WHITE PAPER

Ensuring a Secure Future: Comprehensive Insights into 6G IoT Security and Privacy

AUTHORS
from the SecureCyber Cluster

Arcadian-IoT

Alexandru GLIGA, Ovidiu DIACONESCU - BOX2M
Ross Little ARMITT - Atos
Pedro COLAREJO - Load

IDUNN

Saeid SHEIKHI - University of Oulu, Oulu, Finland

ELECTRON

George ANDRONIKIDIS - Sidroco Holdings Ltd - SID
Panagiotis RADOGLOU-GRAMMATIKIS, Panagiotis SARIGIANNIDIS - University of Western Macedonia - UOWM

ERATOSTHENES

Konstantinos LOUPOS, Konstantinos DAFLOUKAS - INLECOM INNOVATION, Greece

SENTINEL

Ruben COSTA - UNINOVA
Siranush AKARMAZYAN - ITML

SPATIAL

Edgardo MONTES DE OCA, **Manh DUNG NGUYEN, Vinh HOA LA** - Montimage
Blanca ARREGUI, Giulia PASTOR - AUSTRALO
Chamara SANDEEPA, Thulitha SENEVIRATHNA, Bartlomiej SINIARSKI, **Madhusanka LIYANAGE** - UCD

SECANT

Anna ANGELOGIANNI, Thomas KROUSARLIS - UBITECH
Arnolnt SPYROS, Dimitrios KAVALLIEROS, Stefanos VROCHIDIS, Theodora TSIKRIKA - CERTH
Xavier ESPAÑOL, Monica CABALLERO - NTT DATA
Kalliopi LAPIDAKI - Adrestia R&D
Christos GRIGORIADIS - Security Labs Consulting
Sokratis NIFAKOS - Karolinska Institutet
Sergiu MARIN - Polaris Medical
Long MENG - University of Surrey
Saber MHIRI - i2CAT

TRUST aWARE

Juan TAPIADOR - Universidad Carlos III Madrid (UC3M), Spain
Narseo VALLINA - IMDEA Networks (IMDEA), Spain

Abstract

This whitepaper, "Ensuring a Secure Future: Comprehensive Insights into 6G IoT Security and Privacy", comprehensively analyses the security and privacy challenges associated with 6G-enabled Internet of Things (IoT) systems. As 6G technology evolves from previous generations, it promises unprecedented advancements in data transfer speeds, reduced latency, and widespread connectivity. These advancements will significantly impact the IoT ecosystem, which connects myriad devices and enables seamless data exchange. However, this increased connectivity also introduces new cybersecurity threats and privacy concerns.

The whitepaper considers the evolution of 6G IoT cybersecurity, exploring key challenges and potential solutions. It examines research projects, such as TRUST-AWARE, Arcadian-IoT, ELECTRON, IDUNN, ERATOSTHENES, SENTINEL, SECANT and SPATIAL, which address specific security and privacy issues in IoT applications, including smart homes, healthcare, and industrial and businesses environments. Additionally, it discusses the role of AI-empowered security techniques in enhancing real-time anomaly detection and response within 6G IoT networks.

This research focuses as well on analyzing advanced encryption mechanisms designed to secure wireless networks and infrastructures against post-quantum security risks, ensuring the safety and privacy of communication networks in an increasingly connected world.

The aim of this whitepaper is to guide stakeholders in understanding and addressing the complex security and privacy demands of the 6G IoT era, ensuring a secure and resilient connected world by providing insights into these critical areas.

Content

Introduction

The Concept of 6G and its Evolution from Previous Generations of Wireless Communication

The sixth generation of wireless communication, represents the next frontier in mobile connectivity, promising unprecedented speeds, ultra-low latency, and seamless integration of advanced technologies. While 5G focused on enhancing mobile broadband, massive machine-type communications, and ultra-reliable low-latency communications, 6G aims to transcend these capabilities by incorporating new features such as holographic communication, tactile internet, and ubiquitous AI integration. The evolution from 1G through 5G has seen significant advancements: from basic voice communication in 1G to high-speed data and robust connectivity in 5G. Each generation improved upon the last by increasing data rates, reducing latency, and enhancing reliability. 6G is expected to deliver peak data rates of up to 1 Tbps, latency as low as microseconds, and the capacity to support up to 10 million devices per square kilometer. This leap will enable transformative applications, such as advanced augmented reality (AR), virtual reality (VR), and the fully realized Internet of Things (IoT) ecosystem, marking a paradigm shift in how we interact with the digital world.

The role of IoT in Connecting Devices and Enabling Data Exchange

The sixth generation of wireless communication, represents the next frontier in mobile connectivity, promising unprecedented speeds, ultra-low latency, and seamless integration of advanced technologies. While 5G focused on enhancing mobile broadband, massive machine-type communications, and ultra-reliable low-latency communications, 6G aims to transcend these capabilities by incorporating new features such as holographic communication, tactile internet, and ubiquitous AI integration. The evolution from 1G through 5G has seen significant advancements: from basic voice communication in 1G to high-speed data and robust connectivity in 5G. Each generation improved upon the last by increasing data rates, reducing latency, and enhancing reliability. 6G is expected to deliver peak data rates of up to 1 Tbps, latency as low as microseconds, and the capacity to support up to 10 million devices per square kilometer. This leap will enable transformative applications, such as advanced augmented reality (AR), virtual reality (VR), and the fully realized Internet of Things (IoT) ecosystem, marking a paradigm shift in how we interact with the digital world.

Evolution of 6G-IoT Cybersecurity

As the 6G era begins, the cybersecurity landscape for IoT will face new challenges and opportunities. The massive expansion of connected devices and the exponential increase in data flow necessitate robust and adaptive security measures. In previous generations, IoT cybersecurity focused primarily on securing devices and networks against basic threats and vulnerabilities. However, the evolution of 6G will demand more sophisticated and proactive approaches to cybersecurity, driven by the increased complexity and scale of IoT networks. Enhanced encryption techniques, advanced authentication mechanisms, and decentralized security models will be essential to safeguard the integrity, confidentiality, and availability of IoT systems. Artificial Intelligence (AI) and Machine Learning (ML) will play a crucial role in identifying and mitigating threats in real-time, enabling predictive and autonomous security measures. Furthermore, the integration of blockchain technology can provide transparent and tamper-proof data transactions, enhancing trust and accountability within IoT ecosystems. As 6G aims to support critical applications such as autonomous vehicles, remote healthcare, and smart cities, ensuring robust cybersecurity will be paramount to prevent disruptions, protect sensitive information, and maintain the resilience of IoT infrastructures. The continuous evolution of cybersecurity in the 6G IoT landscape will be a dynamic and ongoing process, requiring collaboration, innovation, and vigilance to address emerging threats and vulnerabilities effectively.

Key security and Privacy challenges of 6G and IoT deployments

01

1.1

Security and privacy challenges in healthcare environments

Healthcare is becoming increasingly digitised: from the use of electronic health records to the use of mobile health apps and health care devices, telehealth and telemedicine services. During the last years, also IoT applications are proliferating in the medical field.

The integration of IoT solutions facilitates medical procedures and the clinical status reporting of patients which require continuous medical supervision (e.g., in-house surveillance)[1]. While this digital transformation and the integration of IoT has improved the healthcare industry in many ways, the integration of such solutions could also expose the organisation to serious security and privacy threats[2].

There are several reasons why the healthcare industry is subject to cyber-attacks[3]. Firstly, there is a wide array of hardware and software components used within healthcare: some may have both access to patient data and vulnerabilities of high risk; and they possess varying levels of security. Some may have robust security measures, while others, especially older systems, may have vulnerabilities that make them easy targets for cyberattacks. This diversity makes it challenging to implement uniform security measures across all systems. Furthermore, the rapid adoption of new technologies, driven by the need to improve patient care and operational efficiency, often leads to security being either simply an afterthought or outpaced[4].

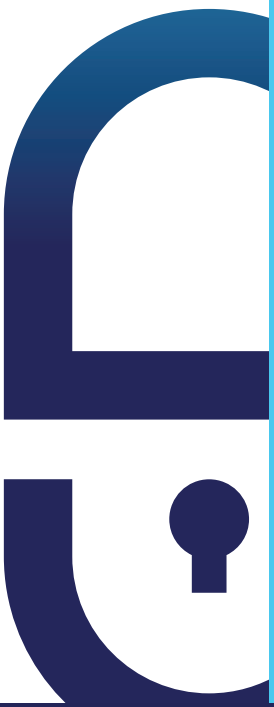
This lag in security implementation creates windows of opportunity for cybercriminals to exploit vulnerabilities. Secondly, patients' health data can be abused in a variety of malicious ways including identity theft and insurance fraud and therefore, have high value on the black market. Thirdly, healthcare institutions as victims of cyber-attacks are likely to quickly accede to demands due to the potential threat to human lives and the legal obligations to ensure patient safety, protect patient data, and ensure their services remain operational. This perceived willingness to, for instance, pay ransoms to regain access to critical systems and data, make healthcare institutions particularly attractive targets for cybercriminals.

Focusing on IoT devices, they have the potential to collect a significant amount of sensitive information, ranging from precise location data to highly personal health records. As a result, the incorporation of this complex network of interlinked devices gives rise to significant apprehensions regarding the privacy of individuals, given the vast amount of data they generate that is susceptible to potential compromise. According to the recent data breach investigation report by Verizon[5], there were recorded 655 data breach incidents in the Healthcare sector from which the 472 have confirmed data disclosure. With regard to the compromised data, 66% were personal, 55% medical, 32% compromised credentials and 20% other breaches. Therefore, the establishment of robust Incident Response Capabilities (IRC) within the healthcare sector is not only a matter of importance but also a necessity. The sector, which has been greatly improved and made more convenient by the use of IoT devices[6], is not devoid of risks throughout its supply chain.

The adaptation of medical IoT devices, known as Internet of Medical Things (IoMT) devices, by healthcare organisations increases the risk of threats against the security and privacy os patient data. IoMT devices inherit the vulnerable nature of IoT, making them susceptible to various cyber-attacks. As a result, the organisation is exposed to more cyber-threats, including attacks which exploit network vulnerabilities to self-propagate to more devices. In particular, the attackers exploit vulnerabilities in IoMT devices to gain access to the system of the healthcare organisation. The SweynTooth vulnerability is a widely documented case of a cyber-attack that occurred within the healthcare sector, significantly impacting devices equipped with Bluetooth technology, specifically those that rely on Bluetooth Low Energy (BLE) for their wireless communication[7]. The foremost driver behind cybersecurity challenges often traces back to hardware-related issues, with many devices still relying on legacy hardware without adequate protective mechanisms or proprietary closed-source software. Smaller establishments with limited resources find themselves at a severe disadvantage, and even among non-technical users, there exists a palpable absence of a pervasive cybersecurity culture.

Consequently, the wide adaptation of IoMT devices in healthcare domain raises several security challenges affecting both the system as well as the users (e.g., healthcare professionals, patients): (i) The exchanged data between IoMT devices mostly includes sensitive patient data such as medical records[8]; (ii) The interaction of a vast number of IoMT devices and heterogeneous networks that connect them, raises complexity and incompatibility issues[9]; (iii) Most manufacturers of healthcare devices tend to intercorporate IoT solutions without utilising appropriate measures to address security and privacy risks; (iv) Considering that most IoMT devices exchange data over insecure wireless networks, they are susceptible to various attacks such as Man in the Middle (MITM) attack[10]; (v) Due to power and computational limitations, many IoT devices do not leverage any built-in encryption mechanism. The exchange of sensitive data with the lack of proper encryption mechanisms, could lead to digital harm of the patient which concerns loss of privacy, Identity theft, and service unavailability[11].

Concerning the movement to 6G, as this technology emerges on the horizon, it brings with it a wave of innovation and unprecedented capabilities. However, with these advancements come significant security challenges that demand thoughtful solutions. These challenges include vulnerabilities in the highly complex and interconnected 6G networks, privacy concerns in the era of data-intensive applications, the necessity for robust authentication and authorization mechanisms, security of IoT devices, and the looming threat of quantum computing. Addressing these issues is paramount to the success and security of 6G networks. In this context, self-sovereign identity (SSI) offers a decentralized and innovative approach to identity management that directly tackles some of those challenges. SSI empowers individuals with control over their personal data, enhances privacy by allowing selective data disclosure, strengthens authentication and authorization through cryptographic methods, secures IoT devices with verifiable identities, and prepares the ecosystem decoupling traditional centralized trust to a decentralized and transparent technologies. By integrating SSI principles, 6G networks can not only meet these security challenges but also provide a foundation for trust and privacy in an increasingly interconnected digital world.



1 Gao, J., Wang, H., & Shen, H. (2020, May). Smartly handling renewable energy instability in supporting a cloud datacenter. In 2020 IEEE international parallel and distributed processing symposium (IPDPS) (pp. 769-778). IEEE.

2 Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98, 660-671.

3 Sendelj R, Ognjanovic I. Cybersecurity Challenges in Healthcare. Stud Health Technol Inform. 2022 Oct 26;300:190-202. doi: 10.3233/SHTI220951. PMID: 36300412.

4 Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648

5 https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

6 Sills, M., Ranade, P., & Mittal, S. (2020, November). Cybersecurity Threat Intelligence Augmentation and Embedding Improvement-A Healthcare Usecase. In 2020 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE.

7 US-CERT. Sweyntooth cybersecurity vulnerabilities. https://us-cert.cisa.gov/ics/alerts/ics-alert-20-063-01

8 F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," in 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Oct. 2017, pp. 112–120. doi: 10.1109/LCN.Workshops.2017.72.

9 P. Waurzyniak, "Securing Manufacturing Data in the Cloud," Advanced Manufacturing, 28-Jun-2016. [Online]. Available: http://advancedmanufacturing.org/securing-manufacturing-data-cloud/.

10 Mamta and S. Prakash, "An overview of healthcare perspective based security issues in Wireless Sensor Networks," in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 870–875.

11 M. Aijaz, M. Nazir, and M. N. Anwar, "Classification of Security Attacks in Healthcare and associated Cyber-harms," in 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT), Dec. 2021, pp. 166–173. doi: 10.1109/ICACFCT53978.2021.9837349.

