5G Security Features, Vulnerabilities, Threats, and Data Protection in IoT and Mobile Devices: A Systematic Review

Alexandre Sousa[1], Manuel J. C. S. Reis[2]

[1]University of Trás-os-Montes e Alto Douro, Quinta de Prados, Portugal
[2]University of Trás-os-Montes e Alto Douro, Engineering Department/IEETA, Quinta de Prados, Portugal
Email: alexandreribassousa@gmail.com

Abstract

The evolution of wireless communications, from the first to the fifth generation, has driven Internet of Things (IoT) advancements. IoT is transforming sectors like agriculture, healthcare, and transportation, but also presents challenges like spectrum bandwidth demand, speed requirements, and security issues. IoT environments, with embedded sensors and actuators, connect to other devices to transmit and receive data over the internet. These data are processed locally or in the cloud, enabling decision-making and automation. Various wireless technologies, including Bluetooth, Zigbee, LoRa, and WiFi, cater to specific IoT applications. 5G, with its high speeds, low latency, and efficient bandwidth sharing, is ideal for high-speed data transmission, and thus it provides robust infrastructure for low-latency and bandwidth-sensitive applications. This latest mobile network technology is being rapidly implemented worldwide, providing unprecedented throughput and low latency, which are crucial for the IoT. This paper presents a comprehensive systematic review on 5G security features, vulnerabilities, threats to mobile devices, security in IoT devices, common attacks to IoT devices and protection of data in this environment. Despite enhanced security, 5G faces challenges like Distributed Denial of Service (DDoS), Man In The Middle (MITM), cross-slice disruptions, and side-channel attacks.

Keywords: IoT, 5G Networks, Security, Mobile Devices.

1. Introduction

The communication paradigm known as IoT (Internet of Things) involves a network of interconnected devices equipped with sensors, actuators, and other technologies to transmit and receive data over the internet [1]. Sensors collect data, which is then processed and analyzed either locally or in the cloud to extract meaningful insights. These processed data can identify patterns, anomalies, or trends, facilitating decision-making and automation. IoT applications

utilize the data sent to the cloud from gateways or edge servers, which are located within the same network as the IoT devices. This concept turns normal objects, or so called "things", into "smart things", shifting the way people interact with these smart things, enabling seamless connectivity, leading to a greater interconnected and data driven society. IoT technologies are being applied to revolutionize multiple sectors, such as, precision farming and crops monitoring in agriculture, healthcare with wearable fitness tracker devices, transportation with smart traffic systems and connected cars, among many another [2].

In the IoT context, there are many different types of architectures that can be implemented, like, for example, Three-level IoT architecture, SDN-based architecture, QoS-Based architecture, Service-oriented architecture, Mobility-First architecture, Cloud/Things architecture, IoT-A Architecture and Social Internet of Things [3]. However, over time new technologies were developed and others were improved, such as 5G, machine learning, edge computing, and Industry 4.0, resulting in the evolution from IoT to IoT 2.0. This new paradigm is an ongoing vision that aims to utilize these technologies fulfilling the needs of the new demands of IoT.

The exponential growth of devices communicating revealed other challenges, like the extreme demand for spectrum bandwidth, need for faster speeds and security [4], [5]. The evolution of this paradigm has been driven by wireless communications, over the years, since the first generation until the present day, with fifth generation mobile networks (5G).

Rahimi et al. [3] purposed a 5G based IoT new architecture (5G-IoT) that implements innovative systems like Nano-Chip-based devices, Heterogeneous Networks (HetNet), Direct Device-to-Device (D2D) Fifth-generation (5G) networks, and Machine-Type Communication (MTC), that involves automated data communication between devices and data transport infrastructure. MTC supports a wide range of applications, like Wireless Software-Defined Networking (WSDN), Mobile Edge Computing (MEC), and Mobile Cloud Computing (MCC).

