An Overview of Security and Privacy Threats for Massive IoT Applications in the 6G Era

Maria Papaioannou
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
m.papaioannou@greenwich.ac.uk

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science, University of South Wales
Pontypridd, UK
jonathan@av.it.pt

***Abstract*— In recent years, global efforts have been directed toward defining the vision and research priorities for 6G mobile networks, expected to exceed the performance of 5G networks and effectively accommodate Internet of Everything (IoE) applications. Specifically, 6G networks are predicted to fulfill the demanding performance needs of emerging disruptive massive IoT applications that are beyond the capabilities of 5G due to its intrinsic constraints. Slated to be commercially available starting in 2030, 6G is set to support a wider array of applications by connecting hundreds of billions of IoT devices. However, the swift proliferation of 6G-enabled IoT devices and their escalating interconnections are likely to amplify the vulnerabilities in 6G-enabled massive IoT applications, leading to greater security and privacy concerns. Consequently, this paper provides a synopsis of the massive IoT applications projected for the 6G era that will enhance human life and outlines the potential security and privacy threats they face. The goal is to highlight critical security challenges that must be addressed to ensure that 6G-enabled massive IoT applications gain the trust of all key stakeholders and achieve their full potential.**

Keywords—6G, 6G vision, massive IoT applications, security threats

I. Introduction

The development of 5G mobile networks, despite their advancements, cannot meet the rigorous performance demands required by emerging disruptive massive IoT applications due to inherent limitations [1], [2]. Thus, the progression to the 6G mobile networks is critical, promising significantly enhanced performance metrics such as 1 Tbps peak data rate, 0.1 ms air latency, 1 μs delay jitter, and 1 Gb/m2 area traffic capacity to surpass 5G limitations and fulfill the needs of these advanced applications [1]–[5].

Expected to be commercially available from 2030, 6G networks will play a crucial role in enabling a plethora of applications across various sectors including Smart City, Smart Home, Smart Manufacturing, Smart Education/Training, Connected Autonomous Vehicles (CAV), and Intelligent Healthcare [1]–[3], [5]. For instance, 6G-enabled IoT devices might be used for health monitoring to detect deterioration in patients with chronic conditions or to gather extensive data for Smart City initiatives such as urban planning and garbage collection, thereby enhancing service quality and reducing public administrative costs.

However, the extensive deployment of 6G-enabled IoT devices and their increasing interconnectivity also elevate vulnerabilities, presenting substantial security and privacy risks [6]. Therefore, the aim of this paper is two-fold: firstly, to provide an extensive overview of massive IoT applications in the 6G era, aiming to improve quality of life, and secondly, to identify and address the potential security and privacy challenges in order to build trust among stakeholders and unlock the full potential of these technologies.

The remainder of the paper is organized as follows: Section II, firstly, outlines the vision and values of 6G, and then discusses a set of representative use case families of massive IoT applications envisioned to be deployed in the 6G era; Section III categorizes the security and privacy threats against 6G networks based on the security objectives that they intend to compromise; and finally Section IV concludes the paper.

II. Synopsis of Massive IoT Applications in 6G

The 6G vision, outlined by the European 6G Flagship project Hexa-X [1], [7] and depicted in Fig.1, aims to integrate the human, digital, and physical worlds into a seamless cyber-physical continuum. This integration will leverage networks to enhance quality of life, incorporating core principles such as sustainability, trustworthiness, and digital inclusion. 6G networks are expected to address the challenges of increased traffic, device proliferation, and the need for energy efficiency, security, and privacy. These future networks will also facilitate advancements in AI and machine learning, transforming data into actionable insights and enhancing human-machine interaction through technologies such as haptic feedback. This vision promises substantial economic growth and innovation across various sectors, aiming for a profound technological and societal transformation in the 2030s and beyond [6].