1.2

Privacy Risks in Smart Home IoT Devices: Challenges and Research Directions

Smart home IoT devices can cause privacy harm to users due to their ability to sense the environment and user activities. Yet, the proprietary and distributed nature of modern IoT products makes it difficult to automatically and empirically assessing their inherent threats and regulatory compliance.

The proliferation of Smart Home Internet of Things (IoT) devices has ushered in a time of unprecedented convenience and automation in our daily lives. These devices encompass a wide spectrum of applications, from thermostats that adjust temperature settings based on occupants' preferences to voice-activated assistants that control various household functions.

These innovations have undoubtedly transformed domestic life, but they also raise significant concerns regarding user privacy. Smart home IoT devices, with their remarkable ability to sense and interact with their environment, to monitor and react to user activities, and their ability to communicate with other devices and applications in the local network possess the potential to cause privacy harms to individuals in ways that were previously inconceivable.

This white paper provides an overview of privacy risks associated with smart home IoT devices, shedding light on the research and technical challenges that have so far hindered the automatic assessment of these risks and regulatory compliance.

Privacy Risks in Smart Home IoT Devices

Smart home IoT devices, equipped with an array of sensors and connected to the Internet, can collect a wealth of data about users, the network, and their environments. This data encompasses information on daily routines, preferences, and even personal conversations.

Several distinct privacy risks emerge from the capabilities of these devices:

1. Data Leakage[12]: Smart home IoT devices can inadvertently or intentionally transmit sensitive user data to remote servers but also to mobile apps running on the same local network[13], potentially falling into the hands of malicious actors or unauthorized third parties.
2. Profiling and Behavioral Analysis: The data gathered by these devices can be used to create detailed user profiles, enabling advertisers and other entities to target individuals with highly personalized content or even for state surveillance.[14] This is both a privacy and a security concern.
3. Eavesdropping and Audio Surveillance[15]: Voice-activated devices have come under scrutiny for their ability to record conversations and transmit them to cloud servers, raising concerns about unwarranted audio surveillance.
4. Unauthorized Access[16]: Inadequate security measures can render smart home IoT devices vulnerable to hacking, allowing unauthorized individuals to gain control over them. This opens the door for additional security and privacy issues,[17] from botnets to remote control of IoT Deployments.[18]

Challenges in Assessing Privacy Risks

As privacy concerns mount, governments and regulatory bodies are beginning to take a more active role in holding manufacturers accountable for data protection and user privacy. The new EU Cyber Resilience Act aims to enforce security requirements for digital products like IoT devices by establishing a framework for secure development and empowering users to make security-aware decisions. This is complemented by a European-wide Cybersecurity Certification Framework (ECCS) and the new NIS 2 Directive, which puts in place cybersecurity requirements including supply chain measures. Key regulatory considerations include:

- Data Protection Laws: Manufacturers must adhere to data protection laws, such as the
- European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), by implementing robust data protection measures and ensuring transparency in data handling practices.
- Security-and-Privacy-by-Design: Integrating security and privacy features into the design and development of smart home IoT devices is essential to preemptively address security and privacy risks.
- Regular Auditing and Testing: Manufacturers should conduct regular privacy audits and security testing of their devices to identify and rectify vulnerabilities and privacy issues.
- Privacy Labels and Certifications: The establishment of standardized privacy labels and certifications for smart home IoT devices can assist consumers in making informed choices while promoting compliance within the industry.

However, ensuring that smart home IoT devices comply with existing security and privacy regulations and standards is a paramount technical and research challenge. In fact, the detection and mitigation of privacy risks associated with smart home IoT devices are hindered by multiple socio-technical challenges, as we discussed in prior work: [19]

- Proprietary Nature of Devices: Many smart home devices are proprietary (i.e., closed source) in nature, making it challenging for independent researchers to access and analyze their firmware and software for potential vulnerabilities or privacy risks.
- Heterogeneity of Devices: The diverse range of smart home IoT devices, each with its own set of sensors, communication protocols, and operating systems, complicates the development of standardized privacy assessment tools, while adding avenues for exhaustively analyzing the security and privacy properties of devices when interconnected with arbitrary devices in the local network.
- Environmental Complexity: The smart home environment itself is complex, with multiple devices interacting with each other. As we demonstrate in a recent analysis, mobile applications and advertising SDKs can abuse standard IoT protocols like UPnP and mDNS to harvest information from the users and the household, such as geolocation data, social structures and socio-economic aspects. 2 Exhaustively and systematically understanding the privacy implications of these interactions requires sophisticated analysis techniques.
- Lack of User Awareness: Users often remain unaware of the data collection and sharing practices of their smart home devices, making it difficult for them to take proactive steps to protect their privacy.

Conclusion

Smart home IoT devices, with their extraordinary capabilities, have the potential to revolutionize our daily lives. However, they also introduce significant security and privacy threats that demand comprehensive assessment and mitigation. Overlooking these risks can lead to violations of user privacy and potentially catastrophic attacks as demonstrated by the Mirai botnet[20].

This paper has outlined the security and privacy risks associated with smart home IoT devices and examined the challenges in assessing these risks, with emphasis on the importance of regulatory compliance and enforcement. To safeguard user privacy in the era of smart homes, a multidisciplinary approach that combines technical innovation, regulatory oversight, and user empowerment is imperative.

[12] Ren, J., Dubois, D. J., Choffnes, D., Mandalari, A. M., Kolcun, R., & Haddadi, H. (2019, October). Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In Proc. ACM IMC 2019.

[13] A. Girish, T. Hu, V. Prakash, D. Dubois, S. Matic, D. Huang, S. Egelman, J. Reardon, J. Tapiador, D. Choffnes, N. Vallina-Rodriguez. (2023). In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes. In Proc. ACM IMC 2023.

[14] Farrell, S., Badii, F., Schneier, B., & Bellovin, S. M. (2023). RFC 9446 Reflections on Ten Years Past the Snowden Revelations.

[15] Dubois, D. J., Kolcun, R., Mandalari, A. M., Paracha, M. T., Choffnes, D., & Haddadi, H. (2020). When speakers are all ears: Characterizing misactivations of iot smart speakers. Proceedings on Privacy Enhancing Technologies, 2020(4).

[16] Edu, J., Aran, X. F., Such, J., & Suarez-Tangil, G. (2021). SkillVet: Automated traceability analysis of Amazon Alexa skills. IEEE Transactions on Dependable and Secure Computing.

[17] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

[18] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[19] Girish, A., Prakash, V., Egelman, S., Reardon, J., Tapiador, J., Huang, D. Y., ... & Vallina-Rodriguez, N. (2022, December). Challenges in inferring privacy properties of smart devices: Towards scalable multi- vantage point testing methods. In Proceedings of the 3rd International CoNEXT Student Workshop (pp. 26-28).

[20] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.

1.3

Risk assessment and management in power and electrical systems; Tools and services for applying failure mitigation in energy infrastructures;Exploring post-quantum cryptography in the electrical grid.

Effective risk assessment and management are crucial to safeguard these systems against evolving threats.

Innovative schemes and algorithms for federated intrusion and anomaly detection are essential to proactively identify and neutralize potential security breaches in the energy sector. Additionally, advanced tools and services for failure mitigation can help maintain the resilience and reliability of energy infrastructures.

In the face of emerging technological challenges, exploring post-quantum cryptography in the electrical grid becomes imperative. Quantum computing poses a significant threat to conventional encryption methods, necessitating the development of robust post-quantum encryption protocols. This whitepaper delves into the multifaceted aspects of securing the connected world, with a particular focus on 6G IoT security and privacy, highlighting the importance of future-proofing our energy infrastructures against quantum-era threats.

The convergence of 6G and IoT technologies with power and electrical systems introduces several critical security and privacy challenges that necessitate effective risk assessment and management. One of the foremost concerns is the preservation of data privacy and confidentiality, given the extensive data exchange in these systems. Protecting sensitive power system data from unauthorized access is paramount, demanding strong encryption and access control mechanisms. Device authentication and authorisation also emerge as pivotal challenges to ensure that IoT devices are accurately identified and authorized to access critical infrastructure, preventing malicious infiltration.

Moreover, the resilience of power and electrical systems against cyberattacks is crucial. These systems are attractive targets for various threats, including malware, DDoS attacks, and zero-day vulnerabilities. To counter these risks, robust intrusion detection systems, regular security assessments, and comprehensive incident response plans are indispensable. The diversity of IoT devices and 6G technologies can lead to issues related to interoperability and standards. Without uniform security protocols, vulnerabilities may emerge due to fragmented security practices. Thus, the establishment and enforcement of industry-wide security standards become vital.

Supply chain security is another area of concern, given the global nature of IoT and 6G device manufacturing. Supply chain attacks, involving unauthorised modifications or hardware compromises during production, can jeopardise the entire power system's security. Stringent supply chain security measures, including hardware attestation and verification, are necessary safeguards. Lastly, human factors and insider threats continue to be significant vulnerabilities. Human errors or malicious actions by individuals with privileged access can result in data breaches or system failures. Addressing these risks requires continuous monitoring, robust employee training, and stringent access controls. In conclusion, as 6G and IoT technologies transform power and electrical systems, proactive management of security and privacy risks is essential. This involves the integration of robust security measures, ongoing risk assessment, and strict adherence to industry standards to uphold the reliability and resilience of power and electrical infrastructure.

Based on the aforementioned remarks, ELECTRON provides a comprehensive framework for cybersecurity management in the energy sector based on three main pillars: (a) collaborative risk assessment and certification, (b) federated detection and (c) dynamic mitigation. First, the ELECTRON mechanisms for risk assessment are provided through a collaborative risk and certification framework called BORDER. BORDER is structured around three essential components, each playing a distinct role in enhancing security and functionality.

First, the Collaborative Risk Assessment System (ARMY) takes charge of dynamic and cooperative risk assessment procedures. Second, the Dynamic Asset Certification System (DARCY) is responsible for certifying EPES assets in real-time, integrating the perspectives of the certification authority, manufacturer, and EPES end-users. DARCY relies on Manufacturer Usage Description (MUD) and its variant, Threat Manufacturer Usage Description (Threat MUD), to accomplish this task effectively. Lastly, the Honeynet as a Service (HaaS) component handles the deployment of EPES honeypots in a cloud-based environment, all while preserving the unique characteristics of EPES entities/devices, including their Internet Protocol (IP) addresses within the EPES production/internal network.

More specifically, ARMY plays a pivotal role in facilitating ELECTRON's collaborative risk assessment through innovative mathematical modules, interdependency graphs, and quantification techniques deployed across multiple levels. It serves as the fundamental backbone of the ELECTRON framework by executing vital risk assessment procedures essential for enforcing security policies within the platform. Specifically, ARMY employs a comprehensive and integrated approach to risk assessment, encompassing the identification and management of assets, threats, and vulnerabilities.

This approach enables ARMY to deliver impact and risk assessments on a per-asset basis, per attack path, and for the entire Electrical Power and Energy System (EPES) infrastructure. To carry out these crucial functions, ARMY draws upon topology information sourced from the underlying SDN-based infrastructure, asset vulnerability details, and MUDs. This approach offers distinct advantages over traditional methods of risk assessment.

Next, DARCY is designed to provide dynamic certification for EPES assets, driven by two distinct perspectives: (a) the viewpoint of the certification authority and (b) the standpoint of the manufacturer. DARCY's primary responsibility involves vigilant monitoring of MUD and Threat MUD Files, along with their updates, to ensure the smooth operation and status of EPES assets.

The DARCY system is structured into two key components: one located on local premises, known as the Threat MUD Manager, and the other situated on manufacturer premises, referred to as the MUD File server. In the first case, DARCY concentrates on retrieving Threat MUD files and translating them into actionable policies. In the second case, it focuses on generating MUD files for EPES devices and makes these descriptors available to any stakeholders involved in the certification process. This is achieved by continually updating the description files stored within the MUD File Servers and Threat MUD file server, ensuring that all parties have access to the latest information pertaining to EPES assets.

Finally, ELECTRON HaaS is responsible for provisioning proactive EPES honeynets, eliminating the need for physical deployment on the EPES organization's premises, thereby reducing deployment, configuration, and maintenance costs. Following a cloud-based "*-as-a-Service" model, ELECTRON HaaS enables the creation of honeynets consisting of cloud-deployed honeypots. It includes a specific component serving as a gateway between the Cloud honeynet and the EPES network.

HaaS comprises three crucial submodules: the Honeypot Manager Core Backend (a), which provides administration and orchestration functions; the Honeypot Manager Core Frontend (b), offering a user-friendly graphical interface; and the Honeypot Manager Agent (c), serving as the link between the cloud honeynet network and the local EPES infrastructure, ensuring seamless integration and communication.

The second pillar of ELECTRON focuses on the federated intrusion detection. In particular, ELECTRON implements a set of intrusion detection systems for the energy domain, taking full advantage of a federated schema. More specifically, ELECTRON introduces a Federated Intrusion Detection and Prevention System (FIDPS) which plays a critical role of identifying intrusions targeting EPES assets, utilizing AI models that have undergone training via federated learning methods. This approach places a strong emphasis on preserving the data privacy of EPES organizations and infrastructures during the training process. Specifically, FIDPS possesses the capability to detect specific cyberattacks aimed at industrial communication protocols, including Modbus/Transmission Control Protocol (TCP), International Electrotechnical Commission (IEC) 61850, IEC 60870-5-104, IEC 60870-5-102, and Profinet. This detection is based on the distinctive characteristics and requirements of ELECTRON end-users. FIDPS leverages network flow statistics from TCP/IP and the attributes of application-layer protocols to achieve this objective. Furthermore, upon detecting potential threats, FIDPS can proactively recommend the implementation of appropriate firewall and Software-Defined Networking (SDN) rules to thwart cyberattacks in a timely manner.

Finally, based on the risk assessment and detection outcomes, ELECTRON introduces a mitigation and prevention framework called BRIDGE. In particular, BRIDGE consists of four core elements focused on using SDN technology and electrical-related measures to address intrusion and anomaly mitigation.