In IoT, it is possible to implement different technologies of wireless communications and each one has their pros and cons and the selection has to be made by analyzing first the application requirements [2]. The common transmission mediums used in IoT are Bluetooth, Zigbee, LoRa and Wifi, where each one is more appropriated for each particular scenario. For example, LoRa uses frequency hopping and spreading sequences to enable multi-spectrum bandwidth sharing without causing interference, which makes it a good option for long range, low power IoT applications that require efficient use of the spectrum and does not need to transmit big data rates. The best solution for high speed data transmission application is 5G, due to its high speeds, low latency and efficient bandwidth sharing [1]. With the deployment of low-latency and bandwidth sensitive mobile and real time applications, this fifth generation has become a critical enabler for IoT, providing a robust infrastructure. The widespread adoption of this communication platform includes a set of features, such as high speed, QoS (Quality of Service), low latency, with modern radio technology, service-oriented design and cloud infrastructure combined with the specifications developed by the third generation of this technology.

The 5GC (5G Core) is made possible by leveraging network slicing and Network Function Virtualization (NFV), where multiple Network Functions (NF) are involved to serve different user requests on the control plane. 5G cellular systems also offer enhanced security with zero

trust and multi-tenant architecture based on availability, confidentiality and integrity. However, the rapid implementation of innovative technologies has also exposed the 5GC to various security challenges. Fifth generation-based applications face security risks such as Distributed Denial of Service (DDoS), Man In The Middle (MITM), cross slice disruptions and side channel attacks.

As mentioned before, the demands on IoT increased with the growth of devices and, as a consequence, the quantity of data transmitted, even though the tools and systems are evolving all the time. However, security remains a critical challenge for the networks themselves, and IoT applications in particular.

The 5G-IoT architecture provides a lot of features, but also challenges. The purpose of this work is to present a systematic review in order to better understanding how security is affected by these platforms and how these challenges can be solved.

To achieve these objectives a research question was addressed:

RQ1: How are 5G and IoT related in terms of remote services, security on mobile devices, and connectivity?

2. Methodology and Research Contribution

To conduct this systematic literature review, we adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines.

A. Objective

The primary objective of this literature review is to explore the relationships between 5G technology and IoT platforms, in the context of security, and provide answers to the research question RQ1 presented above. Both technologies are highly innovative, but their rapid deployment has revealed significant vulnerabilities. While the convergence of 5G and IoT has greatly enhanced IoT systems, security remains a persistent challenge due to their ongoing evolution and advancement. As a result, security has become a crucial area of research and analysis.

B. Search Strategy

The search was conducted on April 25th, 2024, using the Scopus database. The criteria focused on publications from the last six years, spanning 2018 to 2024, and targeted articles with the specified terms in their abstract, title, or keywords. Only English-language journal or conference articles were included. The specific query string used was: TITLE-ABSKEY (5G OR IoT AND security AND mobile AND devices AND remote AND services) AND PUBYEAR > 2017 AND PUBYEAR < 2025 AND (LIMIT-TO (LANGUAGE, “English”)) AND (LIMIT-TO (EXACTKEYWORD, “Internet of Things”) OR LIMIT-TO (EXACTKEYWORD, “Network Security”) OR LIMIT-TO (EXACTKEYWORD, “5G Mobile Communication Systems”)) AND (LIMIT-TO (SUBJAREA, “ENGI”)).

C. Returned Results

Initially, the query using the terms 5G, IoT, mobile devices, and remote services yielded 194 documents. The research was then refined to include only English documents from the last six years (2018 to 2024), resulting in 159 documents. Applying further limitations to the query, focusing on exact keywords such as Internet of Things, Network Security, and 5G Mobile Communication Systems, reduced the number of documents to 69. After being screened by two experts based on their titles and abstracts, 20 papers were selected for this systematic review, and listed as references [1-20] in the references at the end of this work.

D. Critical Security Challenges and Ongoing Research in the Intersection of 5G and IoT

This structured approach enabled a thorough and focused analysis of the intersection between 5G and IoT platforms, emphasizing the critical security issues and ongoing challenges in this rapidly evolving field. This systematic review highlights the need for continuous research and adaptive security measures to keep up with technological advancements. In the following sections, we will present a detailed analysis of the results, followed by a discussion.