In the following, a synopsis of emerging massive IoT applications enabled by 6G is provided to elucidate the

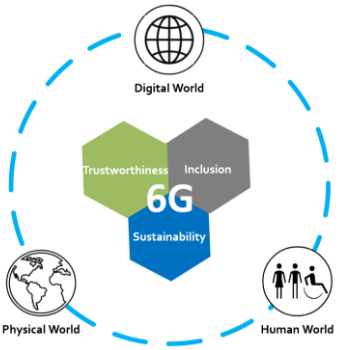

Fig. 1. 6G vision.

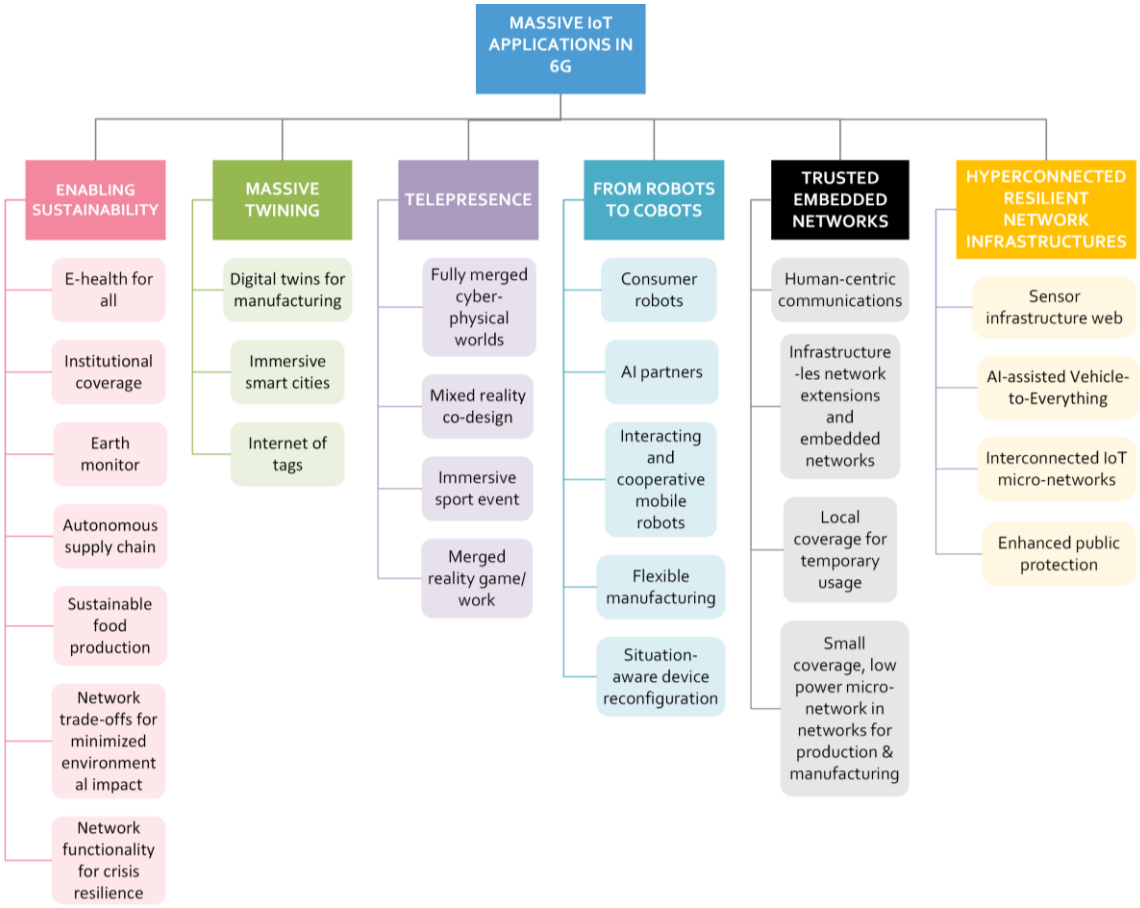

Fig. 2. Synopsis of massive IoT applications in 6G.

transformation and enhancement over current technologies. These applications involve new types of IoT-enabled interactions such as Holographic Communications, Five-Sense Communications, and Wireless Brain-Computer Interfaces [8], [9]. These interactions are expected to bring about massive IoT applications with demanding performance requirements, such as sub-millisecond latency, terabits per second data throughput, extreme energy efficiency, and ultra-low energy consumption [10]—demands that 5G cannot meet. Thus, 6G is positioned to significantly outperform 5G, becoming the crucial enabler for these advanced applications.