The first component is called Network Isolation and Recovery mOdule (NIRO). NIRO serves as a data analysis engine primarily dedicated to EPES (Electric Power and Energy Systems), with its primary function being to assist SDN-C (Software-Defined Networking Controller) in executing the necessary mitigation measures for safeguarding the SDN-based EPES network. NIRO's role involves the processing of security alerts generated by ARMY, as well as potential mitigation actions suggested by DARCY. Depending on the nature of the cybersecurity threat detected, NIRO may either redirect malicious network traffic to a security application, such as a honeypot, or terminate the communication altogether.

Furthermore, NIRO takes into account the sensitivity and criticality of EPES communications. To ensure the appropriate Quality of Service (QoS), NIRO dynamically restructures network flows between hosts using constrained optimization techniques, often employing genetic algorithms. Additionally, in cases involving cybersecurity incidents affecting Phasor Measurement Units (PMUs), NIRO employs an intelligent Decision Support System (DSS) based on matchmaking algorithms. This DSS is designed to restore observability and maintain communication links between PMUs and Phasor Data Concentrators (PDCs).

The second component named Intentional iSOlation anD IslaNding modulE (ISODINE) takes on the responsibility of proactively computing and implementing islanding strategies, creating microgrids and nanogrids with the aim of guaranteeing uninterrupted electrical grid operation in the face of severe cyberattacks or critical system faults.

Utilizing advanced Artificial Intelligence (AI) techniques, ISODINE identifies anomalies indicative of imminent faults and promptly isolates affected grid segments to prevent blackouts and the propagation of adverse cascading effects.

Next, ElectricaL grId reStoration modulE (ELISE) takes on the responsibility of restoring and ensuring the normal operation of the established microgrids and nanogrids, particularly in terms of voltage and frequency stability. In a more comprehensive explanation, ELISE employs a Multi-Agent System (MAS) that coordinates and implements a three-tier control structure. The primary and secondary control levels utilize a hybrid centralised/distributed architecture to eliminate single points of failure.

Meanwhile, a centralized optimal dispatch agent, located at the tertiary control level, ensures the economically efficient operation of each microgrid. Furthermore, various subcomponents within ELISE continuously monitor real-time operations and, in response to any deviations, provide instructions to the relevant asset agents to make necessary adjustments.

Finally, the main objective of BEAM is to establish an energy trading platform based on blockchain technology. This platform will operate within a private fabric network, facilitating direct peer-to-peer energy trading among prosumers.

BEAM intends to utilize a permissioned blockchain system, wherein a set of deployed smart contracts will oversee data sharing by encoding information with relevant data references and shared standards. BEAM is designed to be compatible with the Vickrey-type e-auction format. In this system, each participant can either purchase or sell energy based on their current energy holdings. The Vickrey auction mechanism is characterized by sealed bids, meaning that participants submit their bids without knowledge of other participants' bids. This encourages participants to offer bids that reflect their genuine valuations of the energy they seek to acquire.

1.4

Overview of data protection and cybersecurity challenges faced by SMEs/MEs

European Small to Medium size Enterprises/ Micro Enterprises (referred to henceforth collectively as SMEs) are an important driver for innovation and growth in the EU and act as a catalyst for digital growth (ENISA, 2021[21]).

However, most of the European SMEs, central within EU enterprise policy, face multiple challenges related to personal data protection; ranging from awareness to a clear and practical roadmap to compliance, unlike large enterprises, SMEs lack access to enterprise-grade cybersecurity (CS) technology and capacity-building for compliance, making them increasingly often victims of costly data breaches.

Furthermore, SMEs with inadequate personal data security and limited personnel and resources face difficulties in understanding the risks associated with the development of their technologies and their impact. Despite the constant adaptation of new technologies, especially during the COVID-19 crisis, the level of SMEs information security and privacy standard adoption is relatively low. During the COVID-19 pandemic many SMEs transferred a large portion of their work online by using Cloud services or other means, as well as by enabling remote work.

This caused an increase in CS challenges in the need for a consistent and iterative approach for identifying, assessing and managing risk. In a recent ENISA study, investigating 249 SMEs EU-wide for their overall CS awareness and related concerns, 80% of the surveyed companies reported that CS issues would have a serious negative impact on their business within a week of the issues happening, and 57% saying they would most likely become bankrupt or go out of business (ENISA, 2021).

ENISA identified the major Cybersecurity and Personal Data Protection (PDP) challenges which these enterprises face, based on an EU-wide survey. These are many and of varying types, although a prevalent theme evident among them is the lack of SME management motivation and support. Undoubtedly, when management is aware and motivated towards CS, it will commit to the necessary budget, allocation of resources and the oversight for the effective implementation of these guidelines and practices. Another major aspect is the lack of understandable and workable guidelines for SMEs in coping with these challenges.

Novel tools and services for enabling automated security, privacy and data protection

SENTINEL aspires to bridge the cybersecurity and data protection gaps by boosting SMEs capabilities SMEs' capabilities in this domain through innovation at a cost-effective level. It is designed to address the above-mentioned challenges by mapping security and privacy challenges or barriers to a specific set of requirements which, in turn, is addressed by tools/services of the SENTINEL platform.

A core SENTINEL ambition is to provide tangible benefits for SMEs looking to improve their security privacy awareness and adopt measures towards the protection of personal data for their customers, employees, partners, beneficiaries, etc. This is proposed, having in mind the concept that, security and data breaches are risks not just to the SME's assets and reputation but, more critically, to the fundamental rights and freedoms of individuals, which constitute core EU values, protected under the GDPR.

SENTINEL's key competitive offering is the innovative and cost effective end-to-end digital privacy and data protection framework. SENTINEL provides a one-stop shop platform for SMEs to choose from a plethora of services, (including GDPR CSA (GDPR Compliance Self-Assessment), ROPA (Records of Processing Activities), DPIA (Data Protection Impact Assessment), CSRA (Cybersecurity risk assessment)) that are tailored to their needs, infrastructure, and capabilities. Furthermore, its Cyber Range provides a gamified training and educational content to raise awareness of cybersecurity and data protection best practices and the ability for SMEs to test, evaluate, and train in real-world cyber threat scenarios. In addition, its Identity Management system enables the creation of centralized, trusted digital identities for individuals, relates these identities with specific roles and access rights, and finally uses these identities to securely leverage both user data and SME data, so SENTINEL participants may be GDPR compliant in terms of data portability and data sovereignty.

Apart from its own mechanisms, the SENTINEL platform can also suggest external open-source tools and training to fill the identified gaps. A wide list of free and/or open-source tools covers all the Organisational and Technical Measures (OTM) capabilities that are subject to the SENTINEL methodology.

[21] CYBERSECURITY FOR SMEs: Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), 2021

Finally, the SENTINEL platform can suggest relevant external training resources that can aid the SME users in enhancing their overall privacy and security.

In a nutshell, SENTINEL offers a novel approach to integrated and obtainable privacy and personal data protection and cybersecurity for SMEs at a minimal cost. SENTINEL also helps market opportunity generation for industry partners, while the research community exploits an upgraded level of technological useful sources.

GDPR Compliance Self-Assessment and Data Protection Impact Assessment Framework

For SMEs handing personal data, complying with GDPR implies to implement appropriate Organisational and Technical Measures (OTMs) to ensure and to be able to demonstrate that data processing is performed in accordance with ("GDPR, Art. 24, Paragraph 1") requirements.

These OTMs aim at meeting data protection principles ("GDPR, Art. 5, Paragraph 2"). In addition to these measures related to the handling of personal data, companies must also implement appropriate data protection policies ("GDPR, Art. 24, Paragraph 2"). Within the SENTINEL project, GDPR Compliance Self-Assessment (GDPR CSA) has been developed to allow SMEs to verify whether OTMs are implemented and whether they are appropriate and effective. Based on ISO/IEC 330xx processes assessment method, GDPR CSA uses a process assessment model that organises data protection requirement into six data protection process: Record, Personal Data Lifecycle Management (PDLM), Rights, Consent, Data Protection Management (DPMAN), and Breach.

These processes allow to structure the collection of information related to OTMs implemented. Assessment of their appropriateness and effectiveness depends on the Processing Activity (PA's) privacy risk level. Aiming to allow SMEs to identify (through assessment) and minimise (through recommendations) the risks associated with their personal data processing activities, a DPIA Toolkit has been designed within the SENTINEL project. The DPIA toolkit is a self-assessment module that performs an automated assessment of Processing Activities. It offers the DPIA questionnaire to SENTINEL's self-assessment engine and is based on state-of-the-art tools and questionnaires tailored to the needs of SENTINEL. It comprises 60-70 questions, each offering a choice of "yes" or "no" responses. Following the submission of a response, based on the answers the likelihood, impact the risk score is calculated and returned to the SENTINEL platform for each processing activity, providing some qualitative metadata based on the aforementioned metrics, which can be used both for the presentation and storage of the self-assessment results and for the subsequent recommendations.

Simulations and training through Cyber Range Platform

Aiming at providing an educational, collaborative platform with the best user experience for the SMEs for simulating real-life cybersecurity scenarios the SENTINEL partners have been created a CyberRange gamified environment that is integrated within the SENTINEL platform.

This Gaming interface provides a novel training approach based on the CyberRange to raise awareness of end users. In such a manner, the users can learn in an interactive way the best practice to better protect personal and sensitive data. Four (4) scenarios that demonstrate mechanisms of protection for multiple data storage and accessibility threats have been created to raise SMEs awareness. The covered cyber threats are phishing, malware attack, unsafely removed files, unencrypted disk files, social media presence, password guessing, password reused, and unprotected password. The integration of the Gaming Interface in the SENTINEL platform has been made with OpenID solution. Currently, SENTINEL users can directly be connected to the gaming interface from the SENTINEL platform and test the interface.

1.5

XAI framework for resilient 5G IoT traffic analytics

The rise in encrypted network traffic, driven by the use of HTTPS and Virtual Private Networks (VPN), poses challenges for traditional traffic analysis tools, as they struggle to detect malicious activity.

This, coupled with the sheer volume of traffic from mobile and IoT devices, requires advanced Artificial Intelligence (AI)-based techniques for real-time anomaly detection. We developed three AI-based security applications that correspond to three main steps of Intrusion Detection and Response. Firstly, the Traffic Classification application characterizes network traffic to identify certain types of normal user activities, such as web browsing, chatting, or video streaming. Secondly, the Attack Detection application differentiates between malicious traffic and legitimate traffic to detect popular cyberattacks in 5G or IoT environments. Finally, the Root Cause Analysis application employs a similarity-based machine learning approach to discover the root causes of problems in order to quickly identify appropriate solutions.

While AI holds promise for security management in 5G and IoT networks, challenges such as limited real datasets, lack of explainability, and vulnerability to adversarial attacks need to be addressed. eXplainable Artificial Intelligence (XAI) has emerged, aiming to provide users with a rationale for understanding AI system outputs and fostering trust. However, existing explainable frameworks still lack comprehensive support for adversarial attacks and defenses. Therefore, in addition to accuracy and performance, new requirements concerning trustworthiness, transparency, and robustness also need to be considered.

In the SPATIAL project an AI Platform has been designed and implemented by Montimage , an XAI framework with an intuitive and user-friendly interface for network traffic analysis and classification in 5G/IoT networks. It comprises two principal components: Network Traffic Analysis and XAI for Resiliency.

Firstly, the Network Traffic Analysis component aims to fulfill the need for effective analysis and classification of encrypted traffic using advanced AI techniques. It gathers raw traffic data from networks or 5G/IoT testbeds and constructs AI models to classify vectorized network traffic data for diverse objectives, such as classifying user activity or detecting anomalies in encrypted traffic. Secondly, the XAI for Resiliency component aims to enhance the robustness of AI models built within the Network Traffic Analysis module, making them more resilient against different types of adversarial machine learning attacks. This component injects evasion and poisoning adversarial attacks, such as label flipping attacks and Generative Adversarial Networks (GANs) based attacks, or integrates existing AI-based attack libraries for robustness analysis of AI models. It employs popular model-agnostic post-hoc XAI techniques, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations), to produce post-hoc global and local explanations of model predictions. Furthermore, this component analyzes the robustness of models against adversarial attacks via quantifiable resilience metrics and provides an XAI-based mechanism to detect the existence of adversarial attacks on AI-based systems.

Security of 6G IOT Applications deployments

02

2.1

Emergency and Vigilance

The forthcoming arrival of 6G technology is poised to usher in a new era for Internet of Things (IoT) applications, particularly within the renewable energy sector.

The promise of 6G IoT applications in the renewable energy chain lies in their potential to enhance sustainability and efficiency. However, this technological leap forward comes hand in hand with a host of security challenges that demand careful consideration and mitigation strategies to safeguard these vital systems. In particular, these security challenges are multifaceted.

They encompass preserving the privacy and confidentiality of extensive data exchanges, ensuring robust device authentication and authorisation mechanisms, bolstering resilience against cyber threats such as ransomware and supply chain vulnerabilities, addressing issues related to interoperability and standardized security protocols, implementing stringent supply chain security practices, and mitigating human-related security risks, including insider threats.

These challenges demand the adoption of end-to-end encryption, multi-factor authentication, cybersecurity training, regular vulnerability assessments, adherence to industry-wide standards, and the development of comprehensive incident response plans to safeguard the integrity and reliability of the critical systems underpinning renewable energy production and distribution.

Solutions to the security challenges presented by 6G IoT applications in the renewable energy sector encompass a multi-pronged approach. Implementing robust end-to-end encryption protocols ensures the secure transmission of data between IoT devices, safeguarding data privacy and confidentiality. Employing multi-factor authentication for device access enhances device authentication and authorization processes. Addressing human-related security risks necessitates specialised cybersecurity training for personnel involved in renewable energy systems.

Routine vulnerability assessments and penetration testing help identify and rectify system weaknesses proactively. Supporting and adhering to industry-wide security standards fosters interoperability and uniform security practices. Finally, the development and regular updating of comprehensive incident response plans are essential to minimizing downtime and data loss in the event of a security breach, collectively fortifying the reliability and resilience of these pivotal systems driving renewable energy production and distribution.