3. Results' Analysis

In order to achieve exact results, key information was collected.

Some researchers have forecast the soaring of IoT devices in the future, which in return would demand more resources from IoT system, such as bandwidth, security, privacy efficiency, low latency, battery lifetime, and energy consumption [2]–[4], [6]. Thus, IoT is propelling the progression of the Internet, in what concerns to security and networks, while at the same time it poses certain problems for the Internet, which include the large number of nodes, security issues, and new protocols [6]. To tackle these challenges, a combination of 5G technology and IoT exists that enables these technologies.

The connectivity and speed that comes with using 5G are seamless and faster compared to the previous networks, posing new hazards. 5G benefits from a high level of security and reliability with the implementation of encrypting user traffic and applying authentication between the user equipment and the central station, playing a crucial role in cybersecurity [7]. While earlier cellular networks were more inclined towards keeping connectivity alive, 5G cellular systems have focused on end user anonymity, to employ a more sophisticated approach towards security. This integrated approach is used to deal with problems like identification, access control and audit in the Heterogeneous Computer Networks (HCN) at each layer of the network.

5G enjoys strong security and dependability due to encrypting user traffic and enforcing authentication between user equipment and the central station, which is essential for cybersecurity [7]. The security of access and mobility management in the legacy network also contributes to the advantages of 5G through key hierarchy and handover key management. The most significant improvements in security offered by 5G are:

- Structured persistent user identity and encrypted data transmission;

- Enhanced methods for verifying identity;
- Safeguarding the integrity of data;
- Facilitate entry through secure channels;
- Encryption through Transport Layer Security (TLS) is implemented for communication between network functions within the core network;
- Traceability for easier tracking of activities, conducting security assessments.

Several improvements have been made with the integration of 5G technology into IoT web-based applications. For example, high reliability has been experienced, the applications have been made simpler with more practicality and analytically efficiency, agility, flexibility and availability from 5G technology. These improvements also include the protection of the data stored on the system, protection of the users using the system, protection of the network that supports the system, and protection from cyber-attacks. The confidentiality of stored and transferred data, as well as the safeguard of critical networks and connections depends on clear encryption methods, strong authentication, and effective detectors [6].

Through the implementation of 5G network slicing, resources are divided into logical and virtual networks, in order to cater to use cases with unique characteristics and Service Level Agreement (SLA) demands [7], [8]. In a similar manner, a 5G slice tailored for a critical IoT scenario will have different throughput, latency, and reliability needs, compared to a 5G slice designed for a non-critical use case. The primary obstacles identified in this survey regarding 5G network slicing include the following main challenges:

- the radio resources being transformed into virtual resources;
- defining fine-grained network functions to enhance the composition of services;
- how to effectively carry out seamless coordination and oversight of the services being delivered.

In addition to outlining the benefits of 5G-IoT and its potential uses, in [8] the authors also discussed the limitations, such as scalability, dynamic security, and variety of applications.

However, the issues were addressed in great depth, and the future directions were more generalized than specific. However, researchers face several challenges, such as the need to propose a 5G-IoT architecture that ensures proper communication between long-term machine agents and addresses security issues [6]. This area has not received sufficient attention from security experts and researchers, resulting in limited information and solutions.

The 5G-IoT architecture implements innovative technologies and relies on a structure of eight layers [3]; please refer to figure 1.

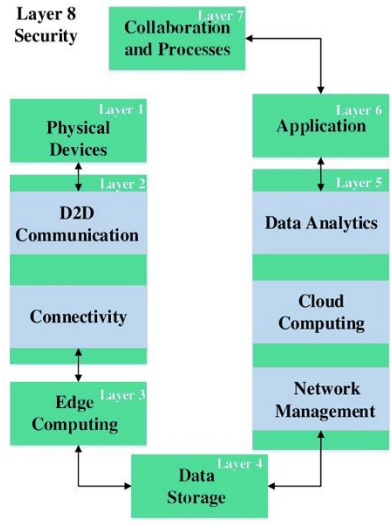

Fig. 1: Layer 8 security block diagram of the 5G-IoT architecture mobile network technology (adapted from [3]).

