com/parent-control/apps-with-disappearing-messages/; https://www.youtube.com/wat

NUMBER | TITLE

441 | Post-cyberpunk

SUMMARY DESCRIPTION

Post-Cyberpunk is a subgenre of science fiction that emerged in response to classic Cyberpunk. While it retains many of the thematic elements of Cyberpunk, Post-Cyberpunk often takes a more optimistic and nuanced approach, emphasizing the potential for technology to empower individuals and focusing on social and political issues. Here's an exploration of the Post-Cyberpunk genre with references to "Altered Carbon" by Richard K. Morgan and "Little Brother" by Cory Doctorow, as well as two additional works by underrepresented authors:
Key Characteristics of Post-Cyberpunk:
Empowerment: Post-Cyberpunk often explores the potential for individuals to harness technology for positive change, emphasizing empowerment and personal agency.
Nuanced Morality: Unlike traditional Cyberpunk, which often depicts a bleak moral landscape, Post-Cyberpunk features characters and situations depicted with increased moral complexity.
Social and Political Issues: The genre delves into contemporary social and political concerns, such as privacy, surveillance, and civil liberties.

SOURCE

Project team
Post-Cyberpunk: Cyberpunks Younger Less Moody Brother
https://theunderdogpress.com/blogs/news/post-cyberpunk-cyberpunks-younger-less-moody-brother?srsltid=AfmBOoo6-nnzUf9qax8a4OvkN-7ipnahtH95E_mY-WCkvNKOJI4kTD3G

NUMBER | TITLE

442 | Crypto-anarchy

SUMMARY DESCRIPTION

Crypto-anarchy, crypto-anarchism, cyberanarchy or cyberanarchism[1] is a political ideology focusing on the protection of privacy, political freedom, and economic freedom, the adherents of which use cryptographic software for confidentiality and security while sending and receiving information over computer networks.[2][3] In his 1988 "Crypto Anarchist Manifesto", Timothy C. May introduced the basic principles of crypto-anarchism, encrypted exchanges ensuring total anonymity, total freedom of speech, and total freedom to trade. In 1992, he read the text at the founding meeting of the cypherpunk movement.

SOURCE

Project team
Crypto-anarchy
https://en.wikipedia.org/wiki/Crypto-anarchy

NUMBER | TITLE

469 | Strava, the exercise app filled with security holes

SUMMARY DESCRIPTION

In recent years, journalists and curious observers have discovered that individuals tasked with sensitive operations, particularly soldiers, have shared their physical activity on Strava, endangering their mission, their identity and even their safety.The military, the bodyguards of the world's most prominent leaders and members of the intelligence services, who are supposed to be well-versed in discretion, can't help but share their sporting exploits with the world on the social media app Strava. An investigation by Le Monde reveals that men charged with protecting Emmanuel Macron, several US presidents and Vladimir Putin can be identified through their use of the sports-tracking app, endangering their mission and the lives of those they protect. Revelations of security flaws of this kind mark the existence of Strava, the leading app of its kind with over 125 million users.

SOURCE

Project team
Strava, the exercise app filled with security holes
https://www.lemonde.fr/en/pixels/article/2024/10/27/strava-the-exercise-app-filled-with-security-holes_6730709_13.html#

NUMBER | TITLE

470 | Crypto-anarchists and cryptoeconomics

SUMMARY DESCRIPTION

Crypto- anarchists and cryptoeconomists design and build decentralised networks as governance systems according to the common prin-
ciples of cryptography, economics, and engineering, and thus,
cryptoeconomics is not new but has historical intellectual roots
in the political ideology of Crypto Anarchy. Cryptoeconomics is a
multidisciplinary field of study concerned with the design of decentralised systems that facilitate the coordination of multiple actors.
Practitioners of crypteoconomics, known as “cryptoeconomists,”
employ engineering and economic methods to create institutional
infrastructure for social coordination. Crypto Anarchy is a political ideology that emphasises autonomy and anonymity and the practice of self-organising through technical means largely attributed
to a counter-cultural subgroup known as the “cypherpunks”. There is a research
demonstrating the link between Crypto Anarchy and cryptoeconomics through the analysis of empirical evidence from primary archival
sources, secondary sources, and academic literature. The implica-
tion of these findings is a deeper understanding of what the
creation of cryptoeconomic systems does in enabling a political
economy of distributed, autonomous coordination. What cryptoeconomists did not adopt and perpetuate is a value for ano-
nymity, which is where the social outcomes of Crypto Anarchy and cryptoeconomics diverge.

SOURCE

Project team
Cryptoeconomics as governance: an intellectual history from “Crypto Anarchy” to “Cryptoeconomics”
https://www.tandfonline.com/doi/pdf/10.1080/24701475.2023.2183643;
https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html;

NUMBER | TITLE

478 | Rising burnout of cybersecurity teams

SUMMARY DESCRIPTION

The increasing sophistication of cybercriminals and the use of AI tools to launch more complex and convincing attacks, combined with escalating global tensions, are fueling an increase in attacks and testing the resilience and adaptability of security teams. Security teams, who were identified as one of the most vulnerable departments to cyberattacks in our Human Risk Review 2023, report heightened stress levels due to escalating cyber security threats. This is further complicated by the alarming shortage of skilled cyber security professionals, with 3.9 million unfilled positions worldwide. The workload for existing teams has led to high stress levels, with surveys indicating that 66% of security team members experience significant work-related stress.

This pressure not only impacts their personal well-being but also increases the possibility of making mistakes and overlooking security breaches. Cybercriminals will continue to exploit this vulnerability in 2024 by specifically targeting exhausted security teams. But not everything is lost: companies can weather the storm by establishing solid career plans to boost employee retention, thus preventing their teams from being understaffed and overworked.

SOURCE

Project team

The cybercrime trends to watch out for in 2024

https://sosafe-awareness.com/blog/the-cybercrime-trends-to-watch-out-for-in-2024/

Subcluster B2 – Technological

List of Signals

- 30 | Planes are under attack from GPS jamming - possible fixes
- 46 | Web 3.0 - A more open, transparent, user controlled web
- 48 | Apple's iMessage is getting post-quantum encryption
- 63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges
- 66 | Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities
- 68 | Global Security Robots Market to Reach $19.3 Billion by 2027
- 79 | Management interfaces
- 96 | US releases highly anticipated post-quantum encryption standards
- 104 | Satellites for quantum communications
- 118 | Geolocation data and privacy
- 135 | Cyber hygiene
- 392 | Quantum error correction technology outperforms world's leading quantum computing company, researchers claim
- 398 | Chrome switching to NIST-approved ML-KEM quantum encryption
- 407 | WebXR allowing for the creation of digital nation-states
- 412 | Web 4.0
- 453 | Privacy Enhancing Technologies in Data Spaces
- 472 | 6G and Reconfigurable Intelligent Surfaces (RIS)
- 475 | Generative AI in cybercrime
- 480 | Biometric scanning
- 485 | Metaverse threats
- 488 | E-evidence - cross-border access to electronic evidence

NUMBER | TITLE
30 | Planes are under attack from GPS jamming - possible fixes
SUMMARY DESCRIPTION
Disruptions to GPS signals, which began near war zones in Europe and the Middle East, are now affecting the busiest oceanic airspace in the world. More than 1700 transatlantic flights cross the North Atlantic between Europe and North America each day. In recent months, a small but growing number of these flights have lost reliable GPS service over Europe or the Middle East and failed to recover it before the ocean crossing. Such interference comes in two forms. GPS jamming transmits powerful signals to overwhelm the weaker radio signals coming from global navigation satellites in space. Another intervention involves spoofing GPS signals, which misleads GPS receivers into falsely reporting that they are hundreds or thousands of miles away from their actual location. The article discussed some possible
SOURCE
Project team Website https://www.newscientist.com/article/2439560-planes-are-under-attack-from-gps-jamming-can-we-find-a-fix

NUMBER | TITLE

46 | Web 3.0 - A more open, transparent, user controlled web

SUMMARY DESCRIPTION

The emergence of blockchain-based technologies such as cryptocurrency, NFTs, metaverse, blockchain, and distributed ledger technology, etc is being seen as the herald of a new era of the internet — a more transparent and open version of the web that would be collectively controlled by users, instead of tech giants like Google and Facebook.