To conclude 6G IoT applications poised for integration into the renewable energy chain offer an inspiring vision of a sustainable and efficient future. Yet, the accompanying security challenges demand vigilant attention. By implementing robust security measures, endorsing industry standards, and maintaining a watchful eye for emerging threats, stakeholders can collectively ensure the reliability and resilience of these pivotal systems. In doing so, they contribute to the advancement of renewable energy and the pursuit of environmental sustainability.

Security of 6G IoT Applications for Emergency and Vigilance

The advent of 6G technology promises to evolve the revolution initiated with 4G and 5G to the way we connect and interact with the world around us. With its ultra-fast speeds, low latency, and massive device connectivity, 6G is set to empower a wide range of applications, including those dedicated to emergency response and vigilance. However, the exponential expansion of the Internet of Things (IoT) in these critical areas also raises significant concerns about security. Some security considerations can be taken in consideration for 6G IoT applications aimed at enhancing emergency response and vigilance:

- **Data Privacy and Encryption**

  6G IoT applications for emergency and vigilance will continue to rely heavily on data collection and sharing. This data may include real-time location information, vital health statistics, surveillance footage, and more. Ensuring the privacy of this data is essential. Robust encryption techniques should be employed to protect sensitive information from unauthorized access. End-to-end encryption ensures that only authorized parties can decipher the transmitted data, safeguarding individuals' privacy and confidential information.

Authentication and Access Control

Securing access to IoT devices and networks is vital. Multi-factor authentication should be enforced to ensure that only authorized personnel can access critical systems. Biometric authentication, smartcards, and secure tokens can add an extra layer of security, reducing the risk of unauthorized access. Proper access control mechanisms must be in place to restrict access to sensitive data and functionalities based on user roles and permissions.

Threat Detection and Prevention

6G IoT applications must employ advanced threat detection and prevention systems. Artificial intelligence and machine learning algorithms can analyze network traffic patterns and device behavior to identify anomalies that may indicate potential security breaches. In case of suspicious activity, automated responses should be triggered to isolate compromised devices or systems, limiting the extent of any potential damage.

Firmware and Software Updates

Regular updates to IoT device firmware and software are crucial for security. Manufacturers should provide timely patches to address vulnerabilities and security issues. Automated update mechanisms can ensure that devices remain up to date with the latest security enhancements, protecting against known threats.

Ethical Considerations

6G IoT applications for emergency and vigilance must also adhere to ethical standards. Data collected should be used solely for its intended purpose and not for any form of unauthorized surveillance or data exploitation. Transparent data policies and compliance with privacy regulations are essential to build trust among users.

To summarize, 6G IoT applications for emergency and vigilance hold the promise of significantly improving our ability to respond to crises and enhance vigilance efforts. However, the security of these applications must be a top priority. By implementing robust data privacy measures, authentication and access control mechanisms, advanced threat detection systems, timely updates, and ethical considerations, we can ensure that 6G IoT applications for emergency and vigilance are not only innovative but also safe and secure, protecting individuals and society as a whole.

2.2

IoT, and Industry 4.0 in the Cloud Era

In the ever-evolving realm of technology, the landscape is transforming at an unprecedented pace.

The advent of 6G, Industrial IoT and Industry 4.0 has ushered in a new era of connectivity, redefining the way we perceive and interact with the digital world. This article post explores the convergence of these cutting-edge technologies, highlighting the pivotal role of cloud computing, the significance of hardware encryption, and the impact on energy and utilities business vertical.

The 6G Revolution

As we bid farewell to the era of 5G, the anticipation surrounding 6G is palpable. Promising faster speeds, lower latency, and unprecedented connectivity, 6G is set to revolutionize the way we communicate and access information. Its potential applications extend beyond smartphones to include the realms of augmented reality, virtual reality, and the Industrial IoT. One significant benefit generated by 6G mixture with iIoT, cloud and hardware encryption will be the capability to run operations on sensors raw data, previously executed into device by edge computing, this time into a cloud software platform, dicreasing the effort of computing of devices and still preserving the data security. This could be the future of energy consunption and production forecasts, realized without a massive computing infrastructure changes.

Industrial IoT and Industry 4.0: A Symbiotic Relationship

The Industrial Internet of Things (IIoT) is the backbone of Industry 4.0, creating a seamless ecosystem where machines, devices, and humans collaborate in real-time. This interconnected web of sensors and actuators facilitates data-driven decision-making, predictive maintenance, and enhanced efficiency and a better infrastructure / industrial physical security. Industry 4.0, on the other hand, represents the fourth industrial revolution, characterized by the integration of smart technologies into manufacturing and explotation processes. Together, IIoT and Industry 4.0 are shaping the factories and critical infrastructures of the future.

Cloud: The Catalyst of Connectivity

Central to the success of these transformative technologies is the omnipresent cloud. Cloud computing acts as the backbone, providing the necessary infrastructure for data storage, processing, and analysis. It enables seamless collaboration, scalability, and accessibility, becoming an indispensable complementary element in the era of 6G, Industrial IoT, and Industry 4.0.

Fortifying Connectivity: Hardware Encryption in focus

With the increasing reliance on interconnected devices and the proliferation of sensitive data, ensuring the security of information becomes paramount. Hardware encryption emerges as a key player, safeguarding data at the device level. By encrypting data at the hardware level, the risk of cyber threats is significantly reduced, ensuring the integrity and confidentiality of information exchanged within the vast network of connected devices. Last, but not least, it is critical the way how cloud software platform are capable of terninating this enxrypted path, considering there are multiple cimputing nodes involved between field sensors & actuators, and data management platform consuming the traffic from / to filed elements. A hardware encryption wihtout other security systems integrated would not be enough.

Energy and Utilities: Navigating the Digital Transformation

The digital transformation propelled by 6G, Industrial IoT, and Industry 4.0 extends its impact to the energy and utilities sector. Smart grids, predictive maintenance, improved consumption and production predictions, and real-time monitoring enhance efficiency, reduce downtime, and pave the way for sustainable practices. The integration of these technologies in the energy and utilities sector not only optimizes resource utilization (by lowering CAPEX and OPEX, and reducing dependencies by human resources), but also reduces risks and contributes to the global push for a greener and more sustainable future.

In conclusion, the confluence of 6G, Industrial IoT, and Industry 4.0 marks a paradigm shift in how we perceive and harness the power of connectivity. The cloud, hardware encryption, and the digital transformation of energy and utilities play pivotal roles in shaping this technological landscape. As we navigate this era of unprecedented connectivity, the possibilities are vast, and the potential for innovation is boundless. Welcome to the future - where the power of connectivity knows no bounds.

2.3

SECANT approach to security in the Healthcare ICT environments that include IoT and connected devices.

In recent years, the deployment of interconnected medical devices has increased dramatically; consequently, access to information has expanded, decision-making has evolved, and patient care has improved.

Along with such developments, interconnected medical devices also present new challenges since the incidence of cybercrimes in hospitals and clinics increase, as described in previous sections.

The SECANT project approaches these challenges and is working to deliver a platform for cyber security risk assessment for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures, and in particular, in the healthcare environment. Among main pillars of the SECANT platform there are: (i) Digital Security and Privacy for the underlying complex ICT infrastructure and (ii) Collaborative Threat Intelligence for collecting, sharing and reporting security incidents. Through these two pillars, SECANT tackles the very important areas of monitoring, threat and vulnerability analysis and risk assessment all of which are necessary components for constructing a resilient and proactive security posture.

The platform includes a monitoring layer, the primary goal of which is the installation of reliable security monitoring methods across the devices and monitoring agents. Real-time insight into an organisation's information technology infrastructure may be achieved by installing cutting-edge intrusion detection and network traffic analysis tools. These can all be used by healthcare organisations to achieve fast discovery of unusual activity and, consequently, rapid incident response and mitigation capabilities.

In SECANT, the monitoring agent component is oriented on discovering new vulnerabilities and collecting data related to network activity, being designed to monitor both internal and external network traffic as well as system logs to identify suspicious activity related to assets in the ICT System. Wazuh[22] is adopted as an event monitoring agent. As an XDR platform, it offers holistic security monitoring that aims at detecting and responding to security incidents by analysing and correlating events in real-time. It is designed to monitor various system events, application events, and user activities, helping organisations maintain a robust security posture and meet regulatory compliance requirements. Suricata[23] is adopted as an intrusion detection system. It is designed to analyse network traffic in real-time and detect various types of security threats. It integrates with external tools and services to extend its functionality and provide additional insights into network activity. Suricata can log network traffic and security events, providing organisations with a record of activity on their network. These logs can be used for forensic analysis and can help organisations identify potential security threats. Suricata's prevention capabilities enable organisations to block malicious traffic from reaching its destination, preventing potential security threats.

While the monitoring agents provide insight into the organization's assets and their security status, SECANT includes also the Threat Intelligence Module (TIM) which enables the SECANT platform to maintain a constantly updated database concerning the evolving threat landscape. In particular, TIM is responsible for the collection, extraction, enrichment and sharing of CTI. TIM gathers cybersecurity data from different external and internal sources, analyses the content and extracts Indicators of Compromise (IoCs) and Indicators of Attack (IoAs) which compose the CTI. The collected data are filtered to avoid storing personal information leveraging rule-based techniques and analysed to extract CTI utilising using rule-based and machine learning based techniques. Subsequently, the collected data is further analysed in order to identify possible correlations between the information collected both from external as well as internal sources (e.g., correlation between CPEs and CVEs). TIM utilises both simple (e.g., MISP correlation) and advanced (e.g., ML-based) correlations of threats. The collection process is achieved both (i) manually through a user-friendly GUI as well as (ii) automatically.

[22] https://wazuh.com

[23] https://suricata.io

[24] https://github.com/telekom-security/tpotce

External sources of TIM include sources such as vulnerability databases, CERT feeds, databases with Proof of Concept (PoC) exploits, social media, forums, and relevant web pages from the Surface Web (e.g., websites relevant to cybersecurity) and the Dark Web (e.g., darknet market). The sources can be specifically selected to include information concerning cyber-threat and vulnerabilities affection 6G IoT devices. With regard to internal sources, TIM utilises different honeypot instances which are deployed and managed using a T-Pot[24] instance. Nevertheless, TIM architecture, allows the utilisation of any type of honeypots or actual devices (e.g., 5G and 6G IoT devices) to gather information and extract CTI. Furthermore, TIM allows the gathering and analysis of data from all type of devices, including 5G and 6G IoT devices. Similarly, the generated CTI can be consumed from all type of devices. Consequently, TIM is considered agnostic concerning the assets, protocols and standards that are used within an infrastructure.

In addition to the monitoring agents and TIM, another valuable tool employed within the SECANT framework for device monitoring and threat detection is BAE (Behaviour Analysis Engine). BAE specialises in analysing entity behaviours specific to IoT healthcare devices to identify anomalies and potential security threats. It leverages machine learning algorithms and advanced analytics to detect deviations from normal patterns of behaviour, enabling organizations to pinpoint suspicious activities early in their lifecycle, before the threat has had an impact on the network. This proactive approach is essential in mitigating cybersecurity risks and ensuring the integrity of IoT healthcare systems. It seamlessly integrates with the existing monitoring agent infrastructure, providing a comprehensive view of network activity, making it easier to detect and respond to security incidents effectively.

Another critical component of the security architecture is the analysis layer including the risk assessment. This ensures that healthcare organisations have an accurate understanding of the specific threats in their environment as well as the vulnerabilities they face. Organisations are in a better position to identify and prioritise possible security risks, determine the potential effect of those risks, and put in place the relevant controls and protections. The methodology places a strong emphasis on conducting continuous risk assessments and vulnerability scans, in order to proactively discover and resolve any vulnerabilities, before they can be exploited by malicious actors.

SECANT includes a Cyber Risk Assessment (CO-CRAE) module for this risk assessment task. The CO-CRAE provides Security Administrators with valuable insights regarding the security level and operational assurance of an IT environment. It enables the evaluation of networks, the evaluation and quantification of risk levels, and the analysis of the impact of exploiting vulnerabilities successfully. The CO-CRAE is in charge of identifying and quantifying hazards, as well as calculating risks. The engine prioritizes complex medical environments with diverse hardware and software assets, taking into account both internal and external threat actors. The risk assessment methodology takes physical and geospatial dependencies into account and is based on innovative interdependency graphs and an extensible model. The objective is to conduct a dynamic, continuous, and near-real-time cyber-physical security risk assessment, taking into account the potential cascading effects of security incidents.

Finally, to foster a culture of cybersecurity vigilance among healthcare workforces, the platform emphasises a robust training component. By providing healthcare personnel with the necessary knowledge and skills to identify and address security issues, organisations can significantly reduce the risk of data breaches and other cybersecurity incidents. The SECANT platform facilitates ongoing skill development for regular users, empowering them to act as a frontline defence against imminent attacks targeted at healthcare stakeholders.

2.4

Personalised health IoT Devices

One of the real-life deployment use cases of ERATOSTHENES project is related to personalized health devices focused on remote patient monitoring devices and gateways.

The pilot aims to develop a personal health gateway and a service for remote patient monitoring and to apply and evaluate ERATOSTHENES technologies in terms of improving trustworthiness and security, related to enrolment and application of medical devices. ERATOSTHENES is currently performing a full-scale integration of its solution to such devices, owned by Tellu company (project partner). TELLU is an IoT application provider in the eHealth market with an Edge-based SaaS for remote patient monitoring and assistance product. The Tellu Health Gateway is the core component of the scenario, which is deployed in patient's home. Tellu Health Gateway is at the core of the service and is responsible for collecting data from various medical sensors and sending them to the back-end Cloud services. The services are related to the analysis of data and their record in the patient's electronic health journal. Abnormal situations, such as fell-down and abrupt increase of blood pressure, are notified to the healthcare team. The gateway also hosts logics for pre-processing the raw data, in order to (i) limit data exchange between the gateway and the Cloud with the aim of preserving bandwidth, (ii) increase security and privacy, and (iii) ensure continuity of services even in case of no Internet connection.

Driven by the market trends, Tellu is aiming at transforming their product from a closed remote patient monitoring service to an open platform for home assistance, with two major extensions:

1) The healthcare gateways will be able to collect data from not only the standard IoT devices distributed by Tellu, but also the patient's own devices;

2) Third-party developers will be able to provide value-added services on top of the Tellu platform, integrating and utilising the sensor data and the standard Tellu services in innovative ways. Tellu will transfer to a platform provider and build an ecosystem around their Edge platform.