A. Physical Device Layer

This layer allows incorporating the lowermost layer, which consists of the wireless sensors, actuators and controllers, that are featured in the IoT. Therefore, as previously stated, physical devices are an inevitable component of every IoT system. It is expected the development of innovative technologies in computing, such as nano-chips, that are expected to reduce the need for high computations while increasing efficiency in power usage. They create massive amounts of pre-processed data that are supposed to be utilized at the analytics layer.

B. Communication Layer

This layer comprises two sub-layers: The Direct Device to Device (D2D) Communication sub-layer, and the Connectivity sub-layer.

The D2D Communication sub-layer depends largely on the processing capacity of physical devices or nods and allows each node to produce distinct data. To further improve the overall operation and productivity of the complete IoT system, these devices build up an HetNet that enables smooth transition. This sub-layer uses Wireless Sensors Network (WSN) communication protocols and procedures to form groups and elect leaders to manage the flow of networking. Some of the key technologies that bolster this sub-layer are millimeter wave (mmWave) that can provide very high data rates, and 5G technology which has emerged as one of the most important tools to expand device to device communication and is among the prime contenders for 5G usage.

In the Connectivity sub-layer, devices connect to a Base Station where they send their analyzed data to a storage through the Intranet. At present, this level has some challenges like only managing a few connections at a time, having different data transfer formats that are incompatible with each other, which can be seen in autonomous vehicles, and having very large messages which make communication slow due to network latency. This sub-layer is expected to get boosted in reliability, performance and flexibility by the growing implementation of the upcoming 5G networks. Another significant technology to indulge here is termed as Advanced Spectrum Sharing and Interference Management (SSIM), and that allows IoT devices to select optimum spectrum in what will cause minimal interference, so that adequate latency, sturdy connections, and multiple data type can flourish.

C. Edge (Fog) Computing Layer

At this tier, information is handled and analyzed at the network edge by specific nodes, with assistance from leaders. As 5G technology becomes prevalent and mobile phones, including smartphones, are established as primary devices, Mobile Edge Computing (MEC) technology emerges as a highly effective solution for challenges at this layer.

D. Data Storage Layer

This level is designed to store the information processed by the devices at the physical edge, when these form a part of storage hubs, as well as the raw information kept in such hubs. It must be highlighted that there is a need for specific security measures, due to the great volume of data and traffic in future applications.

E. Management Service Layer

This layer comprises three sub-layers: The Network Management sub-layer, the Cloud Computing sub-layer, and the Data Analytics sub-layer.

The Network Management sub-layer meets the goal of Network Function Virtualization (NFV) and Wireless SDN to enhance network architecture and several protocols.

The Cloud Computing sub-layer analyzes data collected through edge computing in the cloud through 5G MCC and initiate cloud computing activities in real time, while also apportioning processing tasks to the Mobile Devices.

The Data Analytics sub-layer performs processing from raw data through various analytical methods, in order to gain valuable information and increase Big Data algorithms computational efficiency.

F. Application Layer

This layer enables software to manage new layers and static data, adding various dimensions to different industries and business needs through control apps, vertical and mobile apps, as well as BIT and Analytics. It effectively transforms information into a product, empowering companies to make informed decisions at the right time.

G. Collaboration and Process Layer

This layer acts as a bridge that converts the raw data from the IoT to usable outputs, to which the user can then apply it. To fully harness IoT services, there is a need for efficient and proper interaction among the users involved in the services.

H. Security Layer

This layer safeguards the previous layers by implementing data encryption, user authentication, network access control, and cloud security, all of which utilize forensic analysis to detect and counter cyber threats. Consequently, security and privacy in the proposed architecture are ensured, thanks to the development of a security taxonomy by a team of researchers. From the point of view of this study, this is the most important layer and it will be inspected in the next section.

4. THE 5G SECURITY LAYER

Many researchers have presented novel findings about 5G specifications, but the security aspects of this technology may still be underdeveloped. They have also highlighted new design concerns in the 5G protocol suite that could potentially expose users' locations, downgrade their service to traditional networks like 4G or 3G, and allow tracking of calls, texts, or web browsing.