SOURCE

Project team
Interesting engineering
https://interestingengineering.com/culture/web-3-the-new-internet-is-about-to-arrive

NUMBER | TITLE

48 | Apple's iMessage is getting post-quantum encryption

SUMMARY DESCRIPTION

Apple is launching its first post-quantum protections, on of the biggest deployments of the future-resistant encryption technology to date

SOURCE

Project team
Wired
https://www.wired.com/story/apple-pq3-post-quantum-encryption/

NUMBER | TITLE

63 | Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges

SUMMARY DESCRIPTION

Sixth-generation (6G) mobile networks will have to cope with diverse threats on a space-air-ground integrated network environment, novel technologies, and an accessible user information explosion. However, for now, security and privacy issues for 6G remain largely in concept. This survey provides a systematic overview of security and privacy issues based on prospective technologies for 6G in the physical, connection, and service layers, as well as through lessons learned from the failures of existing security architectures and state-of-the-art defenses. Two key lessons learned are as follows. First, other than inheriting vulnerabilities from the previous generations, 6G has new threat vectors from new radio technologies, such as the exposed location of radio stripes in ultra-massive MIMO systems at Terahertz bands and attacks against pervasive intelligence. Second, physical layer protection, deep network slicing, quantum-safe communications, artificial intelligence (AI) security, platform-agnostic security, real-time adaptive security, and novel data protection mechanisms such as distributed ledgers and differential privacy are the top promising techniques to mitigate the attack magnitude and personal data breaches substantially.

SOURCE

Project team
Professional association
https://ieeexplore.ieee.org/document/9524814

NUMBER | TITLE

66 | Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities

SUMMARY DESCRIPTION

Many Experts believe that the Internet of Things (IoT) is a new revolution in technology that has brought many benefits for our organizations, businesses, and industries. However, information security and privacy protection are important challenges particularly for smart vehicles in smart cities that have attracted the attention of experts in this domain. Privacy Enhancing Technologies (PETs) endeavor to mitigate the risk of privacy invasions, but the literature lacks a thorough review of the approaches and techniques that support individuals' privacy in the connection between smart vehicles and smart cities. This gap has stimulated us to conduct this research with the main goal of reviewing recent privacy-enhancing technologies, approaches, taxonomy, challenges, and solutions on the application of PETs for smart vehicles in smart cities. The significant aspect of this study originates from the inclusion of data-oriented and process-oriented privacy protection. This research also identifies limitations of existing PETs, complementary technologies, and potential research directions.

SOURCE

Project team
Wiely online library
https://onlinelibrary.wiley.com/doi/10.1002/ett.4173

NUMBER | TITLE

68 | Global Security Robots Market to Reach $19.3 Billion by 2027

SUMMARY DESCRIPTION

The global security robots market, valued at $8.7 billion in 2021, is projected to grow to $19.3 billion by 2027, with a CAGR of 14.1%. This growth is driven by increasing adoption due to COVID-19, advancements in AI and automation, and rising security concerns. Key applications include spying, patrolling, explosive detection, and rescue operations across defense, residential, and commercial sectors. Major players like Boston Dynamics, Lockheed Martin, and Northrop Grumman lead the market.

SOURCE

Project team
Global Security Robots Market (2022 to 2027) - Industry Trends, Share, Size, Growth, Opportunity and Forecasts
https://www.globenewswire.com/en/news-release/2022/05/10/2439745/28124/en/Global-Security-Robots-Market-2022-to-2027-Industry-Trends-Share-Size-Growth-Opportunity-and-Forecasts.html

NUMBER | TITLE

79 | Management interfaces

SUMMARY DESCRIPTION

As firms gather data, business systems are needed to make information accessible and actionable.
Entities may want to centralize data, or link systems to make data usable across business units, while also preserving the confidentiality of that information. Management interfaces are software systems that sit between datasets or databases and the employees or entities that access those datasets or databases. These systems can perform several different functions to help preserve privacy and confidentiality. Management systems can create manual and automated access controls for databases. These access controls can be based on authorizations that only some employees have. Other access controls can be purpose-based, in which case, they restrict the use of information to activities that an individual has consented to. These systems can also perform security checks and maintain audit trails of any user who accessed information, along with the purpose of accessing the information. This audit information can be fed into a centralized view to facilitate compliance monitoring. An important element of these kinds of systems is their ability to identify data types, tag information, or add metadata that describes certain characteristics of the data, such as sensitivity. Additionally, sensitive information can be tagged to indicate that it belongs in a more restricted database. Data tagging can also be used to implement individual data rights, such as consent. Information that are collected can be tagged with the consent given, making it easier to identify any inappropriate use of that information.

SOURCE

Project team
Privacy-Enhancing Technologies: Categories, Use Cases and Considerations
https://www.frbsf.org/economic-research/wp-content/uploads/sites/4/Privacy-Enhancing-Technologies-Categories-Use-Cases-and-Considerations.pdf; https://www.sciencedirect.com/topics/computer-science/management-interface

NUMBER | TITLE

96 | US releases highly anticipated post-quantum encryption standards

SUMMARY DESCRIPTION

The US Department of Commerce's National Institute of Standards and Technology (NIST) has finalised its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer.Designed for two essential tasks for which encryption is typically used - general encryption, used to protect information exchanged across a public network, and digital signatures, used for identity authentication – they are the first from NIST's post-quantum cryptography (PQC) standardisation project.

These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions and are ready for immediate use.NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

SOURCE

Project team

Technology Decoded

https://www.globaldata.com/newsletter/details/us-releases-highly-anticipated-post-quantum-encryption-standards_374352/?newsletterdate=2024-08-16&hubspotcategory=gd-technology-verdict-daily&utm_source=worldeconomicforum

NUMBER | TITLE

104 | Satellites for quantum communications

SUMMARY DESCRIPTION

Modern quantum technologies have matured such that they can now be used in space applications, e.g., long-distance quantum communication. The researchers at the Technical University of Munich (TUM) are participating in an international research consortium to develop encryption methods that will apply physical laws to prevent the interception of messages. To safeguard communications over long distances, the QUICK space mission will deploy satellites. A new study proposes using satellite-based single photon sources as a means of secure transmission of information across vast distances. This research not only promises unhackable communication but also opens doors to probing fundamental laws of quantum mechanics and delving into quantum effects in gravity.

SOURCE

Project team

Satellites for quantum communications

https://www.sciencedaily.com/releases/2024/03/240313135442.htm;

https://www.advancedsciencenews.com/satellite-mission-sets-stage-for-unhackable-quantum-communication/

NUMBER | TITLE

118 | Geolocation data and privacy

SUMMARY DESCRIPTION

The infographic 'The World of Geolocation Data' explores issues of how mobile operating systems work, how apps request access to information, and how location datasets can be more or less risky or revealing for individuals and groups. Some suggestions are presented of how location datasets can be technically modified to further mitigate risks to individuals and groups, namely: using proximity instead of location, reducing precision or accuracy, avoiding persistent identifiers, redacting home and work location, redacting sensitive locations, applying de-identifying techniques.

SOURCE

Project team

Understanding the "World of Geolocation Data"

https://fpf.org/blog/understanding-the-world-of-geolocation-data/

NUMBER | TITLE

135 | Cyber hygiene

SUMMARY DESCRIPTION

Cyber hygiene is a crucial aspect of information and communication technology (ICT) security that involves maintaining a secure online environment. It includes practices such as secure password management, avoiding suspicious links, and regularly updating software. The importance of cyber hygiene has been amplified with the increase in digitalization across various sectors such as maritime, railways, and academia, making them vulnerable to cyber threats. The need for cyber hygiene awareness is evident in areas like supply chain management in small and medium enterprises (SMEs), online academic activities, and digital transition in railway systems. Effective cyber hygiene practices can mitigate risks associated with cyber-attacks, enhance the resilience of industries, and promote a safer online environment. The novelty of cyber hygiene as a technology lies in its integration into various sectors, particularly in response to the digital transformation brought about by the COVID-19 pandemic. The increasing dependency on networked ICTs in industries like maritime, railways, and education has necessitated more robust cyber hygiene practices. However, it's observed that traditional training programs often lack sufficient cyber hygiene components, thereby leaving a gap that needs to be addressed for better security management. Moreover, the application of AI in enhancing cyber hygiene is still in its nascent stages, indicating the potential for further development and innovation in this field. Furthermore, the understanding of cyber hygiene awareness through demographic factors like gender, employment status, and academic discipline is a new approach in understanding the culture of cyber hygiene among different user groups. The development of tools like browser extensions that validate websites and promote safe browsing is another novel aspect of the technology. Understanding and improving cyber hygiene practices in different cultural contexts, like in rural communities in developing countries, also adds to the novelty of the technology.

SOURCE

TIM
TIM analytics
http://doi.org/10.1177/09544097221089389 ; http://doi.org/10.1016/j.ijinfomgt.2022.102520 ; http://doi.org/10.1088/1742-6596/2311/1/012002 ; http://doi.org/10.1201/9781003216582-6 ; http://doi.org/10.1007/978-981-19-6414-5_22 ; http://doi.org/10.1108/LHTN

NUMBER | TITLE

392 | Quantum error correction technology outperforms world's leading quantum computing company, researchers claim

SUMMARY DESCRIPTION

Researchers at Korea's KIST Quantum Technology Research Center have developed a breakthrough quantum error correction (QEC) technology, surpassing PsiQuantum's methods in performance and efficiency. This advancement is crucial for scalable quantum computing, where error rates can limit computational accuracy as systems grow. The KIST team, led by Dr. Seung-Woo Lee, achieved a photon loss tolerance threshold of 14%, significantly higher than PsiQuantum's 2.7%, while using comparable resources. This QEC technology, published in Physical Review Letters, marks Korea's debut in world-class quantum research, enhancing error correction for diverse quantum architectures like photon-based, superconducting, and ion trap systems. This innovation promises to accelerate the viability of practical quantum computing and strengthens Korea's competitive standing in the global quantum race, with applications filed for both domestic and international patents.