Current safety/security threats relating to health IoT devices relate to:

- Compromise of data in motion: relating to tampering or sniffing of data between the transfers from possible local gateways up to the devices.
- Sabotage or misuse of Hardware deployed in patient home: tampering of the actual IoT device or gateway.
- DDoS at the could level: distributed denial of service attack localized at the cloud components of the service.
- Compromised identities: of the various roles and actors.
- GDPR breach: as Telecare and Telehealth services manage and process person sensitive information that needs to comply with GDPR.

2.5 Manufacturing Industry

The recent pace of changes and increase in demand in wireless communications towards 6G and smart device technologies via the Internet of Things (IoT) to overcome the major circumscriptions in the existing 5G networks drive a revolution in customer services and applications through fully intelligent and automated remote management systems[25] [26]. Beyond-5G and 6G mobile and communication networks are designed to connect a vast array of devices and users. This extensive connectivity opens them up to a myriad of privacy and security concerns, potentially compromising the stability and trustworthiness of these networks.[27]

Integrating artificial intelligence in 6G is able to provide feasible and impactful solutions for challenging issues relevant to network efficiency improvement which has been a major target for most security and privacy vulnerabilities. In such circumstances need to take extra precautions particularly for physical, network, and application layers to tackle diverse security threats[28]. As Traditional security solutions are no longer fit for 6G, a combination of their revision along with the new security approaches such as novel authentication, encryption, access control, communication, distributed ledger technology (DLT), and malicious activity detection is a key requirement to foster security and trustworthiness[29] [30].

The key 6G technologies in the Industrial Internet of Things (IIoT) domain include: Intelligent Robots (artificial intelligence (AI), machine learning (ML)), distributed ledger (DL) technologies such as Blockchain-based production, and Human-Machine Communication (Industry 5.0)[31]. Moreover, for next-generation networks, Intrusion Detection Methods designed with Federated Learning (FL) are being developed to detect various attack vectors (e.g., DDoS attacks) within 5G core networks[32]. The FL models leverage collaborative learning techniques to improve upon the efficacy of conventional centralized ML models. This innovation permits a multitude of devices, potentially situated in data or network silos, to collaboratively learn a model without necessitating the sharing of data. This not only enhances security and privacy for devices on a large scale but also provides a safeguard against potential breaches, ensuring the integrity and confidentiality of information across the network.

Recently, with the successful deployment of stable cloud-based Large Language Models (LLMs), research focus has pivoted towards their application on network application and cybersecurity. The convergence of Large Language Models, edge networks, and multi-agent systems is paving the way for advanced, self-governed wireless networks with intelligent decision-making capabilities at the edge. The implementation of multi-agent generative AI within wireless networks reveals promising potentials, particularly in intent-based networking[33]. Large Language Models have been successfully implemented for various traditional cybersecurity operations, including cyber threat hunting and ML-based anomaly detection . Furthermore, chaining LLMs have been effectively utilized to fully automate detection and response operations, demonstrating their pivotal role in advancing cybersecurity measures . These innovative approaches underscore the impact of LLMs in delivering interpretable, explainable, and actionable AI, bringing it significantly closer to the users.

[25] Abdel Hakeem SA, Hussein HH, Kim H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors (Basel). 2022 Mar 2;22(5):1969. doi: 10.3390/s22051969. PMID: 35271113; PMCID: PMC8914636.

[26] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[27] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[28] Sheikhi, S. and Kostakos, P., 2023, June. DDoS attack detection using unsupervised federated learning for 5G networks and beyond. In 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (pp. 442-447). IEEE.

[29] Zou, H., Zhao, Q., Bariah, L., Bennis, M. and Debbah, M., 2023. Wireless Multi-Agent Generative AI: From Connected Intelligence to Collective Intelligence. arXiv preprint arXiv:2307.02757.

[30] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[31] Sheikhi, S. and Kostakos, P., 2023, June. DDoS attack detection using unsupervised federated learning for 5G networks and beyond. In 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) (pp. 442-447). IEEE.

[32] Zou, H., Zhao, Q., Bariah, L., Bennis, M. and Debbah, M., 2023. Wireless Multi-Agent Generative AI: From Connected Intelligence to Collective Intelligence. arXiv preprint arXiv:2307.02757.

[34] Tarek Ali and Panos Kostakos, 2023. HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). arXiv preprint https://arxiv.org/pdf/2309.16021.pdf

[35] Mehrdad Kaheh, Danial Khosh Kholgh and Panos Kostakos, 2023. Cyber Sentinel: Exploring Conversational Agents in Streamlining Security Tasks with GPT-4. arXiv preprint https://arxiv.org/pdf/2309.16422.pdf

2.6

Automotive

The second pilot that ERATOSTHENEs implements, relates to connected vehicles and related infrastructure.

The number of connected devices in the automotive industry has grown over the years, and this increase comes along with the evolution of the HW and SW that is integrated into vehicles and infrastructures. Over the last years, the electronic architecture of vehicles has been continuously developed to adapt to the new requirements of the users. Modern vehicles can interact with other connected devices to retrieve information about other vehicles or infrastructures (e.g., vehicles, smart traffic lights, smart speed signs, etc.) to make driving more comfortable and advise for the best possible decision while supporting smart-city and smart-connectivity trends.

These short-range interactions with other vehicles or infrastructure are not the only benefits those modern vehicles can provide to the users. Also, software updates can be executed remotely, eliminating the need to bring the vehicle to the manufacturer facilities, allowing the improvement of the software installed in the ECUs integrated in the vehicles.

However, this progress is also accompanied by concerns of the automotive industry about possible cyber threats and the safety reduction of pedestrians or drivers. This connection can be exploited by cyber criminals to carry out attacks remotely, modifying the vehicle behaviour or hindering its function. The newest 155 and 156 UN regulations are proof of this worry, standardizing cybersecurity and a software update process that the manufacturers must follow on their products.

For this pilot, ERATOSTHENES includes two use cases where a vehicle will be the victim of cyber-attacks. The scenario includes interaction of the vehicle with the infrastructure devices, and we will also describe the challenges for the trust on V2V and V2I communication during the software update.

Current safety/security threats relating to Connected Vehicles relate to:

- A DoS or a DDoS attack can be performed to hinder services or devices functions.
- Intercepting the messages between different devices, perform a man-in-the-middle attack (for example, during the software update process) or sniff the communications to extract meaningful information.
- Devices identity relating to a device which has no access to the different onboard/infrastructure services could try to pretend to be another device being able to gain privileges or tampering possible communications performing a spoofing attack.
- Physical attacks could be performed, compromising the device physically or, for example, injecting code if the hardware permits physical manipulation.
- GDPR breach could occur during a software update.

2.7

INDUSTRY 4.0: Disposable IDs in Industry 4.0 Use case

Industry 4.0 is powered by the Internet of Things technology.

There are more and more IoT devices installed on the industry floor for various processes. Smart connected devices are the driving force for automation and optimization in industries. They reduce cost, increase efficiency, provide predictive maintenance, and lower downtime. These devices consist of microcontroller, memory, general purpose input output (GPIO) pins, communication module (for WiFi, Bluetooth, Serial, SPIetc.).

A big advantage of such devices is their small form factor. They can be easily embedded or retrofitted in existing machines on the industry floor. In the pilot, we focus on securing retrofitting data sourcing applications. It can be performed by adding complete external sensor / gateway networks into the existing shopfloor or by extending machines with gateways to gather data from PLCs or Electronic Control Units (ECUs) and forward them to data services. Data services can be represented by on premise or cloud services / DB. Data analytics and data processing will be done on the data service available.

It is paramount to identify each device uniquely in an industrial network. Because it is dynamic and heterogeneous in nature. The pilot will strengthen the security of connected devices, data transfer services and analytics applications. The core of the pilot will be generating secure disposal IDs for the IoT devices. The ID generation mechanism will be based on Physical Unclonable Functions (PUF) and Distributed ledger technology (DLT). An ID will serve as a fingerprint for a connected device.

ERATOSTHENES

Current safety/security threats relating Industry 4.0 relate to:

- Physical attacks: A device can be compromised if a malicious actor has physical access. It can be manipulated and can be used to gain access to another assets. Data stored on a device can also be stolen in such event.
- Cyber threats: Number of cyberattacks on smart connected devices have increased multifold in the last couple of years with the proliferation of IoT.
- Supply chain attacks: An over the air update solution automatically download and install security patches on IoT devices. A malicious piece of software can be integrated with a security patch.
- DDoS Attack: A distributed denial of service (DDoS) attack can render any service dead. An attacker can flood trust and permission managing service with requests.
- Man in the Middle: The connected assets will communicate through wireless, radio, or internet protocols. An attacker could intercept the communications.
- Compromised Disposal ID: A valid disposal ID is compromised.
- GDPR breach on the service.

2.8

METAVERSE

The metaverse is emerging as a key 6G-based application for the next generation of networking and socialisation.

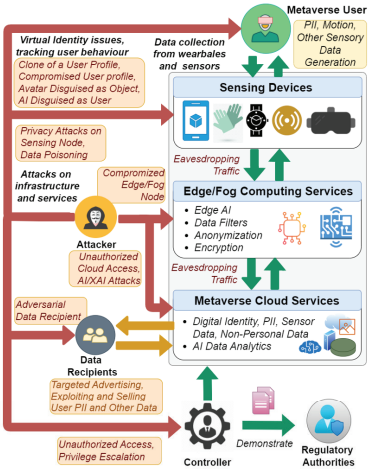


FIGURE 1: Metaverse related vision 6G architecture and potential threats[41] 3. 6G-IOT Security Enables

It already has significant industry attention indicating its potential mainstream adoption. A notable example of this shift is the rebranding of Facebook to Meta, highlighting the company's substantial investment in realising the metaverse[38]. The COVID-19 pandemic has also accelerated the transition from physical to virtual workplaces, with nearly 50% of Europeans now preferring at least partial Work from Home (WFH) arrangements[39], up from 12% before the pandemic. The advent of 6G communication will further enhance the development of the metaverse. With capabilities such as ultra-high peak data rates in the terabit range, extremely low latency communication under one millisecond, enhanced mobility through information exchange across all mediums, and exceptionally high reliability beyond 99.99999%, 6G will be a crucial enabler for the metaverse[40]. It is also expected to create a self-sustaining virtual ecosystem offering fully immersive, real-time experiences and numerous opportunities for users and industries to interact with the world. The large-scale success of the metaverse will be driven by the introduction of 6G networks and enabling technologies. However, the increased interaction through new technologies and numerous third-party services will also present greater possibilities for security and privacy threats.

Figure 01 shows an overview of the security and privacy threats in the metaverse-associated 6G architectures. With the abundance of access to the hardware and communication capability, threats are emerging from the layers that are closely related with the user level. For example, biometric data collected from Virtual Reality (VR) headsets and wearables can create a high risk of privacy exposure if captured by a third party, since they are permanent for a user. Furthermore, there could be numerous flaws in the metaverse's hardware, software, and network. Moreover, a malicious edge computing device deployed or compromised by the attacker may intercept or steal private information, including biometric, motion, and health data. Metaverse may use a variety of Machine Learning (ML) and AI models to determine user actions and intentions from sensor data. An AI model has created a privacy risk if they expose sensitive information about individuals. Inference attack is another significant privacy concern in the metaverse, where an adversary is attempting to infer certain information, such as the membership or properties of a target. Metaverse can consist of many associated ML models running and shared among services such as object detection, facial recognition, and motion sensing in wearable devices. If an attacker gains access to these ML models but not directly to data, they can still infer some properties on the data where the ML models are trained on.

As solutions, several approaches can be undertaken to protect the security and privacy of metaverse. A key step is to ensure the privacy protection of Personally Identifiable Information (PII). For this, techniques like homomorphic encryption, or Differential Privacy (DP) can be used[42]. For example, multiple avatars can be used for a user with different identities and noise can be added in the behaviour and personal details of the avatars, when shared with third parties. Independent authorities should assess the capacity of metaverse-based services. Furthermore, even without any prior requirements from consumers, well-designed services should protect privacy needs by default, by taking steps to secure itself before a data breach occurs.

[38] Kim, J., 2021. Advertising in the metaverse: Research agenda. Journal of Interactive Advertising, 21(3), pp.141-144.

[39] Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S. and Toscano, F., 2021. Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress. Journal of occupational and environmental medicine, 63(7), pp.e426-e432.

[40] Liu, G., Huang, Y., Li, N., Dong, J., Jin, J., Wang, Q. and Li, N., 2020. Vision, requirements and network architecture of 6G mobile network beyond 2030. China Communications, 17(9), pp.92-104.

[41] Sandeepa, C., Wang, S. and Liyanage, M., 2023, June. Privacy of the Metaverse: Current Issues, AI Attacks, and Possible Solutions. In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom) (pp. 234-241). IEEE.

[42] Sandeepa, C., Siniarski, B., Kourtellis, N., Wang, S. and Liyanage, M., 2022. A survey on privacy for B5G/6G: New privacy challenges, and research directions. Journal of Industrial Information Integration, 30, p.100405.

6G-IOT Security Enablers Applications deployments

03

3.1

AI-empowered security

The rise in encrypted network traffic, driven by the use of HTTPS and Virtual Private Networks (VPN), poses challenges for traditional traffic analysis tools, as they struggle to detect malicious activity.

This, coupled with the sheer volume of traffic from mobile and IoT devices, requires advanced Artificial Intelligence (AI)-based techniques for real-time anomaly detection. We developed three AI-based security applications that correspond to three main steps of Intrusion Detection and Response. Firstly, the Traffic Classification application characterizes network traffic to identify certain types of normal user activities, such as web browsing, chatting, or video streaming. Secondly, the Attack Detection application differentiates between malicious traffic and legitimate traffic to detect popular cyberattacks in 5G or IoT environments. Finally, the Root Cause Analysis application employs a similarity-based machine learning approach to discover the root causes of problems in order to quickly identify appropriate solutions.