The work in [9] also addressed the main attack models against privacy, availability, authentication and integrity, which are recalled in table I.

The challenges associated with the 5G IoT architectural framework include: scalability, network management, connection, use of standard, real-time response latency, integration of heterogeneous devices, dependable security, identity and privacy, and finally authentication [10].

As the number of connected devices increases with the deployment of multiple numbers of sensor nodes, new coverage problems and security attacks occur [11]. The growing connectivity of smart devices under 5G IoT networks multiplies the large and diverse set of connected IoT devices and makes the task of securing those devices even more difficult. Rather impressively, these problems of 5G-IoT can be considered soluble, where scalability issues have been pointed out to be solvable via software-defined networking [12]–[14]. Review studies emphasize the urgent need to address these problems and argue that standardization helps protect individual information against the expanding threat landscape of 5G-IoT.

The nature of 5G networks complicates security concerns related to authentication, integrity, and privacy. Voice and data security currently rely on traditional security architectures, which include user identity management, mutual authentication between the network and devices, and communication channel protection. However, this approach is insufficient to secure 5G networks, indicating a need for enhancements in privacy and security technologies [7].

The main threats to IoT security include inadequate encryption, default passwords, proprietary platforms, limited support, and insufficient user awareness [15]. According to [15], attackers persist in attempting to compromise and dominate IoT devices in order to establish their botnet

system. The wide variety of IoT devices creates numerous botnets networks, making it extremely difficult to remove them from intruders. Next, the assailants will target the victim and compromise the service based on the virtual request type, such as HTTP, TCP SYN, DNS, ICMP, and SIP. Following the deployment of the botnet, the attackers utilize the device to carry out attack instructions while keeping their main identity undisclosed. The IoT presents several security challenges due to its computational limitations, such as power constraints, scalability, and its distributed network structure [16]. These issues arise from core system vulnerabilities, connectivity issues, limited control over updates, and data

Table 1: Main attack models against privacy availability and authentication in 5G mobile network technology.

Against Privacy	Against Availability	Against authentication	Against Integrity
Man-in-the-middle attack	DoS attack	Partial message collision attack	Tampering
Impersonation	Free-Riddling attack	Password reuse attack	Cloning
Eavesdropping	Skimming attack	Dictionary attack	Message blocking
Relay attack	Redirection attack	Leak of verifier attack	Spam attack
Collaborated attack	FIFO attack	Forgery attack	–
Tracing attack	Hear	Stolen smart-card attack	–
Spoofing	–	–	–
Stalking	–	–	–
Masquerade attack	–	–	–

With a large number of IoT devices connecting to a network, security often does not receive the necessary attention and can be exploited. Additionally, users have limited control over update timing, as they may not fully understand the internal operating mechanisms of their devices [16].

The lack of sufficient resources to establish and enforce secure policies leaves devices vulnerable to attacks. Additionally, human errors and ignorance can exacerbate these challenges. Users and operators may not follow best practices, such as changing default passwords or regularly updating devices, leading to further security flaws [16].

Considering SDN architecture can enhance network efficiency during the implementation of 5G technology [10]. In the context of SDN-based 5G, key security challenges include spoofing, man-in-the-middle attacks, eavesdropping, malicious activities, and unauthorized connections. These vulnerabilities often arise from inadequate security measures in account authentication between the controller and applications.

5G technology enables the physical network to be sliced into multiple virtual networks and supports numerous Radio Access Networks (RANs) [7], [8]. Network Function Virtualization (NFV) manages virtualization and network slicing within 5G mobile systems, offering benefits such as enhanced mobility, reduced latency, improved resilience, security, and availability. However, maintaining trust in virtualized NFV environments poses challenges [10]. Major security concerns in NFV and 5G technology include data acquisition, protection, authenticity, and integrity. NFV is still evolving, leading to dynamic solutions and potential security complications due to configuration errors. Threat models in NFV include spoofing, sniffing, DoS attacks, flooding, and side-channel attacks.