SOURCE

Project team
Phys Org
https://phys.org/news/2024-09-quantum-error-technology-outperforms-world.html

NUMBER | TITLE

398 | Chrome switching to NIST-approved ML-KEM quantum encryption

SUMMARY DESCRIPTION

Google is enhancing Chrome's post-quantum security by transitioning to the NIST-approved ML-KEM (Module Lattice Key Encapsulation Mechanism) for TLS encryption, replacing the experimental Kyber system. This switch aims to bolster protection against potential quantum computer attacks and to prevent store-now-decrypt-later threats. Unlike Kyber, ML-KEM is fully standardized, receiving NIST endorsement in August 2024. Although the technical differences between Kyber and ML-KEM are minor, they are incompatible, necessitating the change. Google's shift also addresses the efficiency challenge: post-quantum cryptographic exchanges like Kyber significantly increase data sizes, risking network performance. Chrome 131, set for release on November 6, 2024, will exclusively support ML-KEM. Server operators are encouraged to offer dual support temporarily to aid the transition, while a DNS-based IETF proposal could streamline algorithm selection in future. Users on Chrome's development channels can access ML-KEM ahead of the official rollout.

SOURCE

Project team
Bleeping Computer
https://www.bleepingcomputer.com/news/security/chrome-switching-to-nist-approved-ml-kem-quantum-encryption/

NUMBER | TITLE

407 | WebXR allowing for the creation of digital nation-states

SUMMARY DESCRIPTION

A new system with unified login and WebXR could become the bedrock of a new generation of digital engagement. WebXR (Web application programming interface) is set to transform how users, developers, and creators engage with virtual environments. It offers a frictionless, universal platform where anyone with a device that supports a web browser — whether that's a PC, mobile phone, or VR headset — can seamlessly engage in immersive experiences through a simple URL. This could also open up opportunities for building digital sovereignity. The nation-state model is built on the concept of unified governance — centralised rules and structures that create consistency and a sense of identity for its citizens and users. Similarly, in the world of digital platforms, a unified login system serves as the foundation for building digital sovereignty. Just as a unified national ID allows citizens to access services and engage with their government, a unified login system allows users to access a broad range of services within a digital ecosystem with one credential.

The benefits of such a system are manifold. Firstly, it removes the friction associated with managing multiple accounts across various services. Users gain immediate access to multiple areas of a platform, with a consistent experience across devices. Digital sovereignty is a step toward breaking down the barriers that have traditionally limited people to operating within physical borders or disconnected digital ecosystems. When a user can move effortlessly through multiple virtual worlds with a single identity, the potential for building thriving, borderless communities becomes immense. 'WebXR is valued as one of the most promising technologies for universal access to virtual and augmented reality. It gives developers the ability to reach audiences they couldn't previously access, on any device, without needing to convince them to install an app," notes Tony Parisi, a thought leader in immersive technologies.

SOURCE

Project team
The Nation-state Playbook: How a Unified Login System and WebXR Can Shape the Future of Digital Communities
https://medium.com/@bennydoda83/the-nation-state-playbook-how-a-unified-login-system-and-webxr-can-shape-the-future-of-digital-cdbfa59ec59f

NUMBER | TITLE
412 | Web 4.0
SUMMARY DESCRIPTION
Web 4.0 is a concept under development. Web 4.0 definition, often referred to as the “Intelligent Web,” represents the latest phase in the internet’s evolution. It incorporates advanced technologies like artificial intelligence, big data, cloud computing, and the Internet of Things (IoT) to create a more interconnected, intelligent, and data-driven digital environment. This enables personalized experiences, efficient automation, and enhanced decision-making. Web four point zero fosters greater decentralization and democratization of information and services, reducing reliance on centralized platforms in favor of peer-to-peer networks and decentralized protocols. Web four point zero employs advanced cryptographic technologies and decentralized architectures to provide enhanced security and privacy safeguards for users’ data and communications.
SOURCE
Project team What Is Web 4.0: An Overview of the Latest Evolution of the Internet https://www.strivemindz.com/blog/what-is-web-4-0/

NUMBER | TITLE
453 | Privacy Enhancing Technologies in Data Spaces
SUMMARY DESCRIPTION
Data Spaces are an approach towards trusted data sharing where the trust stems from a governance framework which is supported by technological means. PETs on the other hand derive trust from mathematical principles and do not have to rely on governance and agreements. The novel aspect is to combine the two approaches in such a way that PETs can be easily used in the context of Data Spaces. For this, the Data Spaces architectures and standards need to be further elaborated, and PETs need to be adapted in such a way that they can be deployed within a Data Space, preferably in an automatic way.
SOURCE
Experts https://bdva.eu/download/92/publications/5196/leveraging-the-benefits-of-combining-data-spaces-and-privacy-enhancing-technologies.pdf

NUMBER | TITLE
472 | 6G and Reconfigurable Intelligent Surfaces (RIS)
SUMMARY DESCRIPTION
Global demand for higher data rates, lower latency and energy-efficient connectivity is skyrocketing. The highly anticipated launch of 6G by 2030 is expected to intensify this pressure even further. To meet these challenges, future networks will need to be engineered for enhanced capacity and connectivity and with a strong focus on environmental sustainability. Enter reconfigurable intelligent surfaces (RIS), platforms that use metamaterials, smart algorithms and advanced signal processing to turn ordinary walls and surfaces into intelligent components for wireless communication. Akin to the idea of “smart mirrors”, RIS enable the precision focusing control of electromagnetic waves, reducing interference and the need for high transmission power. Equally, RIS are highly adaptive and can dynamically adjust configurations according to real-time demands. This adaptability enables efficient use of resources and enhances energy efficiency in wireless networks. Market intelligence reports suggest that RIS will be central to the telecommunications landscape in the coming years.
SOURCE
Project team Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges DOI: 10.1109/OJCOMS.2023.3273507; https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2024.pdf

NUMBER | TITLE

475 | Generative AI in cybercrime

SUMMARY DESCRIPTION

In 2024, the transformative impact of AI on cyber security will take center stage, building upon the momentum of the preceding year. In 2023, malicious actors harnessed tools like WormGPT to not only enhance the speed at which they create content, such as phishing emails, but also to increase the sophistication and effectiveness of their attacks. However, this is merely the tip of the iceberg, as the accessibility and commercialization of AI increases, with projections expecting over 300 million users in 2024 and 700 million by 2030.
This democratization of AI technology has lowered the barrier of entry for cybercriminal activities and increased the potency of multichannel attacks. Technologies like deepfakes and voice cloning are now widely available. Recently, attackers used a voice clone of a teenage girl to demand a $1 million ransom from her mother. The rapid progress of generative AI, as seen in ChatGPT's ability to interpret images, introduces new concerns like prompt injection and the ability to bypass CAPTCHA codes. Multi-factor authentication (MFA) is also becoming susceptible to AI attacks, as shown in the incident at Retool, where attackers claiming to resolve a payroll issue posed as the IT team and tricked an employee into sharing their credentials on a fake landing page. Later, using the AI-generated voice of an IT team member, the attackers asked for the OTP token to bypass Multi-Factor Authentication (MFA). This complex plan enabled them to take over 27 customer accounts and steal valuable cryptocurrency.

SOURCE

Project team
The cybercrime trends to watch out for in 2024
https://sosafe-awareness.com/blog/the-cybercrime-trends-to-watch-out-for-in-2024/

NUMBER | TITLE

480 | Biometric scanning

SUMMARY DESCRIPTION

The increasing use of biometric-based recognition represents a general shift away from graphical user interfaces (GUIs) that depend on a keyboard or screen to biometric-enabled UIs such as voice-user interfaces (VUIs) and other natural-user interfaces. Biometric scanning is based on machine-learning systems, techniques and algorithms that collect unique biometric features to identify individuals and infer attributes about them. Examples include voiceprints (used in voice recognition technology and voice-activated devices), facial scans (used in facial characterization and facial recognition technology), behaviour and gestures (recognition based on bodily movements), physiological (such as flushed skin, or heart rate), and potentially genetic information. Biometric interfaces will require organizations to assess how to apply traditional data protection and privacy principles in the absence of a screen or manual device input. Development of this technology will further blur the divide between law enforcement and consumer privacy concerns. Organizations building, selling and deploying biometric scanning technologies should also consider fairness and justice concerns, such as data training shortfalls related to lack of diversity that can create or perpetuate systemic bias. In addition, security applications relying on biometric scanning systems may need to consider their accuracy as the market for 'biometric camouflage' makeup, clothing and wearables grows.