To systematically discuss the representative 6G-enabled massive IoT applications, the discussion is organized into six use case families. These categories are derived from the European 6G Flagship project Hexa-X [7], [11], [12], and include: 1) Enabling sustainability, 2) Massive twinning, 3) Telepresence, 4) Robots to cobots, 5) Trusted embedded networks, and 6) Hyperconnected resilient network infrastructures. A visualization of the categorization of the representative use case families and respective use cases for 6G-enabled massive IoT applications is given in Fig. 2. These families serve as a first baseline to guide future research directions on 6G, informed by ongoing European research activities [4]. The use cases within these families are considered evolutionary or disruptive [12], [4]. Evolutionary use cases extend the capabilities of 5G with new features, while disruptive ones open new horizons, leveraging 6G to transform society. Although the use cases are categorized under specific families, many of them have potential overlaps with multiple families, illustrating the interconnected nature of these future technologies.

A. *Enabling Sustainability*

The introduction of 6G networks is expected to bring a significant expansion in mobile network applications, greatly surpassing previous generations [7], [11], [12]. Additionally, 6G aims to enhance sustainability and tackle societal issues by supporting the UN Sustainable Development Goals (SDGs) and reducing environmental impacts across various sectors [7], [11], [12]. Within its sustainability focus, 6G will address major research challenges such as environmental preservation and promoting the sustainable development of societies. Achieving the SDGs will require 6G to deliver extreme performance and wide-reaching service coverage, which are crucial for fostering services in underserved areas, bridging the digital divide, monitoring and mitigating environmental problems, and improving sustainable operations [7], [11], [12]. Moreover, trustworthiness is vital in ensuring wide acceptance and reliance on 6G systems as they address critical societal and environmental challenges. The *Enabling Sustainability* use case family encompasses the following specific applications [6], as illustrated in Fig. 2: (i) E-health for all, (ii) Institutional coverage, (iii) Earth monitor, (iv) Autonomous supply chain, (v) Sustainable food production, (vi) Network trade-offs for minimized environmental impact, and (vii) Network functionality for crisis resilience.

B. *Massive Twining*

The concept of Digital Twin (DT), or massive twinning, is poised to expand significantly across a variety of sectors including manufacturing, logistics, transportation, digital health, social interactions, entertainment, public safety, and

defense in the 6G era [7], [11], [12]. DTs are virtual models that provide real-time simulations of physical entities, accurately reflecting their structure, function, and behavior. These models are pivotal for improving urban life quality, increasing productivity, enhancing sustainability, and transforming critical industries including healthcare and public safety [7], [11], [12]. The deployment of DTs involves high demands for data transfer, low latency, high reliability, and greater capacities than currently available. Creating fully synchronized and accurate digital replicas of physical and human environments will be resource-intensive, requiring detailed physical representations and sophisticated analytics for scenario testing and insight generation [7], [11], [12]. It is crucial that these solutions are sustainable, reliable, and globally applicable. High-resolution, interactive 4D mapping and other advanced tools will support dynamic DTs and virtual environments that integrate with real-time, multi-sensory mapping and analytics, enabling comprehensive data mapping and system monitoring to improve operational reliability and situational awareness. The *Massive Twinning* use case family includes the following specific applications [6], as depicted in Fig. 2: (i) Digital twins for manufacturing, (ii) Immersive smart cities, and (iii) Internet of tags.