Security technologies include data encryption mechanisms like Advanced Encryption Standard (AES), key exchange mechanisms such as Diffie-Hellman (DH), and Rivest-Shamir-Adleman (RSA) for managing data transfer, exchange, and digital signatures [6]. These methods heavily rely on robust cryptographic protocols. Choosing high-performance computing platforms can pose challenges for future IoT devices with limited computing capabilities. Additionally, to support future IoT networks, models and protocols need reengineered authentication and authorization mechanisms. Integrating blockchain technology into IoT networks enhances decentralization, ensuring secure, independent, and transparent transactions and interactions. In this framework, blockchain acts as the universal ledger for all devices, verifying the legitimacy of communications [10]. According to the work in [17], incorporating blockchain mechanisms within the fog layer can address platform issues, leveraging fog nodes for intensive processing tasks. Effective 5G solutions must prioritize functionality, enhanced security, and privacy techniques. Haris and Al-Maadee [10] also highlight blockchain's potential to resolve IoT's decentralization, compatibility, privacy, and security challenges.

Blockchain is a distributed ledger technology that breaks down data into blocks linked together using cryptographic hash functions. It serves as a decentralized record of transactions across a public network, widely adopted across various applications, notably in IoT. The blockchain organization includes smart contract and consensus algorithms for data exchange resulting in less risk of external influence between the involved parties. The consensus mechanism is a fundamental and essential element of blockchain technology, as it evaluates each transaction using a consensus algorithm before recording it in the ledger [10]. The transaction details recorded in the ledger are permanent and cannot be altered or erased once written. A blockchain consists of a sequential chain of blocks, each secured by a hash of the next block [10], [17]. When a new transaction is initiated, a node process it. This node, or block, is then propagated to other nodes where it undergoes verification. Once all nodes validate the transaction, the new block is added to the blockchain ledger, effectively recording the transaction.

In a blockchain, a block comprises several key elements [10]:

- A series of operations with an exchange of values (transactions, that is, the material part of data);
- A timestamp;
- A Merkle tree, also known as a binary hash tree, is utilized to verify the integrity of the block, adding an extra layer of implemented security;
- The identity of each block is determined by the hash of the previous block, establishing its position within the blockchain. This interconnected structure ensures the creation of an unbroken chain of blocks;
- Smart contracts are scripts that enable computer program execution on the blockchain, often incorporating access policies. It is essential to ensure that the blockchain permits the execution of these policies to control access and manage data operations on its blocks.

The advantages of blockchain, particularly in terms of security, can be summarized as follows [17]:

- Decentralization: In blockchain, it means there is no central authority governing the system or dictating policies. Transactions are validated through the consensus of all nodes in the network, rather than relying on a single authoritative figure or a select few;
- Distribution of information: It is noteworthy that each network component maintains a copy of the blockchain, eliminating the need for any node to keep its information confidential;
- Data transparency and auditability: Because the blockchain contains a complete record of every transaction and is accessible to all participants, it enables tracking and monitoring of all transactions to verify the authenticity of activities within the network;
- Robustness: The blockchain is transparent and resistant to manipulation by any group of individuals or organizations.

In this architecture, blockchain serves as the universal ledger ensuring trust in all communication between smart devices. Decentralized IoT offers enhanced security, decentralization, and openness protecting against attacks and vulnerabilities targeting centralized cloud data [18]. Additionally, blockchain facilitates node communication through cryptographic hash functions, making it highly resistant to unauthorized access [10], [17].

Despite its advantages, blockchain encounters several challenges, including high energy consumption, scalability issues, slower data transactions, lack of standardization, limited storage capacity, and computational constraints [10], [17]. The computational expense and energy intensity of block mining are significant drawbacks. Moreover, storing data on IoT nodes demands substantial storage and computational resources. Security concerns such as DoS attacks and maintaining trust among nodes also pose challenges. Ghorbani, Mohammadzadeh, and Ahmadzadegan [15] emphasize the critical need to enhance IoT device security, particularly in authentication to network base stations. Utilizing technologies like machine learning and blockchain can strengthen authentication processes and enhance network monitoring capabilities.