- While AI holds promise for security management in 5G and IoT networks, challenges such as limited real datasets, lack of explainability, and vulnerability to adversarial attacks need to be addressed. eXplainable Artificial Intelligence (XAI) has emerged, aiming to provide users with a rationale for understanding AI system outputs and fostering trust. However, existing explainable frameworks still lack comprehensive support for adversarial attacks and defenses. Therefore, in addition to accuracy and performance, new requirements concerning trustworthiness, transparency, and robustness also need to be considered.
- Within the scope of the SPATIAL project, montimage designed and implemented the Montimage AI Platform (MAIP), an XAI framework with an intuitive and user-friendly interface for network traffic analysis and classification in 5G/IoT networks. It comprises two principal components: Network Traffic Analysis and XAI for Resiliency. Firstly, the Network Traffic Analysis component aims to fulfill the need for effective analysis and classification of encrypted traffic using advanced AI techniques. It gathers raw traffic data from networks or 5G/IoT testbeds and constructs AI models to classify vectorized network traffic data for diverse objectives, such as classifying user activity or detecting anomalies in encrypted traffic. Secondly, the XAI for Resiliency component aims to enhance the robustness of AI models built within the Network Traffic Analysis module, making them more resilient against different types of adversarial machine learning attacks. This component injects evasion and poisoning adversarial attacks, such as label flipping attacks and Generative Adversarial Networks (GANs) based attacks, or integrates existing AI-based attack libraries for robustness analysis of AI models. It employs popular model-agnostic post-hoc XAI techniques, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations), to produce post-hoc global and local explanations of model predictions. Furthermore, this component analyzes the robustness of models against adversarial attacks via quantifiable resilience metrics and provides an XAI-based mechanism to detect the existence of adversarial attacks on AI-based systems.

3.2

Enabling Secure and Scalable Identity Management for the Internet of Things (IoT) with SSI in 6G Networks

ARCADIAN-IoT

Mobile technology has facilitated the proliferation of connected devices, the so-called Internet of Things (IoT) across many sectors from smart cities, to telehealth, industry and beyond.

The prevalent identity management for IoT Devices today include centralized identity management, X.509 certificates, shared secret and also simple userId & password solutions[43]. These identity management solutions suffer from known security vulnerabilities, privacy concerns and scalability issues.

The mobile industry is now working on the sixth generation of cellular network technology 6G[44] which is being touted to revolutionize the way we connect and interact over virtual reality, sensory and telehealth IoT Devices, voice-controlled AI assistants, Autonomous Vehicles etc.

6G´s primary goal is to provide this necessary bandwidth and low latency technology for real-time data exchange to facilitate this new era.

However, as traditional centralized identity and certificate-based management systems have known limitations and are not the best fit to handle the exponential growth of IoT devices and their greater penetration into our personal lives, that require ever more scalable, secure and privacy preserving identity solutions. Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) have emerged as promising technologies, building on the principles of Zero Trust[45] (never trust, always verify, least privilege, etc., to address these challenges.

This paper explores in more detail these technologies so to facilitate 6G use cases with State-of-the-Art secure and scalable decentralized and distributed identity management for IoT devices, systems and the end users that rely on them.

SSI is a decentralized approach to identity management that gives individuals and organizations control over their own identities. In an SSI system, individuals own and manage their own identities in mobile or web wallets, which store Verifiable Credentials issued by trusted parties to attest such things as national eID, drivers license, employee ID etc. just like a real wallet holds such physical ID cards. Cryptographic technology is used to sign the Verifiable Credentials so to prove that they were issued by a trusted organization or presented by a specific end user´s wallet. This cryptographic information is associated with Decentralized Identifiers (DIDs) managed by end user´s and organizations themselves rather than Certificate Authorities in the case of X.509 certificates.

In the case of EBSI (European Blockchain Services Infrastructure[46]), Issuers DIDs are published on a decentralized blockchain, where the EBSI ledger contains the cryptographic material associated to the Issuer´s DID that is used by verifiers to check it is an authentic credential. This ensures trust is ensured by one well known trusted organization in a decentralized and highly scalable approach provided by the distributed ledger technology. This is illustrated in the following EBSI Issuer Trust Model[47] figure.

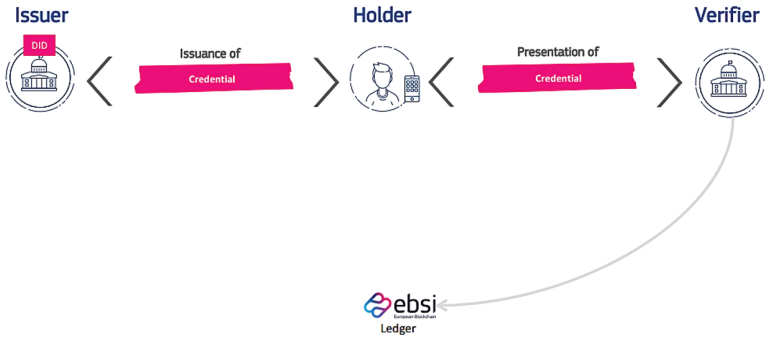


FIGURE 2: EBSI Issuer Trust Model

To prove their identity to others, individuals can create verifiable credentials (VCs) that are issued by trusted parties. VCs are cryptographically secure documents that contain information about an individual's identity, such as their name, date of birth, and education. When an individual presents a VC to a verifier, the verifier can verify the VC's authenticity and the information it contains.

In ARCADIAN-IoT project[48] various DIDs were used depending on the scenario, e.g. DID:PEER[49] privacy preserving DID for mobile wallets, DID:WEB[50] for Issuers and constrained devices and DID:PRIV[51] for IoT Devices. These were deployed and proven with SSI authentication for various domain pilots such as Drones (M2M use cases) and their users, Patients and Medical Professionals (P2M use cases).

In the case of IoT Devices that have sufficient resources to support cryptographic operations, an SSI Agent is able to be deployed on the device and integrated with the business logic to support ZTP making use of the device fingerprint to be issued as a Verifiable Credential by a trusted security framework, which is later used for authentication purposes. The figure below demonstrates the use of SSI in this approach used in the ARCADIAN-IoT project.

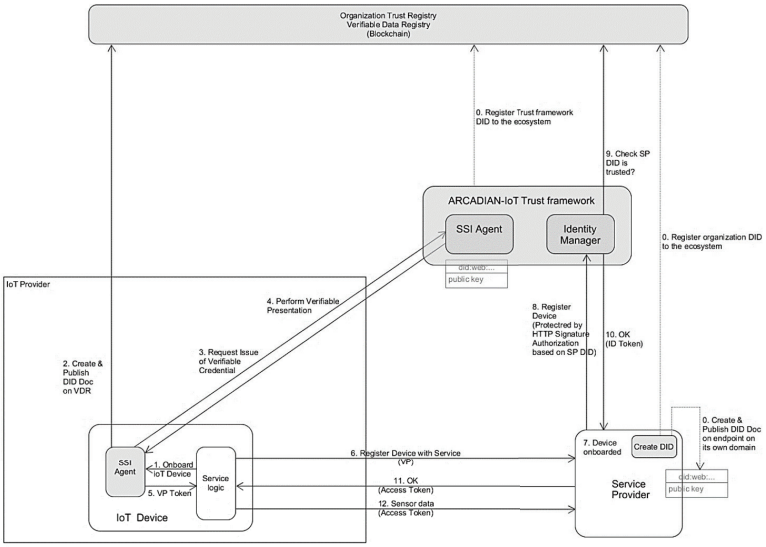


FIGURE 3: ARCADIAN-IoT IoT Device SSI Registration

This approach followed a secure ZTP approach with the device generating its own DID on a permissioned blockchain, which only members of ecosystem can access, and identity claims based on its device fingerprint, were issued to the IoT Devices as a Verifiable Credential.

However, constrained IoT devices in ARCADIAN-IoT do not contain enough processing power to perform the necessary cryptography signing operations. Therefore, the solution devised was for an IoT GW platform to handle the DID authentication on behalf of the constrained IoT Devices with DID challenge / response towards the ARCADIAN-IoT trusted framework for authorising token-based access to Service Provider systems. The IoT Device used a shared secret for authentication with the IoT GW. This approach taken in ARCADIAN-IoT for constrained IoT Devices is shown below in the following figure.

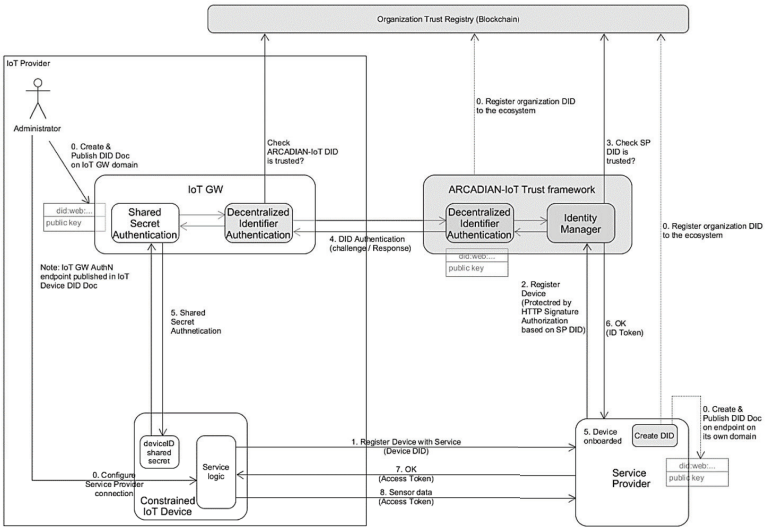


FIGURE 4: ARCADIAN-IoT Constrained IoT Device SSI Registration

From the above figure, we can see that the IoT Device itself does not support an SSI agent and this is because it lacks sufficient resources to support the public private key cryptographic signing of Verifiable Credentials. Considering the aims of 6G, include to support increased bandwidth and for ever more constrained IoT Devices it would be advantageous that SSI agents make use of the cryptographic capabilities of eSIM deployed with IoT Devices.

Therefore, it is concluded that a key area for further exploration in the convergence of 6G with SSI and Decentralized Identifiers is to provide guidelines on the cryptographic signing algorithms implementation on eSIM's for handling the signing of verifiable presentation for IoT Devices and to align with EBSI guidelines to achieve greater interoperability. This will bring an extra level of public private crypto security, zero touch provisioning and lifecycle management capabilities that is not currently available for constrained devices.

Considering the P2M interoperability achieved by EBSI in Europe on establishing integration guidelines[52] and certification of compliant mobile wallets[53], then this is an important area that is needed to promote the M2M interoperability and 6G standardisations should consider collaboration with EBSI to ensure wider SSI interoperability amongst IoT Device vendors.

[43] Landscape of IoT security
Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller

[44] https://www.etsi.org/newsroom/news/2307-3gpp-commits-to-develop-6g-specifications#:~:text=3GPP%20has%20developed%20international%20standards,of%206G%20global%20harmonized%20standards.%22&text=%22Success%20is%20something%20that%20we%20must%20work%20to%20maintain.

[45] https://trustoverip.org/blog/2022/02/22/no-i-dont-trust-you-implementing-zero-trust-architecture-in-the-world-of-self-sovereign-identity-ssi/

[46] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[47] https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/597952490/Chapter%205%20-%20Issuer%20Trust%20Model%20.pdf?version=1&modificationDate=1666602514393&api=v2#:~:text=Trusted%20Issuer%20(TI)%20is%20responsible,it%20manages%20a%20DID%20document.

[48] https://www.arcadian-iot.eu/

[49] GitHub - decentralized-identity/peer-did-method-spec: A rich DID method that has no blockchain dependencies. The verifiable data registry is a synchronization protocol between peers.

[50] https://w3c-ccg.github.io/did-method-web/

[51] Private DID method implemented on Hyperledger Fabric Permissioned Blockchain in ARCADIAN-IoT Project

[52] https://hub.ebsi.eu/vc-framework

[53] https://hub.ebsi.eu/wallet-conformance

3.3 Distributed Ledger Technology (DLT)

The objective of 6G technology is to deliver enhanced transmission rates, improved reliability, increased bandwidth, extremely low latency, efficient resource and energy usage, and effective security for a broader spectrum of devices and services.

Within the domain of 6G Internet of Things (IoT), Distributed Ledger Technology (DLT) plays a pivotal and multifaceted role in shaping the interaction and auditable information exchange between interconnected devices. According to 5GGP[54], "The blockchain-based platform is one of the most prominent technologies to unleash the potential of 6G system." DLT offers a distributed and highly secure framework that aligns seamlessly with the exacting requirements of 6G IoT. One of its fundamental advantages is the assurance of data immutability and transparency. Every piece of information exchanged between IoT devices is recorded on the ledger in a manner that cannot be altered or tampered with, guaranteeing the integrity of data flows. This property not only enhances security but also eliminates the need for reliance on third-party authorities to validate and oversee transactions[55].

However, DLT's impact goes beyond security. Its distributed nature allows for improved resource utilization and management, which is particularly vital in the context of massive IoT environments[56]. By decentralizing control and decision-making, DLT can optimize the allocation of resources, leading to more efficient and sustainable operations. This aspect of DLT's utility aligns perfectly with the demands of 6G IoT, where an enormous number of devices, often with varying resource requirements, need to coexist and operate seamlessly.

In the case of the SECANT project, it includes the Trust and Accountability Module (TAM), that integrates a DLT for safely storing and exchanging sensitive healthcare information. The DLT functions as an immutable repository, reinforced with cryptographic primitives, for storing sensitive data, including healthcare-related and other security-sensitive data. This combination of cryptography and immutability enables healthcare organizations to enhance data integrity, auditability, and transparency. In turn, this promotes interoperability among healthcare entities, extending its reach to cybersecurity and government agencies in an effort to defend medical organizations from cyberattacks.

To ensure security and privacy in blockchain environments, it is essential to differentiate between public and private ledgers and use advanced cryptographic primitives. A hybrid DLT architecture that incorporates private and public channels (states) is central to this innovation. Through the use of cryptographic access controls, only authorized parties can gain access to and interact with particular data segments. This configuration ensures both the data's integrity and the creation of an audit trail that records all transactions and access attempts.