SOURCE

Project team
Privacy 2020
https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf

NUMBER | TITLE

485 | Metaverse threats

SUMMARY DESCRIPTION

The metaverse is a cloud distributed, multi-vendor, immersive-interactive operating environment that users can access through different categories of connected devices (both static and mobile). It uses Web 2.0 and Web 3.0 technologies to provide an interactive layer on top of the existing internet. As proposed, it is an open platform for working and playing inside a VR/AR/MR/XR environment. This concept is comparable to existing MMORPG platforms, but while each MMORPG represents a proprietary single virtual world, the metaverse will allow players to seamlessly move between virtual spaces together with their virtual assets. The metaverse is not merely a platform for human users; it will also be a communications layer for smart city devices through which humans and AI can share information. The Metaverse threats include: NFTs, the Darkverse (possible space for underground market), financial fraud, privacy issues, cyber-physical threats, etc.

SOURCE

Project team
Metaverse or Metaworse?
https://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf

NUMBER | TITLE

488 | E-evidence - cross-border access to electronic evidence

SUMMARY DESCRIPTION

More than half of all criminal investigations today include a cross-border request to access electronic evidence such as texts, e-mails or messaging apps. That is why the Commission proposed several actions to make it easier and faster for police and judicial authorities to access the electronic evidence they need in investigations to catch and convict criminals, including terrorists. The e-evidence package will make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals. It consists of a Regulation and a Directive, which will: create a European Production Order; create a European Preservation Order; include strong safeguards; create a decentralised IT system through which all communication between authorities and service providers can take place in a secure and reliable way, ensuring authentication of all participants; oblige service providers to designate an establishment or appoint a legal representative in the Union; provide legal certainty for businesses and service providers:

SOURCE

Project team
E-evidence - cross-border access to electronic evidence
https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

Subcluster B3 – Economical

List of Signals

- 459 | Weaponisation of AI
- 461 | Digital economy
- 465 | Cyber threats_WEF
- 467 | Cybercrime scale
- 479 | Public sector as a prime target for hackers

NUMBER | TITLE
459 | Weaponisation of AI
SUMMARY DESCRIPTION
Exploiting weaknesses in artificial intelligence (AI) and machine learning (ML) models, which are developed to detect and prevent intrusion attempts, has become a prevalent tactic both cybercriminal organizations and nation-states employ. Businesses must adopt AI-driven cybersecurity solutions in anticipation of the widespread use of offensive AI. As the battle in cyberspace evolves into a contest between competing algorithms, only an autonomous response system can counteract AI-enhanced attacks with the necessary speed and efficiency. By proactively implementing AI-powered defense measures, businesses can safeguard themselves in this changing digital landscape. Weaponized AI refers to deploying algorithms designed to undermine performance and disrupt the regular operations of benign AI algorithms. This form of AI can create advantageous attack scenarios in both digital and physical domains, granting those who employ it a significant technological edge over their targets. To counteract the weaponization of AI and its potential misuse, policymakers, engineers, researchers, and various stakeholders must cooperate and engage in open dialogue. Investing in digital and media literacy enhances societal resilience and develops sustainable solutions. As AI-driven attacks become more sophisticated, ethical design, deployment, and appropriate regulations are necessary to ensure responsible behavior in cybersecurity. This study provides a comprehensive perspective on the weaponization of AI and its implications for cybersecurity.
SOURCE
Project team The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review https://www.sciencedirect.com/science/article/pii/S1877050924014492

NUMBER | TITLE
461 | Digital economy
SUMMARY DESCRIPTION
It is considered to be one of the largest markets in the world where US region currently holds 38 percent of the global market while the EU share decreased twice during the last decade – from nearly 22 percent in 2013 to nearly 11 percent in 2024 (as of 2022 the UK is indicated separately).According to OECD Digital Economy Outlook 2024, while the “digital economy” is no longer strictly confined to the ICT sector, this sector remains at its heart, underpinning digital innovation. Using a novel nowcasting model that leverages big data and machine-learning techniques, the report assessed that in the past decade the ICT sector grew about three times faster than the total economy in OECD countries and in 2023, it reached new heights, growing 7.6% on average in the OECD. With constantly growing data feeding this ecosystem, which creates immense value but also risks for privacy and safety on line.
SOURCE
Project team OECD Digital Economy Outlook 2024 (Volume 1) https://www.oecd.org/en/publications/2024/05/oecd-digital-economy-outlook-2024-volume-1_d30a04c9.html; https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/

NUMBER | TITLE
465 | Cyber threats_WEF
SUMMARY DESCRIPTION
According to 2023 Global Cybersecurity Outlook, the data protection and cybersecurity concerns created by geopolitical fragmentation are increasingly influencing how businesses operate and the countries in which they invest . The WEF survey showed that character of cyberthreats has changed. The top two concerns among respondents are they now believe that cyberattackers are more likely to focus on business disruption and reputational damage. Among key findings, cyber executives are now more likely to see data privacy laws and cybersecurity regulations as an effective tool for reducing cyber risks across a sector. The Outlook highlighted that 91% of business and cyber leaders surveyed believed geopolitical instability could drive a far-reaching cyber event in the next two years
SOURCE
Project team Global Cybersecurity Outlook 2023 https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

NUMBER | TITLE
467 | Cybercrime scale
SUMMARY DESCRIPTION
Overall, cybercrime is predicted to cost the world $9.5 trillion USD in 2024, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China . It is expected that global cybercrime damage costs will grow by 15 percent per year over the next two years, reaching $10.5 trillion USD annually by 2025.
SOURCE
Project team Cybercrime To Cost The World $9.5 trillion USD annually in 2024 https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

NUMBER | TITLE
479 | Public sector as a prime target for hackers
SUMMARY DESCRIPTION
The public sector has become a prime target for hackers. The sensitive information they handle, their outdated systems, and the reduced security budgets have placed this sector at the top of the most-targeted sectors list by the European Agency for Cybersecurity. And when it comes to public entities, even the simplest attack can have far-reaching consequences. In fact, the average cost of a cyberattack in the public sector mounted to an alarming $2.60 million in 2023, according to IBM's Cost of a Data Breach 2023.
SOURCE
Project team The cybercrime trends to watch out for in 2024 https://sosafe-awareness.com/blog/the-cybercrime-trends-to-watch-out-for-in-2024/

Subcluster B4 – Environmental

List of Signals

- 489 | Raw material supply risks for companies in the digital sector
- 490 | Digital technologies - impact on nature
- 491 | Critical raw materials

NUMBER | TITLE
489 | Raw material supply risks for companies in the digital sector
SUMMARY DESCRIPTION
With the development of ever more powerful computers and smartphones, the multiplication of connected devices in our offices and homes, and the promises of Artificial Intelligence and 5G, digital technologies have us ever more dreaming of a "dematerialized" economy, freed from the physical limits of the real world. However, the digital sector is becoming increasingly resource-hungry, and not just in terms of fossil fuels. Dependent on raw materials such as copper, gold and lithium, digital technologies also rely on much lesser-known metals such as indium, tantalum and gallium to manufacture the equipment that enables it to exist (computers and smartphones, but also transmission networks and data centers). While we don't expect to come up against geological constraints (i.e., "emptying the reserves") in the next 10 years, other issues are likely to restrict access to the raw materials on which the digital sector depends: competing uses, geopolitical risks, environmental and social risks, and the illusion of recycling. By 2050, to meet projected demand, the quantity of metals required could represent 3 to 10 times current production volumes.
SOURCE
Project team carbone4 https://www.carbone4.com/en/analysis-risk-raw-material-digital

NUMBER | TITLE
490 | Digital technologies - impact on nature
SUMMARY DESCRIPTION
The digital sector alone accounted for 4% of global greenhouse gas emissions in 2019. With strong growth, the digital sector's carbon footprint could increase 60% by 2040. It also accounts for 4.2% of primary energy consumption and 0.2% of water consumption worldwide. In addition to GHG emissions, extraction and refining have a strong impact on environmental and human health. Open-pit mining alters the landscape, the soil and the local hydrological regime. Ore extraction and element separation generate chemical effluents (cyanide, arsenic, lead, sulfates, mercury, etc.). In addition to these materials, which are harmful to biodiversity and human health, the production of digital raw materials generates a colossal quantity of inert waste, resulting from the crushing of rocks.
SOURCE
Project team carbon4 https://www.carbone4.com/en/analysis-risk-raw-material-digital