C. Telepresence

Telepresence allows individuals to feel fully present at a real-world location in real-time, using all five senses, despite being physically elsewhere [7], [11], [12]. This technology enhances human interactions, not only with each other but also with objects within both the physical and digital realms. Telepresence seeks to expand sensory data transmission and enhance the capabilities of human senses. However, its effective implementation faces challenges such as the need for high data rates, low latency, and high reliability to avoid issues like nausea and incomplete experiences. Supported by a network of interconnected networks and intelligent systems to boost performance, telepresence also emphasizes sustainability and trustworthiness [7], [11], [12]. Its global availability and sustainable delivery could support the United Nations' Sustainable Development Goals by reducing the necessity for travel. The *Telepresence* use case family includes the following specific applications [6], as illustrated in Fig. 2: (i) Fully merged cyber-physical worlds, (ii) Mixed reality co-design, (iii) Immersive sport event, and (iv) Merged reality game/work.

D. From Robots to Cobots

The 6G system evolves robots into "cobots" (collaborative robots) that collaborate and establish symbiotic relationships to efficiently complete complex tasks and meet human needs [7], [11], [12]. Trustworthiness and digital inclusion are key in enhancing both human-machine and machine-machine interactions. This cooperative approach allows for the sustainable completion of complex tasks using existing capabilities without additional sophisticated machinery. It also fosters new business models where machinery can handle specialized, on-demand tasks, support production in small batches, and utilize advanced techniques like additive manufacturing. The primary challenges for this use case family include ensuring trustworthiness, particularly important due to the reliance on connected intelligence and collective decision-making [7], [11], [12]. Other challenges include managing resource allocation and adapting network topologies for extreme performance needs in areas such as industrial applications, which require precise positioning, high dependability, and low latency. Additionally, promoting sustainability and facilitating meaningful human-machine interactions and AI partnerships are crucial to address the challenge of inclusion [7], [11], [12]. The *From Robots to Cobots* use case family encompasses the following specific applications [6], as shown in Fig. 2: (i) Consumer robots, (ii) AI partners, (iii) Interacting and cooperative mobile robots, (iv) Flexible manufacturing, and (v) Situation-aware device reconfiguration.

E. Trusted Embedded Networks

The Trusted Embedded Networks use case family comprises scenarios that involve sub-networks or networks of networks, where a high degree of trustworthiness is essential [7], [11], [12]. Traditionally, mobile communications have relied on cellular networks, but certain applications necessitate local or private communication networks to handle highly sensitive information within broader network structures [7], [11], [12]. These situations call for network topologies and security frameworks that extend beyond traditional cellular network architectures. To safeguard sensitive data, trusted embedded networks and independent sub-networks such as body area networks or on-board networks for Automated Guided Vehicles (AGVs) need to be seamlessly incorporated into larger networks or maintained as private, on-premises networks. The *Trusted Embedded Networks* use case family includes the following applications [6], as depicted in Fig. 2: (i) Human-centric communications, which focus on privacy and security in personal interactions; (ii) Infrastructure-less network extensions and embedded networks; (iii) Local coverage for temporary use; and (iv) Small coverage, low power micro-networks in networks designed specifically for production and manufacturing.

F. Hyperconnected Resilient Network Infrastructures

The Hyperconnected Resilient Network Infrastructures use case family focuses on scenarios that involve sub-networks or networks of networks, demanding a high level of resilience [7], [11], [12]. While cellular networks have traditionally been the primary mode of communication, certain situations require localized or private networks to protect highly sensitive information [7], [11], [12]. These specific needs call for network architectures and security protocols that go beyond standard cellular frameworks. To ensure the secure handling of sensitive data, robust embedded networks and specialized sub-networks, such as body area networks or on-board networks for AGVs, need to be seamlessly integrated into larger networks or kept as private networks on-site [7], [11], [12]. The *Hyperconnected Resilient Network Infrastructures* use case family includes the following specific applications [6], illustrated also in Fig. 2: (i) Sensor infrastructure web, which focuses on extensive sensor networks for data collection and monitoring; (ii) AI-assisted Vehicle-to-Everything (V2X), enhancing communication between vehicles and various entities; (iii) Interconnected IoT micro-networks, which facilitate detailed IoT deployments; and (iv) Enhanced public protection, aimed at improving safety and emergency responses.