Towards the direction of authentication and access control, the privacy toolkit, built under the TAM, brings the novel Attribute-Based Encryption (ABE) and Attribute Based Acces Control (ABAC) schemes. In particular, the ABE schemes in SECANT allow for fine-grained access control over CTI information exchanged between hospitals and other relevant stakeholders. ABE schemes encrypt CTI data with access policies or attributes. Users can be assigned attributes based on their roles, responsibilities, and clearances. This means that only users with specific attributes can decrypt and access particular pieces of CTI data, ensuring that sensitive information is only available to authorized personnel. Besides, ABE schemes facilitate secure sharing of CTI information among authorized users. When a piece of CTI data is encrypted using ABE, it can be securely shared with others who have the necessary attributes. This makes collaboration on threat analysis and incident response more efficient without compromising data security.

[53] 5GPPP Architecture Working Group, "The 6G Architecture Landscape European perspective", December 2022 [Available] https://5g-ppp.eu/wp-content/uploads/2022/12/6G-Arch-Whitepaper_v1.0-final.pdf

[54] Pajooh, H. H., Demidenko, S., Aslam, S., & Harris, M. (2022). Blockchain and 6G-Enabled IoT. Inventions, 7(4), 109.

[55] Xu, H., Klaine, P. V., Onireti, O., Cao, B., Imran, M., & Zhang, L. (2020). Blockchain-enabled resource management and sharing for 6G communications. Digital Communications and Networks, 6(3), 261-269.

In addition to innovative Attribute-Based Encryption (ABE) schemes, SECANT introduces a robust proxy encryption scheme to enhance healthcare data protection. This scheme ensures secure server-to-server communication and data sharing within the healthcare ecosystem. The primary goal is clear: safeguard privacy, data integrity, and accountability in healthcare data exchange. The proxy encryption scheme acts as a vigilant guardian, establishing secure channels, mitigating unauthorized access risks, and upholding data security standards. The data privacy commitment extends beyond encryption, promoting trust and transparency in healthcare transactions. Accountability is ensured based on roles and clearance levels. The two-tiered security approach, combining ABE schemes and the proxy encryption scheme, creates an unbreachable shield around healthcare data, preserving trust and well-being throughout its journey in the healthcare supply chain.

3.4

Adoption of SSI and decentralized identity management

In decentralized infrastructures utilizing DLT technologies, the administration of identities becomes a complex undertaking, further compounded by the inclusion of privacy prerequisites.

Currently, there is a growing trend known as Self Sovereign Identity (SSI), which has the ability to meet access control requirements in 6G ecosystems. It achieves this by ensuring trust in both digital identity and personal data throughout data exchanges. SSI enables the identity owner to retain full control (I.e., sovereignty) over their identity, without any central authority overseeing the credential. Individual identity owners are accountable for overseeing their unique IDs and credentials, while the blockchain associates the public keys of each entity with the respective identifiers. SSI can be utilized not only for the identification of users, but also for the identification assets and services.

A roadmap for the adoption of SSI within the 6G ecosystem becomes a critical approach. This journey begins with standardization efforts, collaborating with international standards bodies and consortiums to ensure that SSI solutions are interoperable across the diverse landscape of 6G networks. Telecom service providers and network service consumers, become key actors. Integration of SSI principles into their network architectures becomes paramount, ensuring that SSI-based authentication and authorization mechanisms are fundamental components of the network's fabric.

Moreover, the extension of SSI must encompass the Internet of Things (IoT) devices proliferating within 6G networks. Ensuring these devices possess secure, verifiable identities contributes to the overall security and trustworthiness of the IoT ecosystem. Simultaneously, raising awareness among end-users about the advantages of SSI in terms of data control and privacy is crucial. Encouraging individuals to embrace SSI-based identity solutions for accessing the services is central to this effort. Engaging with administration bodies and regulators to establish a supportive legal and regulatory framework for SSI is equally imperative. There are references of broad collaboration within the EU, like the case of the EBSI (European Blockchain Services Infrastructure), which aims for standardization and accessible framework to enable those technical implementations. Recognizing SSI-based identities as legally valid and aligning data protection and privacy regulations with SSI principles is a cornerstone of this initiative.

In parallel, nurturing developer communities and developing pilot experiences that focus on SSI within the 6G ecosystem empowers innovation and application development. Cross-industry collaboration, spanning sectors like healthcare, finance, and government, paves the way for diverse SSI use cases, demonstrating the versatility and value of decentralized identity.

Pilot projects and testbeds play a pivotal role in validating the effectiveness of SSI within 6G networks, providing tangible proof of concept and illustrating the benefits to stakeholders. To ensure user-centricity, prioritizing intuitive, user-friendly interfaces and control mechanisms in SSI implementations empowers individuals to seamlessly manage their digital identities. In essence, by taking these multifaceted steps and fostering a collaborative ecosystem, the adoption of self-sovereign identity within the 6G environment unfolds as a decentralized and secure solution, ultimately enhancing user privacy, security, and trust in the next generation of communication networks.

3.5

XAI for Security and Privacy

XAI plays a crucial role in enhancing security and privacy in advanced network technologies like B5G by providing transparency and interpretability to complex AI/ML models.

By deobfuscating the black-box nature of ML methods, XAI enables the identification of responsible parties and attributes in case of security breaches or malfunctions, thus improving accountability. Traditional security measures such as encryption and access lists may not offer the same level of insight into the inner workings of AI systems as XAI does. Encryption techniques like data obfuscation and cryptography are essential for privacy preservation in networking, but when combined with XAI, they can create a more robust security framework for B5G applications. This synergy between XAI and encryption methods not only enhances the resilience of B5G telecommunications but also addresses the evolving security challenges introduced by AI-driven technologies

Interpretability Techniques: Interpretability methods in XAI aim to make AI/ML models more understandable to stakeholders. Techniques such as feature importance analysis, SHAP (SHapley Additive exPlanations), LIME (Local Interpretable Model-agnostic Explanations), and decision tree visualization can help users comprehend how a model arrives at its decisions. By providing insights into the model's inner workings, interpretability techniques enhance transparency and trust in AI systems. By using methods such as counterfactual explanations, attention mechanisms, and rule-based explanations, stakeholders can gain insights into why a model made a specific decision. Explainable models not only enhance transparency but also enable users to identify and rectify biases or errors in the system, thereby improving security and fairness.

However they can be coupled with privacy techniques as anonymization and differential privacy to even further enhance their effectiveness. Some of those privacy techniques are discussed below.

Anonymization and Obfuscation: Anonymization techniques involve masking or altering data to protect individuals' identities while maintaining data utility for analysis. By applying anonymization methods to sensitive information used in AI models, privacy risks can be mitigated. Similarly, obfuscation techniques involve obscuring or hiding critical information within the model to prevent unauthorized access or inference. These methods can safeguard sensitive data and prevent malicious actors from exploiting vulnerabilities in the system.

Differential Privacy: Differential privacy is a privacy-preserving technique that adds noise to the data before it is used in AI algorithms. This noise ensures that individual data points cannot be distinguished, thereby protecting the privacy of individuals in the dataset. By incorporating differential privacy mechanisms into AI models, organizations can prevent the leakage of sensitive information and maintain data confidentiality.

It is also important to note that XAI can be applied to variations of AI techniques such as Federated learning and unsupervised ML. Federated learning is a collaborative approach where multiple parties train a shared model without sharing raw data. By integrating XAI techniques into federated learning frameworks, organizations can ensure that model updates are explainable and auditable across distributed environments. This enhances the security and privacy of sensitive data while maintaining the performance of AI models in decentralized settings. Post-hoc XAI methods for unsupervised learning involve analyzing and interpreting the outcomes of unsupervised ML algorithms. Techniques such as clustering visualization, anomaly detection explanation, and latent space exploration can help uncover patterns and insights from unlabelled data. By applying post-hoc XAI to unsupervised learning tasks, organizations can enhance the security of their systems by detecting anomalies and identifying potential threats.

3.6 Privacy Techniques

In the developing landscape of 6G-enabled IoT, safeguarding privacy emerges as an increasingly complex yet essential requirement .

As the proliferation of interconnected devices continues to accelerate, the potential for privacy breaches amplifies exponentially. In response, a comprehensive array of advanced privacy techniques is indispensable to mitigate risks and fortify privacy in this hyperconnected ecosystem. One approach for this is the use of Differential Privacy (DP) . It offers a mathematical framework to inject controlled noise into data queries, by deliberately adding noise to conceal original individual data points while still enabling meaningful analysis at aggregate levels. This approach ensures that sensitive information remains confidential, even in the presence of adversaries seeking to infer private details from seemingly innocuous data.

Another approach is the use of Multi-Party Computation (MPC), which introduces a paradigm where multiple parties can collaboratively compute functions over their respective datasets without exposing the underlying inputs to each other . By distributing computation across multiple entities, MPC preserves privacy while enabling collaborative analysis and decision-making, thus fostering trust in decentralised IoT environments.

Furthermore, knowledge distillation emerges as a technique to minimise the transmission of sensitive data between IoT devices and centralised servers. By distilling knowledge from large, complex models into more compact representations, this approach reduces the amount of information exchanged without compromising the efficacy of data-driven applications. This limits the exposure to potential privacy breaches.

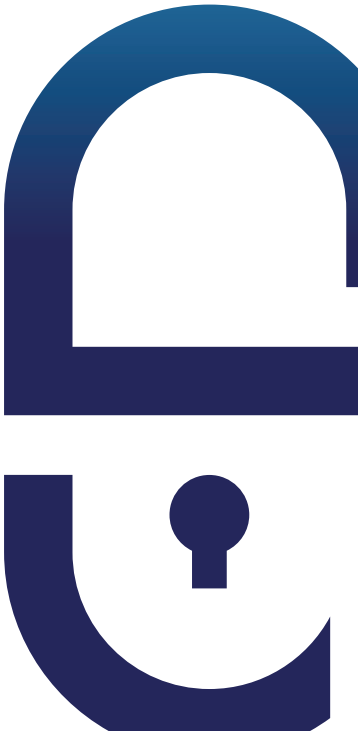
[60] Narra, K.G., Lin, Z., Wang, Y., Balasubramaniam, K. and Annavaram, M., 2019. Privacy-preserving inference in machine learning services using trusted execution environments. arXiv preprint arXiv:1912.03485.

[61] Lu, Y., Huang, X., Dai, Y., Maharjan, S. and Zhang, Y., 2019. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), pp.4177-4186.

Trusted Execution Environments (TEEs)[60] are another option for IoT that offer secure enclaves where critical computations can be executed in isolation from the underlying system, shielding them from unauthorised access and ensuring the integrity and confidentiality of sensitive operations. Leveraging hardware-based security mechanisms, TEEs provide a fortified foundation for executing privacy-sensitive tasks within the inherently vulnerable IoT landscape.

Moreover, blockchain[61] technology emerges as a distributed ledger framework that upholds transparency, immutability, and decentralisation, thereby mitigating the risks associated with centralised data repositories and intermediaries. By recording transactions in an append-only fashion across a network of nodes, blockchain ensures data integrity and accountability, maintaining enhanced trust and privacy in IoT transactions and interactions.

The aforementioned techniques constitute a robust framework for safeguarding security and privacy of data and the users in the era of 6G-enabled IoT. By integrating such techniques, stakeholders can establish resilient safeguards to protect sensitive data, foster trust among interconnected devices, and uphold the fundamental right to privacy in the digital age of 6G.



Risk Management in 6G and IoT

04

4.1

Risk Management in 6G and IoT

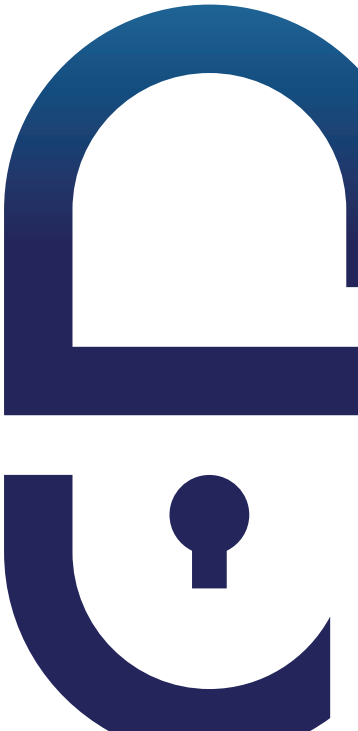
Security plays a crucial role in the rapidly changing and evolving landscape of 6G and Internet of Things (IoT) networks.

Due to the intricate nature and large size of these networks, it is crucial to prioritize continuous monitoring and evaluation of potential threats. Continuous monitoring is crucial to protect the security and integrity of data and operations in increasingly sophisticated network settings. It is in this context the CO-CRAE framework, as proposed by SECANT, comes into play.

CO-CRAE offers a comprehensive framework designed to monitor networks in real-time, identifying and evaluating potential risks as they emerge. This dynamic approach aligns perfectly with the dynamic nature of 6G and IoT networks, where new vulnerabilities and threats can surface at any moment. The ability to continuously assess risk enables network operators to remain proactive and responsive in safeguarding their systems. CO-CRAE, when effectively implemented, can provide these intricate networks with the means to stay ahead of evolving security challenges.

SECANT

An essential characteristic of the SECANT system, especially significant in the realm of 6G and IoT networks, is the computation of attack paths. These sophisticated networks frequently have several potential vulnerabilities due to their distributed and heterogeneous character. Conventional methods of evaluating risk may not be sufficient in accurately recognizing and reducing these risks. The SECANT risk assessment approach not only identifies and quantifies threats, but also uncovers the attack paths that potentially compromise the network's integrity. This kind of profound understanding is essential in protecting these complex networks from sophisticated dangers and ensuring their continual operation.



Encryption

05

5.1

Encryption Protocols in Post-Quantum 5G and Beyond Networks

The evolution of mobile networks to 5G and 6G networks brings significant advancements in speed, reliability, and capacity.

However, this progress necessitates robust encryption protocols to safeguard against the emerging threat of quantum computing. Traditional encryption methods like RSA and ECC are vulnerable to quantum attacks, prompting the development of post-quantum encryption techniques. This paper reviews various post-quantum cryptographic methods, including lattice-based, hash-based, multivariate, and code-based cryptographies, highlighting their strengths and potential vulnerabilities. Additionally, the paper explores the application of these encryption protocols in 5G networks to ensure the confidentiality, integrity, and authenticity of transmitted data. By addressing the challenges of implementing these protocols in diverse computing environments, this research aims to enhance the security of future communication infrastructures.