NUMBER | TITLE

491 | Critical raw materials

SUMMARY DESCRIPTION

Critical raw materials (CRMs) are raw materials of high economic importance for the EU, with a high risk of supply disruption due to their concentration of sources and lack of good, affordable substitutes. The EU's demand for base metals, battery materials, rare earths and more are set to increase exponentially as the EU divests from fossil fuels and turns to clean energy systems which necessitate more minerals. CRM are also important to the EU for: industrial value chains; strategic technologies, such as space and defence; climate, energy and environment. Currently, there are 34 CRM identified, and they are mostly sourced outside the EU. The EU will never be self-sufficient but aims to diversify its supply.Currently, for certain critical raw materials, the EU is solely dependent on one country:

China provides 100% of the EU's supply of heavy rare earth elements
Turkey provides 98% of the EU's supply of boron
South Africa provides 71% of the EU's needs for platinum

SOURCE

Project team
EU
https://www.consilium.europa.eu/en/infographics/critical-raw-materials/

Subcluster B5- Political/policy

List of Signals

- 40 | Mosaic warfare
- 58 | The Alaska Supreme Court Takes Aerial Surveillance's Threat to Privacy Seriously, Other Courts Should Too
- 59 | Opportunities in Data Governance: Creating a G20 Data Space
- 67 | Selecting Privacy-Enhancing Technologies for Managing Health Data Use
- 69 | China wants to start a national internet ID system
- 95 | UN Cyber crime convention
- 97 | New Digital Identity models for travels
- 101 | China deploys sattelites in preparation for global internet services
- 395 | Australia Threatens to Force Companies to Break Encryption
- 400 | Planned EU laws on child sexual abuse have sparked a bitter privacy row. Why?
- 410 | digital identity wallet
- 454 | Anonymous Credentials
- 455 | Crypto-war
- 456 | US-China tech race
- 463 | European competitiveness
- 464 | European Digital Decade
- 468 | EC Political Guidelines 2024-2029
- 473 | Niinisto report
- 483 | Access to E-Evidence- High Level Group recommendations
- 484 | Self propagating Zero Click Gen AI worm spreads malware and jailbreaks AI models
- 487 | EU AI Act

NUMBER | TITLE
40 | Mosaic warfare
SUMMARY DESCRIPTION
Exploits a mesh of nodes containing concepts around edge networks, data lakes, networks of low-cost sensors, multi-domain information networks, and autonomous and manned systems to create decision making advantages. AI is certainly applied in this exploitation and should find a good application in surveillence networks.
SOURCE
Project team Science and Technology Trends 2023 https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

NUMBER | TITLE

58 | The Alaska Supreme Court Takes Aerial Surveillance's Threat to Privacy Seriously, Other Courts Should Too

SUMMARY DESCRIPTION

In March, the Alaska Supreme Court held in State v. McKelvey that the Alaska Constitution required law enforcement to obtain a warrant before photographing a private backyard from an aircraft. In this case, the police took photographs of Mr. McKelvey's property, including the constitutionally protected curtilage area, from a small aircraft using a zoom lens.

SOURCE

Project team
Electronic Frontier Foundation
https://www.eff.org/deeplinks/2024/05/alaska-supreme-court-takes-aerial-surveillances-threat-privacy-seriously-other

NUMBER | TITLE

59 | Opportunities in Data Governance: Creating a G20 Data Space

SUMMARY DESCRIPTION

Amid today's digital order, polarised by technological competition and geopolitics, this policy briefa identifies three challenges in data governance-rent captors/ producers vs. users/consumers of the digital economy, public vs. private sector competition, and divergent views on international data free flow with trust (DFFT). The focus is on the challenges and opportunities in operationalising DFFT in the G20. Material interests are camouflaged as normative divergences, hampering consensus- building in defining shared principles in data governance. Since 2016, the G20 has focused on digital connectivity as a driver for economic prosperity. As such, it is uniquely placed to consider digital transformation, digital inclusion, and DFFT. This brief proposes four recommendations towards creating a G20 Data Space: to clarify the definition of DFFT; to de-dogmatise and be pragmatic; to ensure fair and equitable data access and sharing; and to initiate 'Create and Reform' processes towards consolidating a G20 digital agenda

SOURCE

Project team
Global solutions
https://www.global-solutions-initiative.org/policy_brief/opportunities-in-data-governance-creating-a-g20-data-space/

NUMBER | TITLE

67 | Selecting Privacy-Enhancing Technologies for Managing Health Data Use

SUMMARY DESCRIPTION

Privacy protection for health data is more than simply stripping datasets of specific identifiers. Privacy protection increasingly means the application of privacy-enhancing technologies (PETs), also known as privacy engineering. Demands for the application of PETs are not yet met with ease of use or even understanding. This paper provides a scope of the current peer-reviewed evidence regarding the practical use or adoption of various PETs for managing health data privacy. We describe the state of knowledge of PETS for the use and exchange of health data specifically and build a practical perspective on the steps needed to improve the standardization of the application of PETs for diverse uses of health data.

SOURCE

Project team
Research journal
Frontiers in Public Health

NUMBER | TITLE

69 | China wants to start a national internet ID system

SUMMARY DESCRIPTION

The government wants to take over the job of verification from the companies and give people a single ID to use across the internet.

The Ministry of Public Security and the Cyberspace Administration of China say the proposal is meant to protect privacy and prevent online fraud.

A national internet ID would reduce “the excessive collection and retention of citizens’ personal information by internet platforms on the grounds of implementing real-name registration,” the regulators said.

Use of the ID system by websites and apps would be voluntary, according to the proposal, which is open for public comment until the end of August.

SOURCE

Project team

New York Times

https://www.nytimes.com/2024/07/31/business/china-national-internet-id.html

NUMBER | TITLE

95 | UN Cyber crime convention

SUMMARY DESCRIPTION

The committee established by the UN General Assembly to negotiate a new UN cybercrime convention agreed in draft this week, has received criticism after three years of work. The General Assembly is expected to adopt the convention later this year as the first global legally binding instrument on cybercrime.

Over a five-year cycle involving Member States, academic institutions, civil society and the private sector, the UN cyber convention includes tools to enhance international cooperation, support law enforcement efforts, technical assistance, and capacity-building relating to cybercrime.

Multinational technology conglomerate Cisco released a statement saying that the convention falls short of what is needed and has urged UN Member States to better align with the authorities and protections already in the Budapest Convention.Eric Wenger, Senior Director for technology policy at Cisco said: “Criminal groups are leveraging advanced technology to operate across borders, necessitating that law enforcement agencies have the capabilities to prevent, investigate, and prosecute these crimes while also protecting human rights.

"The UN Convention does not sufficiently protect basic human rights and poses risks to the rule of law. Rather than specifically focusing on hacking and cybercrimes, it broadly aims at the misuse of computer networks to disseminate objectionable information. This represents a misalignment with the values of free speech.”

SOURCE

Project team

Cisco says UN cybercrime convention does not go far enough

https://www.globaldata.com/newsletter/details/cisco-says-un-cybercrime-convention-does-not-go-far-enough_374423/?newsletterdate=2024-08-16&hubspotcategory=gd-technology-verdict-daily&utm_source=worldeconomicforum

NUMBER | TITLE

97 | New Digital Identity models for travels

SUMMARY DESCRIPTION

The report outlines three identity models that, they argue, will play a fundamental role in the future of secure and seamless travel.
1) ICAO released the Digital Travel Credential (DTC) that presents an opportunity to accelerate seamless travel using a global standard with a clearly defined ICAO governance. This virtual credential is an exact representation of the ePassport, containing the holder's facial image, biographical data, and security features. Once generated, DTC can be securely stored on the holder's device and shared with travel service providers (e.g., border agencies) ahead of travel to provide required information.
2)The International Organization for Standardization (ISO) is developing mobile driving license (mDL) standard that is gaining a lot of traction, especially in the US, where the number of states offering mDLs is rapidly growing due to increasing demand for contactless forms of digital ID. This mDL specification supports privacy-preserving techniques like selective disclosure where only required information and not the whole credential is shared.
3) W3C standards for decentralized (or self-sovereign) identity and verifiable credentials (VCs) re-envision the way we share, access, control, and manage our online personal information. Decentralized digital identity gives individuals full control of their digital identities and has privacy by design at its core. With the right governance and trust frameworks in place, this new wave of digital identity credentials could be accepted across sectors and borders, support a wide variety of interactions, and help move towards a fully digital travel experience.