III. Security and Privacy Threats in Massive IoT Applications in 6G

6G networks are expected to support a wide range of applications handling sensitive information across various

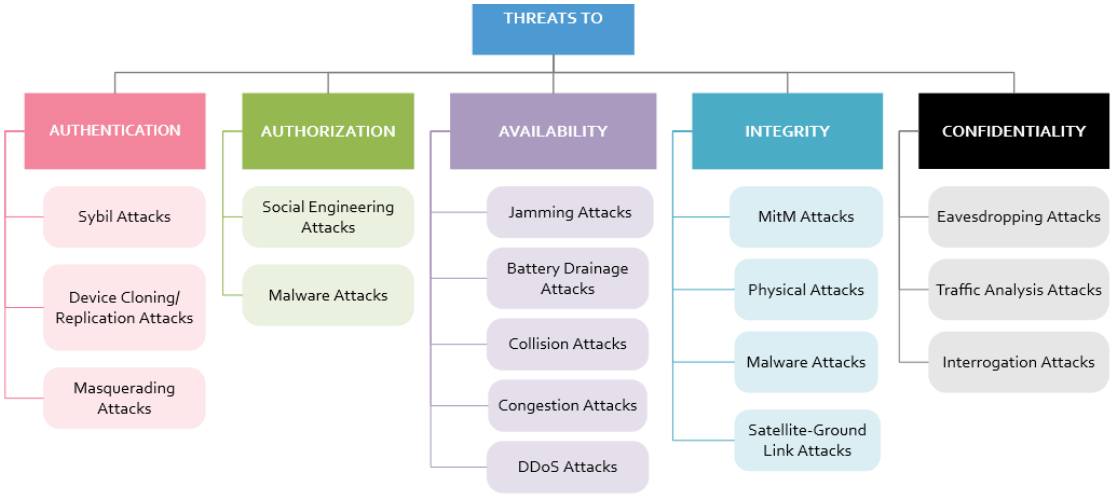

Fig. 3. Synopsis of security and privacy threats in massive IoT applications in 6G.

sectors, including healthcare, finance, government, defense, and industry [5], [13], [14]. For instance, healthcare applications may involve transmitting sensitive patient data such as real-time health monitoring, necessitating secure transmission to protect privacy and ensure reliable care, while financial applications might require secure processing of critical data such as transactions and personal details to prevent fraud and protect privacy. Given the sensitivity of the data involved, security and privacy concerns are heightened. To address this, the aim of this section is to give a structured approach to categorize security threats targeting 6G networks. This approach is based on the specific security objectives these threats aim to compromise, helping stakeholders understand and mitigate potential vulnerabilities effectively. A synopsis of the categorization of the security threats in massive IoT applications in 6G is illustrated in Fig. 3.

A. *Threats to Authentication*

Authentication: In 6G networks, authentication is crucial for verifying the identities of communicating entities (entity authentication) as well as the authenticity of the transmitted messages (message authentication) [5], [6], [13], [14]. IoT devices often have constrained resources, there is a significant need for lightweight authentication that provides necessary security without overwhelming the device's limited computational and memory capacities.