1. Introduction

The fifth generation of mobile networks (5G) and emerging technologies like 6G are designed to significantly enhance speed, reliability, and capacity[62] [63]. However, the increasing reliance on these networks highlights the need for robust encryption methods capable of withstanding quantum computing threats[64]. Encryption techniques are essential for maintaining the security and privacy of communication networks[65]. As technology advances, conventional encryption methods become vulnerable to quantum computer attacks, prompting the security community to actively discuss the implications of quantum computing on public-key cryptography.

To address these challenges across various computing platforms, such as cloud and IoT environments, and to accommodate different scenarios, post-quantum protocols incorporate a comprehensive set of primitives[66]. These protocols must support the computation of encrypted data using robust asymmetric key cryptography and provide security beyond traditional methods.

With the rapid expansion of network communication, there is an urgent need for enhanced security, increased bandwidth, and efficient management of emerging technologies. Robust encryption protocols are crucial in protecting extensive wireless networks from sophisticated security threats. This research aims to analyze and investigate various encryption mechanisms that can secure wireless networks and infrastructure against post-quantum security risks.

2. State of the art

The development of post-quantum encryption techniques has been driven by the increasing need for secure communication in emerging technologies such as 5G networks. Traditional encryption methods like RSA and ECC are vulnerable to being broken in polynomial time with the advent of quantum computing. Consequently, new encryption protocols that can withstand quantum attacks are essential. Recently, several post-quantum encryption mechanisms, including hash-based cryptography, multivariate-quadratic-based cryptography, and lattice-based cryptography, have been developed. Many of these techniques have been approved by international agencies like NIST (National Institute of Standards and Technology) as potential post-quantum benchmarks. This section reviews some of these encryption protocols and discusses their strengths and weaknesses.

Lattice-based cryptography:

Lattice-based algorithms were first introduced by Miklos Ajtai[67], who proposed secure cryptographic algorithms based on complex lattice problems. This method employs lattice properties to develop encryption systems. A lattice-based public-key encryption system was later designed, with Oded Regev's 2005 scheme providing a reliable and stable method[68]. This approach utilizes lattices and a generalization of the parity learning problem. A lattice is a specific arrangement of points in n-dimensional vector space, used in various fields[69].

The two main theoretical foundations for lattice-based cryptography are the challenges of the closest vector problem (CVP) and the shortest vector problem (SVP)[70]. Lattice-based cryptographic techniques are generally time-efficient and straightforward while offering security guarantees based on high complexity[71]. Notable lattice-based techniques include NTRU (Nth degree Truncated Polynomial Ring-based Univariate) encryption, based on the SVP on a lattice, and Ring-LWE (Learning

with Errors across rings), based on the Ring-Learning with Errors problem[72]. NIST has suggested NTRU and Ring-LWE as potential post-quantum benchmarks capable of resisting quantum computers.

Hash-based cryptography:

Hash-based cryptography builds encryption systems using the properties of cryptographic hash functions. This approach began with the one-time signature (OTS), where each key pair is used only once to sign a message[73]. If an OTS key pair signs two separate messages, an attacker might forge signatures and compromise personal information. One of the most well-known hash-based techniques is the XMSS (Extended Merkle Signature Scheme), built on the Merkle-Damgrd architecture[74]. Another approach is SPHINCS (Simple Hash-based Signatures), based on the Winternitz one-time signature technique[75]. NIST has proposed XMSS and SPHINCS as potential post-quantum standard candidates resistant to quantum computers.

Multivariate cryptography:

Multivariate cryptography constructs encryption systems using the properties of multivariate equations[76]. It is based on the problem of solving nonlinear equation systems over finite fields[77]. This approach is a candidate for post-quantum cryptography. One of the most well-known multivariate quadratic-based systems is Rainbow, which relies on multivariate quadratic equations[78].

Code-based cryptography:

Most current public-key cryptographic algorithms rely on the complexity of factorization or the discrete logarithm problem[79]. In contrast, code-based encryption is built on the NP-hard problem of decoding unknown error-correcting codes[80]. Two notable code-based cryptography algorithms are named after their creators, Robert McEliece[81] and Harald Niederreiter[82]. However, these algorithms have a significant disadvantage: their large key sizes compared to traditional cryptographic protocols like RSA[83]. This makes them challenging to deploy on resource-constrained devices such as embedded systems and microcontrollers.

3. Encryption protocols in 5G and beyond

A mobile communication network comprises two primary components: the radio access network (RAN) and the core network. The RAN connects individual devices to their core networks via radio communications, while the core networks support individual users[84]. A critical advancement in 5G design over LTE's EPS (evolved packet system) architecture is the extensive adoption of cloud and virtualization capabilities, offering a wide range of customizable services. Consequently, there is an urgent need to research and develop robust encryption protocols to protect 5G infrastructures and communications against quantum computing threats. The algorithms and cryptographic protocols discussed in the previous section could be instrumental in securing post-quantum network communications. In 5G networks, encryption techniques are essential for ensuring the confidentiality, integrity, and authenticity of information transmitted through the network[85]. The common use of encryption protocols for 5G network security is illustrated in Figure 5.

62 Saeid Sheikhi and Panos Kostakos. "DDoS attack detection using unsupervised federated learning for 5G networks and beyond". In: 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE. 2023, pp. 442–447.

63 Ahmed Al-Ansi et al. "Survey on intelligence edge computing in 6G: Characteristics, challenges, potential use cases, and market drivers". In: Future Internet 13.5 (2021), p. 118.5

64 Chi Cheng et al. "Securing the Internet of Things in a quantum world". In: IEEE Communications Magazine 55.2 (2017), pp. 116–120.

65 Sushil Kumar Singh et al. "Quantum communication technology for future ICT-review". In: Journal of Information Processing Systems 16.6 (2020), pp. 1459–1478.

66 Hamid Nejatollahi et al. "Post-quantum lattice-based cryptography implementations: A survey". In: ACM Computing Surveys (CSUR) 51.6 (2019), pp. 1–41.

67 Mikl os Ajtai. "Representing hard lattices with O (n log n) bits". In: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing. 2005, pp. 94–103.

68 Oded Regev. "Lattice-based cryptography". In: Annual International Cryptology Conference. Springer. 2006, pp. 131–141.

69 Hamid Nejatollahi et al. "Post-quantum lattice-based cryptography implementations: A survey". In: ACM Computing Surveys (CSUR) 51.6 (2019), pp. 1–41.

70 Masaya Yasuda. "A survey of solving SVP algorithms and recent strategies for solving the SVP challenge". In: International Symposium on Mathematics, Quantum Theory, and Cryptography. Springer, Singapore. 2021, pp. 189–207.

71 Chris Peikert et al. "A decade of lattice cryptography". In: Foundations and trends® in theoretical computer science 10.4 (2016), pp. 283–424.

72 Tobias Oder et al. "Lattice-based cryptography: From reconfigurable hardware to ASIC". In: 2016 International Symposium on Integrated Circuits (ISIC). IEEE. 2016, pp. 1–4.

73 Daniel J Bernstein et al. "SPHINCS: practical stateless hash-based signatures". In: Annual international conference on the theory and applications of cryptographic techniques. Springer. 2015, pp. 368–397.

74 Johannes Buchmann, Erik Dahmen, and Andreas H ulsing. "XMSS-a practical forward secure signature scheme based on minimal security assumptions". In: International Workshop on Post-Quantum Cryptography. Springer.2011, pp. 117–129.

75 Daniel J Bernstein et al. "SPHINCS: practical stateless hash-based signatures". In: Annual international conference on the theory and applications of cryptographic techniques. Springer. 2015, pp. 368–397.

76 Vasileios Mavroeidis et al. "The impact of quantum computing on present cryptography". In: arXiv preprint arXiv:1804.00200 (2018).

77 Jintai Ding and Albrecht Petzoldt. "Current state of multivariate cryptography". In: IEEE Security & Privacy 15.4 (2017), pp. 28–36.

78 Jintai Ding and Dieter Schmidt. "Rainbow, a new multivariable polynomial signature scheme". In: International conference on applied cryptography and network security. Springer. 2005, pp. 164–175.

79 Raphael Overbeck and Nicolas Sendrier. "Code-based cryptography". In: Post-quantum cryptography. Springer, 2009, pp. 95–145.

80 Christian Wieschebrink. "Two NP-complete problems in coding theory with an application in code based cryptography". In: 2006 IEEE International Symposium on Information Theory. IEEE. 2006, pp. 1733–1737.6

81 Robert J McEliece. "A public-key cryptosystem based on algebraic". In: Coding Thv 4244 (1978), pp. 114–116.

82 Harald Niederreiter and Chaoping Xing. Algebraic geometry in coding theory and cryptography. Princeton University Press, 2009.

83 Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: Communications of the ACM 21.2 (1978), pp. 120–126.

84 Ramon Ferrus et al. "On 5G radio access network slicing: Radio interface protocol features and configuration". In: IEEE Communications Magazine 56.5 (2018), pp. 184–192.

FIGURE 5: The usage encryption protocols for 5G networks security

Confidentiality: Cryptographic techniques such as AES, ECC, and ZRTP are used to encrypt data transmitted over the network, preventing unauthorized access. This encryption is crucial for protecting sensitive information, such as personal data and financial transactions, from cybercriminals and other malicious actors.

Integrity: To ensure data integrity, 5G networks employ cryptographic hash methods. These methods provide a unique digital fingerprint for the data, allowing any alterations made during transit to be detected.

Authenticity: Asymmetric key encryption, such as Elliptic Curve Cryptography (ECC), is used to verify the identities of senders and receivers. This helps prevent man-in-the-middle attacks, where an adversary intercepts transmissions and pretends to be one of the communicating parties to access sensitive information.

Key Management: Cryptographic algorithms like Internet Key Exchange (IKE) are used to create and manage secure links between endpoints. This involves the secure transfer of cryptographic keys necessary for encrypting and decrypting data transmitted through the network.

Encryption protocols have various additional applications in 5G networks, including securing specific network services. For example, real-time transport protocol (RTP) and voice-over IP (VoIP) connections are protected using cryptographic techniques such as ZRTP and SRTP. Additionally, protocols like SIKE, McEliece, and NTRU are suggested to secure particular domains of 5G networks, including the Internet of Things (IoT), mobile networks, and machine-to-machine (M2M) communication.

With the advancement of quantum computing, the security of current encryption algorithms may be compromised. Therefore, post-quantum cryptography techniques are being investigated and proposed to protect 5G and future networks. It is also essential to consider that various wireless communication networks employ encryption protocols and methods to ensure security and prevent data compromise, extending beyond just 5G networks.

Quantum computing has the potential to vastly enhance computational power, enabling it to break conventional encryption methods used in 5G networks. This poses a significant threat to the integrity of network technologies and the information they transmit. Given these potential risks, it is imperative to continue research and development in post-quantum encryption to create techniques capable of withstanding quantum threats, ensuring the security of network connectivity and the data transmitted.

Future research should focus on assessing the viability and effectiveness of post-quantum encryption techniques in real-world 5G networks. Additionally, exploring ways to make post-quantum encryption more practical, such as by reducing key sizes, would be highly beneficial. By addressing these challenges, we can better prepare for a future where quantum computing is a reality, ensuring that our communication networks remain secure.

Conclusion

Integrating 6G technology and the Internet of Things (IoT) promises transformative advancements in connectivity, data exchange, and automation across various sectors. However, this evolution brings significant security and privacy challenges that must be addressed to ensure a safe and resilient connected world.

6G enhances connectivity and data exchange capabilities and introduces new vulnerabilities. Protecting the vast amounts of data generated and transmitted by IoT devices requires robust security measures and advanced privacy techniques. Innovative solutions to mitigate privacy risks in smart homes and ensure GDPR compliance for SMEs are critical.

The security of 6G IoT applications spans various sectors, including healthcare, energy, manufacturing, and smart cities. Each sector faces unique challenges, such as safeguarding patient data in healthcare, securing smart grids in energy, and protecting industrial control systems in manufacturing. Ensuring the security of these applications is vital for maintaining the integrity and reliability of essential services.

AI-empowered security solutions are essential for managing the complexity and scale of 6G IoT networks. AI-based techniques for traffic classification, attack detection, and root cause analysis provide real-time responses to emerging threats. Additionally, the adoption of decentralized identity management and self-sovereign identity (SSI) techniques enhances security and privacy across various applications.

Effective risk management is crucial for addressing the security, trust, and operational assurance requirements of 6G networks. Risk assessment methodologies, including risk quantification and attack path discovery, offer valuable insights into mitigating potential threats. By predicting cascading effects of attacks and enhancing network resilience, these methodologies ensure robust protection against both known and unforeseen risks.

As we move forward into the 6G IoT era, it is imperative to continuously innovate and adapt our security and privacy strategies. By leveraging advanced technologies, fostering collaboration among stakeholders, and adhering to stringent regulatory frameworks, we can create a secure and trustworthy connected world. This whitepaper serves as a comprehensive guide for navigating the complex landscape of 6G IoT security and privacy, ultimately contributing to the successful deployment and operation of next-generation networks.

As we transition into the era of 5G and look forward to the advancements promised by 6G, the security of our communication networks becomes more critical than ever. The potential vulnerabilities introduced by quantum computing necessitate a shift towards post-quantum cryptographic protocols to ensure robust encryption and protection. This paper has highlighted the urgent need for advanced encryption mechanisms capable of withstanding quantum-era threats, emphasizing their importance in maintaining the integrity and privacy of extensive wireless networks. By proactively addressing these challenges, we can secure the connected world, safeguarding our digital infrastructure against future risks and ensuring the reliable and secure operation of our increasingly interconnected systems.

DISCLAIMER

The information, documentation and figures available in this publication are provided by several funded projects (listed above) and do not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

This document does not reflect the opinion of any of the projects' partners or any organisations with which the experts are affiliated. The different projects and their consortium partners are not liable for any consequence stemming from the reuse of this publication.

Funded by the European Union