SOURCE

Project team
Digital identity models: What's next for secure and seamless travel?
https://www.weforum.org/agenda/2023/05/emerging-digital-identity-models-secure-and-seamless-travel/

NUMBER | TITLE

101 | China deploys sattelites in preparation for global internet services

SUMMARY DESCRIPTION

The first satellites for China's ambitious G60 mega-constellation are in orbit in preparation for offering global satellite internet services. The project aims to compete in the commercial satellite internet market with SpaceX's Starlink, providing regional coverage by 2025 and global coverage by 2027. It will be infrastructure to support China's rapidly growing commercial space sector, including its satellite internet initiatives which are making rapid advances. Central to China's ambition is the concept of cyber sovereignty—the notion that each nation has the right to govern its digital domain. In practice, China has used this principle to build a heavily censored surveillance system supporting the Chinese Communist Party's power, widely condemned for violating human rights. Satellite internet is more controllable due to its centralised infrastructure, where data is routed through a limited number of ground stations or gateways. This enables censorship and surveillance as service providers and authorities can more easily monitor, block and filter content. Countries that use China's satellite internet service providers could more easily control what information is accessible within their borders, much as the Great Firewall of China operates domestically.China is already exporting its digital authoritarianism through such initiatives as the Digital Silk Road, providing technologies and governance models that enable censorship, surveillance and social control to other countries.The centralised nature of satellite internet may also make countries more vulnerable to cyber espionage by the Chinese government or malicious actors.

SOURCE

Project team
China may be putting the Great Firewall into orbit
https://www.aspistrategist.org.au/china-may-be-putting-the-great-firewall-into-orbit/

NUMBER | TITLE

395 | Australia Threatens to Force Companies to Break Encryption

SUMMARY DESCRIPTION

Australia's Assistance and Access Act of 2018 allows the government to compel tech companies to break their own encryption, potentially creating security vulnerabilities in the process. The Act enables three key mechanisms for law enforcement: Technical Assistance Requests (TARs) for voluntary cooperation, Technical Assistance Notices (TANs) for compulsory decryption support, and Technical Capability Notices (TCNs) that mandate companies to develop new methods for accessing encrypted data. Although the most controversial provision, TCNs, has not yet been used, ASIO director Mike Burgess recently indicated that they may soon be employed in national security cases. Burgess claims that secure, lawful access could be designed without weakening encryption, but critics argue that backdoors inherently endanger data security. If Australia enforces this law, it could create significant challenges, especially for companies like Apple and WhatsApp, as the required changes might compromise the privacy and security of all users.

SOURCE

Project team
Bruce Schneier
https://www.schneier.com/blog/archives/2024/09/australia-threatens-to-force-companies-to-break-encryption.html

NUMBER | TITLE

400 | Planned EU laws on child sexual abuse have sparked a bitter privacy row. Why?

SUMMARY DESCRIPTION

The EU's proposed child sexual abuse (CSAM) law has sparked a heated privacy debate. The law would mandate tech companies to scan user communications, including encrypted messages, for CSAM using client-side scanning (CSS) technology. Supporters argue this is essential for protecting children, as voluntary measures by tech companies have been insufficient, with CSAM content increasing significantly. Advocates like survivors Rhiannon and Mié emphasize that Europe's democratic safeguards would prevent misuse, and assert that tech companies must prioritize child safety over data privacy.

Opponents, however, warn that scanning encrypted messages could undermine digital privacy, risking mass surveillance and setting a dangerous precedent. Experts caution about technical flaws, such as high false-positive rates and potential misuse by authoritarian regimes. Critics also argue that scanning technologies need further refinement to prevent wrongful accusations and preserve legitimate privacy. EU ministers now face balancing these opposing perspectives, possibly delaying more controversial aspects until the technology matures.

SOURCE

Project team
Euronews
https://www.euronews.com/my-europe/2023/10/19/planned-eu-laws-on-child-sexual-abuse-have-sparked-a-bitter-privacy-row-why

NUMBER | TITLE

410 | digital identity wallet

SUMMARY DESCRIPTION

The EU Digital Identity Wallet is a collaboration between the EU institutions and the Member States. Together, they are working across two main streams of work to make EU Digital Identity Wallets a reality that can be used by citizens, residents, and businesses across Europe. EU Digital Identity Wallets will enable users to access online services, store and share digital documents, and create binding signatures. EU Digital Identity Wallets are the European Union's response to the challenges of digital identification. Every EU Member State will offer its own wallet app, built to the same specifications, to all citizens, residents and businesses in the next few years. Each version of the wallet will be interoperable and will work wherever you are in Europe. With this, the digital documents digital documents will be:

Secure: Strong cryptographic encryption keeps your data safe
Privacy-preserving: Private by design; only necessary information is shared.
Cross-border: Many digital documents will be accepted wherever you are in Europe.

SOURCE

Project team
A digital ID and personal digital wallet
https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

NUMBER | TITLE

454 | Anonymous Credentials

SUMMARY DESCRIPTION

"After extensive debate the eiDAS 2.0 regulation (electronic identification and trust services) defined explicit and reasonable privacy requirements. Unfortunately, we believe that some of the currently suggested design aspects of the EU Digital Identity Wallet (EUDIW) and its credential mechanism fall short of the privacy requirements as it relies on cryptographic methods that were never designed for such requirements.
The technology that fits the eiDAS 2.0 regulation bill is called anonymous credentials and achieves both strong unlinkability with suitable pseudonyms and selective disclosure guarantees facilitating utility and privacy tradeoffs and is by now close to market. Exploring this technology in the context of the EU Digital Identity Wallet (EUDIW) could give European technology companies an advantage in the digital identity space."

SOURCE

Experts
https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211

NUMBER | TITLE

455 | Crypto-war

SUMMARY DESCRIPTION

Crypto Wars is an unofficial term for attempts by the US and allied governments to restrict public and foreign access to strong cryptography in order to avoid decoding by national intelligence agencies.
The goal of these acts is clear: no one or nation can rely on encryption methods that are unbreakable by national spy agencies. As a result, no one would be safe from snooping by agencies like the NSA, the CIA, or the FBI. This condition stems from a difficult period in history, the Cold War. On the one hand, the Western block aimed to safeguard its communications and prevent the Eastern block from obtaining robust encryption technology. They, on the other hand, desired to do the same. Both camps sought to spy on each other at the same time, seeking for methods to break their systems. A circumstance that prompted some unusual responses.
During the first crypto war, in the 1990s, privacy campaigners and security experts fought against broad US cryptography export controls and purposeful encryption weakening. The outcome of the conflict is primarily to blame for the growing usage and availability of encryption techniques, as well as the global expansion of e-commerce. Steven Levy, a former Newsweek chief technology correspondent who literally wrote the book on the first crypto war in 2001, summed up the outcome in five words: "public crypto was our friend," implying that the US government's position shifted away from viewing cryptography solely as a threat to national security.
With the Snowden revelations in 2013, the world was engulfed in a second crypto war, which continues to this day. The current topic of disagreement is whether government agencies should have unrestricted access to communications data and the ability to unlock personal electronic devices.
To some kind of a crypto war, we can put governments efforts to make applications such as WhatsApp and Telegram decrypted, so they could access the conversations. WhatsApp for example has end to end encryption, which means that no third-party (even government) can not read or access it.

SOURCE

Project team
What are crypto wars
https://bitmarkets.com/en/education/tutorials/what-are-crypto-wars;
https://news.law.fordham.edu/jcfl/2023/03/31/the-crypto-wars-and-the-future-of-financial-privacy/

NUMBER | TITLE

456 | US-China tech race

SUMMARY DESCRIPTION

The United States' current rivalry with China should be seen as a technology race in which the ability to imagine, discover and apply innovations will decide who wins. While the United States spends more than China on research and development (R&D), China's state-centred system enables it to transform funding and talent into deployed capabilities faster than the United States' private-enterprise-centred system can. Accordingly, the US must avoid complacency about the inherent advantage of the democratic-capitalist system in scientific discovery and devise more effective mechanisms for stimulating free enterprise to develop new military technology. This requires the US Department of Defense to devote more resources to R&D by asking allies to contribute more for military operations, and to better incentivise military innovation by investing funds in private enterprise to defray start-up costs before production can yield steady revenue. As for emerging military technologies: While sound investment calls for a long view, short-term timing is critical. A wave of new technologies of enormous military potency – artificial intelligence (AI), quantum computing, chip and battery design, revolutionary space networks – is cresting. These technologies can improve Chinese targeting of US forces. AI can operate uncrewed aircraft and ships, multiply the quality of intelligence and foster flexible decision-making. Quantum computing can accelerate data processing and improve cyber security. Better, smaller chips and batteries can revolutionise microelectronic and energy performance. And a large network of satellites is a force multiplier in all battlefield domains and across vast geographical areas.

SOURCE

Project team
Winning the US–China Technology Race
https://www.tandfonline.com/doi/full/10.1080/00396338.2024.2380198#d1e120

NUMBER | TITLE

463 | European competitiveness

SUMMARY DESCRIPTION

Europe largely missed out on the digital revolution led by the internet and the productivity gains it brought: in fact, the productivity gap between the EU and the US is largely explained by the tech sector. The EU is weak in the emerging technologies that will drive future growth. Only four of the world's top 50 tech companies are European'. In order to digitalise and decarbonise the economy and increase our defence capacity, the investment share in Europe will have to rise by around 5 percentage points of GDP to levels last seen in the 1960s and 70s. Among proposed areas for action: Europe must profoundly refocus its collective efforts on closing the innovation gap with the US and China, especially in advanced technologies.