Traditional methods, particularly those based on Public Key Infrastructure (PKI), fall short in adequately securing the widespread deployment of IoT devices due to inefficiencies and scalability issues. These shortcomings expose vulnerabilities that can be exploited by adversaries, making the authentication process in massive IoT networks a prime target for various types of attacks. Several types of attacks target the authentication process in massive IoT networks including the following [5], [6], [13], [14]:

1) Sybil Attack: In this attack, an IoT device may claim multiple fake identities, thus allowing rogue devices to masquerade as legitimate ones. This situation enables the rogue node to connect with multiple other IoT devices, thereby maximizing its influence and potentially leading the system to erroneous conclusions. Sybil attacks are differentiated based on factors such as the mode of communication between nodes (direct or indirect), the origin of identities (fabricated or stolen), and the timing of sybil identities' activities (synchronous or asynchronous).

2) Device Cloning/Replication Attacks: These attacks involve capturing a sensor device, extracting its encrypted information, and then using this data to create multiple device clones within the network. These clones can then compromise the authentication and overall security objectives of the network. The success of device cloning attacks often stems from the absence of location-based authentication schemes that would otherwise prevent multiple devices from being authenticated in the same location.

3) Masquerading Attacks: In such attacks, an adversary may pose as a legitimate user by inserting rogue devices to gain unauthorized access to services, or they might impersonate an IoT device to provide fraudulent services to users. These attacks are particularly menacing in sectors such as healthcare, where Internet of Medical Things (IoMT) devices play critical and potentially life-saving roles.

To fortify the security of massive IoT networks in 6G against these threats, it is imperative to implement robust authentication mechanisms. This includes the use of advanced, scalable authentication methods that can handle the extensive scale and diversity of IoT devices. Incorporating location-based authentication schemes and enforcing stringent security protocols are essential steps to enhancing the security of the authentication process and mitigating the risks posed by these sophisticated attacks.

B. *Threats to Authorization*

Authorization: Authorization within 6G networks involves granting permissions to access specific network resources or services [5], [6], [13], [14]. It ensures that only authorized devices or personnel can access sensitive functions or data, thereby preventing unauthorized use. Access control systems are typically utilized to enforce these authorization policies effectively. Adversaries may exploit weak *authorization* mechanisms within 6G networks to gain unauthorized access to network resources. Several types of attacks target the authorization process in massive IoT networks [5], [6], [13], [14], including the following:

1) Social Engineering Attacks: Due to users' limited familiarity with security practices and insufficient training, IoT devices are especially susceptible to social engineering attacks. In these attacks, malicious actors impersonate legitimate entities to gain unauthorized access to networked IoT devices. This vulnerability is especially concerning in critical sectors such as healthcare, where compromised devices monitoring vital signs could endanger lives.

2) Malware Attacks: Weak authorization can allow malware to infect IoT devices in massive IoT networks. These compromised devices can then act as bots to propagate the attack within the network, leading to further unauthorized access to network services and sensitive data.

To effectively counter authorization risks in 6G networks, a comprehensive strategy is required. Strengthening authorization through advanced, dynamic access controls that adapt to evolving conditions and threats is critical. Additionally, educating users on security best practices and awareness of threats like social engineering can greatly reduce breaches. Adopting a security-by-design approach from the outset in IoT applications and network infrastructure enhances resilience by addressing vulnerabilities early. Regular security audits and updates to authorization protocols are also vital to guard against emerging threats, collectively ensuring the robust security of 6G networks and the protection of sensitive data and IoT devices [5], [6], [13], [14].

C. Threats to Availability

Availability: This security objective ensures that network services are continuously available to authorized users and are resilient against attacks aimed at disrupting service delivery. In 6G era, IoT technology is increasingly being adopted in various applications to address the limitations of centralized cloud-based systems. Nonetheless, such systems that depend on a vast network of interconnected IoT devices encounter challenges related to resource and computational limitations, affecting the reliability of services. Various forms of attacks targeting different network layers can significantly impact the *availability* of these services within 6G networks, including the following [5], [6], [13], [14]:

1) Jamming attacks: These attacks disrupt communication channels or computing resources by flooding them with excessive messages, thereby impeding normal service operations. For instance, in a healthcare scenario where IoT devices are crucial for alerting caregivers about patient needs, jamming can delay critical alerts, endangering patient lives.

2) Battery drainage attacks: These attacks exploit the limited battery life of IoT devices by sending fraudulent messages to deplete their energy rapidly in order to make them unavailable to the legitimate user.

3) Collision attacks: These attacks occur when multiple nodes transmit data on the same frequency, causing confusion at the receiver's end and leading to the loss and retransmission of data, thereby straining network resources.

4) Congestion attacks: These attacks involve flooding the network with unnecessary messages, which leads to channel overload and the unavailability of timely services and data.

5) Distributed denial-of-service (DDoS) attacks: These attacks leverage IoT botnets to flood network nodes with excessive requests, severely disrupting service availability. Increasingly sophisticated and automated, DDoS attacks exploit vulnerabilities across numerous devices, making them challenging to mitigate. IoT networks, with their limited resources, are particularly vulnerable compared to robust cloud platforms. The growing trend of using botnets for widespread attacks significantly restricts access for legitimate users and reduces their ability to use network resources effectively.

To safeguard service availability in 6G IoT networks, key measures include implementing strong security protocols like advanced encryption and robust authentication to prevent unauthorized access. Anti-jamming techniques such as frequency hopping and spread spectrum are vital for thwarting jamming attacks. Energy-efficient protocols help mitigate battery drainage and collision issues, while network monitoring tools and intrusion detection systems are crucial for quickly addressing DDoS or congestion attacks. Regular security audits and timely updates to network firmware and software are also essential for maintaining robust defenses and ensuring reliable service continuity in 6G networks.

D. Threats to Integrity

Integrity: Integrity assures that data is not altered or destroyed in an unauthorized way. Maintaining data integrity is essential in 6G networks to ensure that the information transmitted remains accurate and unmodified during transmission. This is particularly vital in applications including AI-assisted Vehicle-to-Everything (V2X) or precision healthcare, where human safety could depend on the reliability of the data. Threats to the integrity of 6G networks might include the following attack types:

1) Man-in-the-Middle (MitM) Attacks: These attacks occur when an attacker intercepts and potentially alters the communication between two parties without their knowledge. For example, in Internet of Medical Things (IoMT) networks, MitM attacks can modify medical data being transmitted to remote servers or stored on wearable devices, thus jeopardizing data integrity.

2) Physical Attacks: If an adversary gains physical access to an IoT device, they can tamper with its components to alter its behavior and stored data. Such attacks directly threaten the integrity and functionality of the device and the network.

3) Malware Attacks: The absence of robust malware detection systems for the vast number of IoT devices makes them susceptible to attacks that compromise their integrity. Attackers can deploy malicious software to exploit vulnerabilities in the device's networking software and hardware, causing damage and disruption.

4) Satellite-Ground Link Attacks: In networks involving satellite communications, legitimate nodes may be tampered and converted into malicious nodes. This manipulation can lead to data tampering during transmission between satellites and ground stations. Detecting such attacks is complex, as the compromised nodes still maintain valid identities while running malicious operations.

To protect the integrity of 6G networks, it is crucial to implement advanced security protocols, including strong encryption and authentication, as well as physical security

measures to prevent unauthorized access. Advanced malware detection and enhanced intrusion detection systems, particularly for complex configurations like satellite-ground links, are also vital. Regular security audits and updates are essential for addressing vulnerabilities swiftly. Also, educating users and administrators on security best practices will further strengthen defenses against integrity attacks, ensuring the reliability of 6G networks and their devices.

E. Threats to Confidentiality

Confidentiality: Confidentiality ensures that sensitive data information remains inaccessible to unauthorized entities. In the 6G context, confidentiality is crucial for protecting sensitive data transmitted between IoT devices and network gateways. However, the vast scale and limited resources of IoT devices in 6G networks present substantial challenges in maintaining high levels of data confidentiality, making the network vulnerable to various security threats, such as:

1) Eavesdropping: Adversaries might intercept data during transmission, such as when a wearable sensor sends a patient's vital signs to a smartphone. By monitoring and accessing the transmitted data, they can gain unauthorized access to sensitive information.