SOURCE

Project team
The future of European competitiveness
https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

NUMBER | TITLE

464 | European Digital Decade

SUMMARY DESCRIPTION

The European Digital Decade policy programme has set concrete targets and objectives for Europe 2030 in four broad areas: government, skills, business and infrastructure. For instance: Tech up-take: 75% of EU companies using Cloud, AI, or Big Data; Key Public Services: 100% online
e-Health: 100% of citizens have access to medical records online
Digital Identity: 100% of citizens have access to digital ID

SOURCE

Project team
Europe's Digital Decade
https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

NUMBER | TITLE

468 | EC Political Guidelines 2024-2029

SUMMARY DESCRIPTION

The document sets the political priorities for the upcoming ter m m of the new European Commission. Among key goals and objectives identified: boosting productivity with digital tech diffusion; focus our efforts on becoming a global leader in AI innovation; AI Factories initiative; Apply AI Strategy; European AI Research Council; European Data Union Strategy; Putting research and innovation at the heart of our economy; new European Biotech Act; Union of Skills; A new era for European Defence and Security: 'We will look at all of our policies through a security lens'; building a true European Defence Union; Defence projects, starting with a European Air Shield and cyber defence; Preparedness Union Strategy, as part of this - further strengthening our cyber defence capabilities, coordinating national cyber efforts and securing our critical infrastructures. A safer and more secure Europe: There can be no hiding place for organised crime in Europe – either offline or online. A new European Internal Security Strategy. This will help ensure that security is integrated in EU legislation and policies by-design.
We need to provide law enforcement with adequate and up-to-date tools for lawful access to digital information, while safeguarding fundamental rights. I will propose to make Europol a truly operational police agency and more than double its staff over time. This should come with a strengthened oversight and mandate.

SOURCE

Project team
Europe's Choice

NUMBER | TITLE

473 | Niinisto report

SUMMARY DESCRIPTION

Focus on comprehensive EU preparedness. Among proposed measures: Ensure the creation of a robust framework for lawful access to encrypted data to support the fight of Member States' authorities against espionage, sabotage and terrorism, as well as organised crime. There are signs that in several recent cases of sabotage, perpetrators were recruited and instructed via digital communication applications. Therefore, the ability of lawfully accessing encrypted data is important to counter such threats, while fully respecting fundamental rights and without undermining cybersecurity.

SOURCE

Project team
Safer Together
https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

NUMBER | TITLE

483 | Access to E-Evidence- High Level Group recommendations

SUMMARY DESCRIPTION

In recent years, despite the creation, transmission and storage of ever greater quantities of data, access to data for law enforcement purposes has emerged as a key challenge to carry out investigations and prosecutions into criminal offences and to effectively enforcing law. The EU has put in place strong rules to facilitate cross-border access to electronic evidence (the "EU e-evidence rules"). However, the absence of data retention obligations negatively affects the effectiveness of e-evidence rules, as there is no guarantee that all the information subject to European preservation or production orders, including traffic data, data requested for the sole purpose of identifying the user, and subscriber data, is available. Moreover, the EU e-evidence rules cover solely data in possession of service providers and do not address the challenge of encryption. Therefore, without operative measures for lawful access to data, this risks to fall short in ensuring effective law enforcement. The High Level Group on access to data for effective
law enforcement (HLG), was initiated by the Swedish Presidency and composed of high-level representatives of the Member States, the Commission, relevant EU bodies and agencies, and the EU Counter-Terrorism Coordinator, in June 2023. HLG maintains that law enforcement authorities face increasing operational challenges when seeking to lawfully access data digitally generated, processed or stored in a readable format. The Group formulated a number of key drivers, e.g. access to data at rest in a user's device, the HLG identified as main issue; he pace of technological developments related to encryption of information on devices to be rapid to the point that existing decryption tools and techniques are becoming
ineffective; the lack of cross-border law enforcement cooperation mechanisms concerning the sharing of digital forensic tools between Member States; networks such as the European Network of Forensic Science Institutes (ENFSI17) dedicated to coordination and knowledge-sharing of digital forensic methods, tools, and best practices, are key for digital forensic practitioners across the EU. Experts highlighted notably the current absence of any level of harmonisation of data retention legislation across the EU; On accessing content data despite encryption, experts extensively discussed and agreed upon the need for law enforcement to have access to data en clair. HLG also formulated a number of recommendations, e.g.: Mapping and connecting existing digital forensic networks while increasing accessibility, avoiding overlaps, and fostering leadership; To reflect on mechanisms for pooling knowledge, to ensure that digital forensics tools can be shared between Member States in an environment of trust, whilst taking into account national rules; The development of a mechanism at EU level for jointly purchasing the licenses of digital forensic tools, to share them among Member States; Increasing funding for research and development of tools for data acquisition, access to data in clear including decryption capabilities, and artificial intelligence-based capacities for data analysis with clear deliverables, and promoting the Europol Tool Repository as a central hub for the dissemination of these tools, etc.

SOURCE

Project team
Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement
https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf

NUMBER | TITLE

484 | Self propagating Zero Click Gen AI worm spreads malware and jailbreaks AI models

SUMMARY DESCRIPTION

In what's an example of yet another innovative and crippling use of technology to do evil a worm that uses clever prompt engineering and prompt injection attacks has been shown to be able to trick Generative Artificial Intelligence (GenAI) apps and models like ChatGPT into propagating malware – and much more. in a laboratory setting, three Israeli researchers demonstrated how an attacker could design "adversarial self-replicating prompts" that convince a generative model into replicating input as output. In other words if a malicious prompt comes in, the AI app or model in question will turn around and push it back out, allowing it to spread to further AI agents. The prompts can be used for stealing information, spreading spam, poisoning models, and more.

SOURCE

Project team
Self propagating Zero Click Gen AI worm spreads malware and jailbreaks AI models
https://www.fanaticalfuturist.com/2024/10/self-propagating-zero-click-gen-ai-worm-spreads-malware-and-jailbreaks-ai-models/

NUMBER | TITLE
487 | EU AI Act
SUMMARY DESCRIPTION
The AI Act is the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally. The AI Act (Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence) provides AI developers and deployers with clear requirements and obligations regarding specific uses of AI. At the same time, the regulation seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises (SMEs). The AI Act is part of a wider package of policy measures to support the development of trustworthy AI, which also includes the AI Innovation Package and the Coordinated Plan on AI. Together, these measures guarantee the safety and fundamental rights of people and businesses when it comes to AI. They also strengthen uptake, investment and innovation in AI across the EU. The AI Act is the first-ever comprehensive legal framework on AI worldwide. The aim of the new rules is to foster trustworthy AI in Europe and beyond, by ensuring that AI systems respect fundamental rights, safety, and ethical principles and by addressing risks of very powerful and impactful AI models.
SOURCE
Project team AI Act https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

Subcluster B6 - Relevant for 2+ dimensions

List of Signals

- 45 | The Battle for Digital Privacy Is Reshaping the Internet
- 60 | Opportunities for synthetic data in nature and climate finance
- 94 | The rise of Big Cyber risk: Are businesses too reliant on just a few cybersecurity vendors?
- 102 | Smart toys spy on kids
- 401 | Unveiling the Dark Web: How Privacy Coins Fuel the Trade of Criminal Material Online
- 474 | World in Polycrisis
- 476 | Hacktivism and digital dissent
- 477 | Disinformation-as-a-Service
- 481 | Internet of Bodies (IoB) and Brain-Machine Interfaces
- 482 | Smart communities

NUMBER | TITLE
45 | The Battle for Digital Privacy Is Reshaping the Internet
SUMMARY DESCRIPTION
Apple introduced a pop-up window for iPhones in April that asks people for their permission to be tracked by different apps. Google recently outlined plans to disable a tracking technology in its Chrome web browser. And Facebook said last month that hundreds of its engineers were working on a new method of showing ads without relying on people's personal data. Now that system, which ballooned into a $350 billion digital ad industry, is being dismantled. Driven by online privacy fears, Apple and Google have started revamping the rules around online data collection. Apple, citing the mantra of privacy, has rolled out tools that block marketers from tracking people. Google, which depends on digital ads, is trying to have it both ways by reinventing the system so it can continue aiming ads at people without exploiting access to their personal data.
SOURCE
Project team The New Yord Times https://www.nytimes.com/2021/09/16/technology/digital-privacy.html

NUMBER | TITLE
60 | Opportunities for synthetic data in nature and climate finance
SUMMARY DESCRIPTION
This paper delves into the intricacies of synthetic data, emphasizing its growing significance in the realm of finance and more notably, sustainable finance. Synthetic data, artificially generated to simulate real-world data, is being recognized for its potential to address risk management, regulatory compliance, and the innovation of financial products. Especially in sustainable finance, synthetic data offers insights into modeling environmental uncertainties, assessing volatile social and governance scenarios, enhancing data availability, and protecting data confidentiality. This critical review attempts first ever classification of synthetic data production methods, when applied to sustainable finance data gaps, elucidates the methodologies behind its creation, and examines its assurance and controls. Further, it identifies the unique data needs of green finance going forward and breaks down potential risks tied to synthetic data utilization, including challenges from generative AI, input quality, and critical ethical considerations like bias and discrimination
SOURCE
Project team Frontiers in AI https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2023.1168749/full

NUMBER | TITLE

94 | The rise of Big Cyber risk: Are businesses too reliant on just a few cybersecurity vendors?