2) Traffic Analysis: This form of passive interception allows adversaries to analyze communication patterns and extract confidential data without directly accessing the content of the communications. This technique can reveal significant information from patterns and metadata associated with the data flows.

3) Interrogation Attacks: In these attacks, a malicious actor impersonates a legitimate entity to send requests to other devices in the network, to extract sensitive information.

To protect data confidentiality in 6G networks, several mitigation strategies are essential. Lightweight cryptographic solutions should be implemented to suit IoT devices with limited resources, ensuring security without overwhelming their capabilities. Enhancing authentication and authorization mechanisms is critical to defend against impersonation and unauthorized access. Additionally, employing secure communication protocols with encryption and detection features helps prevent data interception during transit. Finally, continuous monitoring and anomaly detection systems are necessary to promptly identify and address potential security breaches, thereby safeguarding sensitive information across diverse applications within the 6G network.

IV. CONCLUSIONS

This paper has systematically explored the forthcoming landscape of 6G mobile networks with a dual focus. Firstly, it has provided an extensive overview of massive IoT applications anticipated in the 6G era, designed to enhance the quality of life through advanced use case families such as Enabling Sustainability, Massive Twinning, Telepresence, From Robots to Cobots, Trusted Embedded Networks, and Hyperconnected Resilient Network Infrastructures. These applications not only promise to extend the capabilities of current technologies but also to integrate seamlessly into everyday human activities, thereby significantly improving societal functions and environmental sustainability. Secondly, the paper has discussed the pivotal security and privacy challenges intrinsic to these advanced networks. By categorizing threats based on the security objective that they intent to compromise, namely authentication, authorization, availability, integrity, and confidentiality, this work highlights potential countermeasures to safeguard these systems. The ultimate goal is to foster a robust basis that builds trust among all stakeholders and unlocks the full potential of 6G technologies. Thus, ensuring the security and privacy of these networks is not just a technical necessity but a prerequisite for realizing the vast benefits of the 6G era.

ACKNOWLEDGMENT

This research work was sponsored by R-PODID supported by the Chips Joint Undertaking (GA 101112338) and its members, including the national top-up funding by Fundação para a Ciência e Tecnologia (KDT/2022/RIA/R-PODID/INSTITUTO DE TELECOMUNICAÇÕES).

REFERENCES

[1] M. A. Uusitalo *et al.*, "6G Vision, Value, Use Cases and Technologies from European 6G Flagship Project Hexa-X," *IEEE Access*, vol. 9, pp. 160004–160020, 2021.

[2] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.

[3] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling Massive IoT Toward 6G: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, Aug. 2021.

[4] "The 6G Architecture Landscape European perspective Version 1.0, December 2022."

[5] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The Roadmap to 6G Security and Privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[6] G. Mantas, F. B. Saghezchi, J. Rodriguez, and V. Sucasas, Eds., *Security and Privacy for 6G Massive IoT*. Wiley (Accepted to be published).

[7] "Hexa-X – Connecting human, physical, and digital worlds." .

[8] The 5G Infrastructure Association, "European Vision for the 6G Network Ecosystem," *5GIA*, 2021.

[9] U. M. Malik, M. A. Javed, S. Zeadally, and S. ul Islam, "Energy-Efficient Fog Computing for 6G-Enabled Massive IoT: Recent Trends and Future Opportunities," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14572–14594, Aug. 2022.

[10] D. C. Nguyen *et al.*, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022.

[11] Hexa-X Deliverable D1.2, "Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum," Apr. 2021.

[12] Hexa-X Deliverable D1.3, "Targets and requirements for 6G – initial E2E architecture," 2022.

[13] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, pp. 53–87, 2022.

[14] M. Papaioannou *et al.*, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, no. May, pp. 1–15, 2020.