SUMMARY DESCRIPTION

The recent CrowdStrike global outage caused by a bug in a software update posed a question about what risks are posed by overreliance on such a small number of cybersecurity service and platform vendors.The worldwide temporary chaos was a result of distributing a faulty update to CrowdStrike's Falcon Sensor security software and resulted in a Windows system crash across multiple industries from transport to healthcare.

Insurers estimate the outage will cost US Fortune 500 companies around $5.4bn prompting businesses to ask how they can avoid this happening to them.

Some of the top US cyber companies have software programmes running on most company devices including Palo Alto Networks, Fortinet, Cisco, Cloudfare, Zscaler, and, of course, CrowdStrike. If there is an issue with one of these major players, then there is a risk of severe disruption to organisations relying solely on these companies, and often this can lead to increased criminal activity when a major vendor's vulnerabilities are exposed.

SOURCE

Project team

Technology Decoded

https://www.globaldata.com/newsletter/details/are-businesses-too-reliant-on-just-a-few-cybersecurity-vendors-_374604/?newsletterdate=2024-08-20&hubspotcategory=gd-technology-verdict-daily&utm_source=worldeconomicforum

NUMBER | TITLE

102 | Smart toys spy on kids

SUMMARY DESCRIPTION

Toniebox, Tiptoi, and Tamagotchi are smart toys, offering interactive play through software and internet access. However, many of these toys raise privacy concerns, and some even collect extensive behavioral data about children, report researchers at the University of Basel.

SOURCE

Project team

How smart toys spy on kids: what parents need to know

https://www.unibas.ch/en/News-Events/News/Uni-Research/How-smart-toys-spy-on-kids--what-parents-need-to-know.html

NUMBER | TITLE

401 | Unveiling the Dark Web: How Privacy Coins Fuel the Trade of Criminal Material Online

SUMMARY DESCRIPTION

Privacy coins like Monero are increasingly implicated in the dark web's criminal economy, particularly in child sexual abuse material (CSAM) trade, according to Chainalysis's 2024 Crypto Crime Report. While Bitcoin is still commonly used for CSAM purchases, Monero's privacy features make it popular among vendors for laundering and concealing funds post-transaction. The report highlights Monero's use via instant exchangers—non-custodial, anonymous platforms that enable fast crypto exchanges without KYC verification, aiding CSAM vendors in hiding transaction trails.

Regulators have pressured exchanges like Binance to delist privacy coins, citing risks of money laundering and insufficient KYC and AML protections. However, blockchain analysis has also been a crime-fighting tool: in 2019, law enforcement leveraged Chainalysis to dismantle a major CSAM site, leading to arrests and victim rescues. The report underscores the dual nature of crypto: a tool for both privacy-focused crime and law enforcement breakthroughs.

SOURCE

Project team

Cryptonews

https://cryptonews.com/news/unveiling-the-dark-web-how-privacy-coins-fuel-the-trade-of-criminal-material-online/

NUMBER | TITLE
474 | World in Polycrisis
SUMMARY DESCRIPTION
Experts evaluating the short- and long-term challenges facing the planet for the World Economic Forum's Global Risks Report 2023, found the risk of polycrises is growing. The Report uses the term, to explain how, "present and future risks can also interact with each other to form a 'polycrisis' – a cluster of related global risks with compounding effects, such that the overall impact exceeds the sum of each part". The intersection of current risks with emerging crises poses the greatest risk of a polycrisis.
SOURCE
Project team This is why 'polycrisis' is a useful way of looking at the world right now https://www.weforum.org/agenda/2023/03/polycrisis-adam-tooze-historian-explains/; https://www.weforum.org/agenda/2023/01/polycrisis-global-risks-report-cost-of-living/

NUMBER | TITLE
476 | Hacktivism and digital dissent
SUMMARY DESCRIPTION
Global instability has spurred a surge in both cybercrime and incidents involving hacktivists, who launch targeted cyberattacks aligned with their political or social motivations. The growing hacktivism trend, which increased by 27% in 2023, is expected to increase even more in 2024, especially in the context of the growing geopolitical tensions and conflicts. In fact, the more recent conflict between Israel and Gaza highlights the escalation and further implications of this threat.But hacktivism is not solely confined to political or warfare contexts. It also extends to social causes. The recent cyberattacks on Scandinavian Airlines by Anonymous Sudan in response to a far-right nationalist group's actions and the VulzSec hacking group compromising French police data in retaliation for police brutality are stark examples of some of the possible motivations behind the activities of hacktivists. This symbiotic relationship between hacktivists and cybercriminals creates a complex cyber threat landscape where vulnerabilities exposed by one faction are exploited by the other. With such a high number of cyberattacks coming from several sources and motivated by different reasons, organizations will struggle to identify who is targeting them and, in turn, how to adapt their cyber security strategies accordingly.
SOURCE
Project team The cybercrime trends to watch out for in 2024 https://sosafe-awareness.com/blog/the-cybercrime-trends-to-watch-out-for-in-2024/

NUMBER | TITLE
477 | Disinformation-as-a-Service
SUMMARY DESCRIPTION
"Disinformation-as-a-Service" (DaaS) is becoming a pivotal tool for hackers, especially in destabilizing governments and organizations. This tactic, which involves the deliberate spread of false information, is increasingly being used by many different actors to manipulate public opinion, damage reputations, and influence business and political landscapes. We saw this in the Slovakian elections, where attackers used an AI-generated deepfake audio to spread disinformation. Now, as the US elections approach, there's a real concern that similar tactics could be used to influence public opinion and affect voting decisions.Beyond political agendas, financially motivated cybercriminals are expected to leverage DaaS to destabilize organizations and harm their reputation. CEOs, who are often targeted because of their high visibility, are especially at risk. Since it's quite simple for hackers to obtain their voice or video clips, these can be twisted into making shocking statements that can hurt the image of the businesses they lead.
SOURCE
Project team The cybercrime trends to watch out for in 2024 https://sosafe-awareness.com/blog/the-cybercrime-trends-to-watch-out-for-in-2024/

NUMBER | TITLE
481 | Internet of Bodies (IoB) and Brain-Machine Interfaces
SUMMARY DESCRIPTION
IoB refers to a network of medical and biometric devices that attach to or are inside of our bodies and connected to the Internet. While people have largely accepted wearables like smartwatches, IoB devices may also include devices such as smart contact lenses, Bluetooth-enabled 'smart pills', and Wi-Fi enabled 'pacemakers'. These more intimate devices raise a number of legal, ethical and security challenges, including who should have access to the data they generate, how to mitigate risks of malicious hacking, how to apply existing legal frameworks, and who is liable for vulnerabilities, malfunctions, or breaches. A brain-machine interface, also known as computer-brain interface, mind-machine interface, direct-neural interface or human-machine interface is a computer interface that can connect humans and machines by allowing people to communicate and control devices with their thoughts alone. These interfaces have promising medical and commercial applications but also raise significant privacy and security concerns, such as the risk of 'brain-jaking'.
SOURCE
Project team Privacy 2020 https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf

NUMBER | TITLE
482 | Smart communities
SUMMARY DESCRIPTION
Smart community or a smart city generally refer to a city or locality that integrates ICT and IoT sensors into its traditional infrastructure (e.g. roads, parks, buildings, etc.) with the aim of connecting and enhancing lives of its citizens and providing responsive environments. The importance and impact of smart cities will increase with the trends towards urbanization, as 70 % of the world's population is estimated to live in cities by 2050. Because of the vast amounts of data collection and consolidation possible in these wired cities, there are significant concerns about the risks to individual privacy, particularly with respect to sensitive information (e.g. facial recognition, mobility data, etc.) and deployment of a wide range of sensors that capture data in public space. Limited individual control and the impact of security breaches could expose people to significant risks.
SOURCE
Project team Privacy 2020 https://fpf.org/wp-content/uploads/2020/01/FPF_Privacy2020_WhitePaper.pdf

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
— at the following standard number: +32 22999696,
— via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/write-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KJ-01-26-322-EN-C

Publications Office
of the European Union

ISBN 978-92-68-42190-1