5. DISCUSSION

Most previous reviews have focused on either privacy and security concerns, technological drivers enabling 5G-IoT layers, requirements for 5G-enabled IoT, or the challenges, prospects, and opportunities of 5G-IoT.

The security challenges in 5G include: rapid network traffic fluctuations, security risks from radio interference, user plane integrity, mandatory network security measures, infrastructure Denial of Service (DoS) attacks, signaling storms, and DoS attacks targeting end-user devices.

From the literature reviewed, it is evident that while some studies have outlined the challenges and potential of 5G-IoT technology, there is a scarcity of comprehensive discussions on current technical issues [6], [17]. Sicari, Rizzardi, and Coen-Porisin [17] highlight various challenges including security, privacy, data management, rogue node detection, and trust establishment in 5G-enabled IoT systems. However, there remains insufficient investigation into integrating

standardization into these protocols or leveraging existing tools and techniques to effectively address these security concerns.

Security and privacy issues are paramount concerns in developing IoT devices and solutions [6]. The concept of 'Security by Design', advocated by contemporary government practices, aims to fortify the IoT as a robust and scalable network. This approach includes measures such as identification, authentication, assumed network connectivity, and considerations for potential interception of communications. Given the layers of network architecture in 5G, all layers must incorporate robust security services. Key considerations in securing IoT networks include device identification and deployment strategies. However, deploying existing internet security mechanisms on Machine Type Communication (MTC) devices, which may lack processing power for heavy tasks, poses a significant challenge.

Key security parameters in modern mobile networks include authentication to guarantee data integrity, ensuring service availability, and maintaining confidentiality. With the advent of critical applications leveraging 5G, privacy becomes paramount, necessitating architectural considerations such as observability, unlinkability, anonymity, and pseudonymity, as suggested by [19], [20]. These measures enhance subscriber identity protection and add an additional layer of security.

Addressing these concerns requires establishing effective and adaptable measures, standards, and protocols capable of evolving to combat emerging threats [6]. Collaboration among industry stakeholders, standards bodies, and governmental and non-governmental regulators is crucial to integrating safety and security features into the design of 5G networks. This collaborative effort is essential to create a stable and resilient 5G network infrastructure that supports the next generation of IoT-enabled connectivity without compromising user privacy and security.

The coverage area has a high density of devices with high mobility, which is unlike traditional networks. While new 5G networks offer higher speeds than their predecessors, covering large areas remains a challenge. Additionally, 5G-IoT devices require longer battery life, because 5G consumes more power than previous generations, leading to power-related issues for IoT devices and the need for backup batteries in smart devices [6].

6. CONCLUSION

We have seen that most previous reviews have focused on various aspects of 5G-IoT integration, such as privacy and security concerns, technological enablers, and the challenges and opportunities presented by this technology. Key security challenges in 5G include network traffic fluctuations, radio interference risks, user plane integrity, mandatory security measures, infrastructure Denial of Service (DoS) attacks, signaling storms, and end-user device DoS attacks. While some studies have highlighted the challenges and potential of 5G-IoT, there is a lack of comprehensive discussions on current technical issues and the integration of standardization into security protocols.

The concept of "Security by Design" aims to create robust and scalable IoT networks by incorporating measures like identification, authentication, and communication interception

considerations. Given the complex 5G network architecture, robust security must be integrated at all layers, including device identification and deployment strategies. However, existing internet security mechanisms are often too resource-intensive for Machine Type Communication (MTC) devices with limited processing power.

Modern mobile network security parameters, such as authentication, service availability, and confidentiality, are crucial, especially with critical applications leveraging 5G. Privacy considerations like observability, unlinkability, anonymity, and pseudonymity are essential to enhance subscriber identity protection. Addressing these concerns requires establishing adaptable measures, standards, and protocols capable of evolving to combat emerging threats. Collaboration among industry stakeholders, standards bodies, and regulators is vital to integrating safety and security features into 5G network designs.

5G networks face additional challenges, such as covering large areas with high device density and mobility, and addressing the higher power consumption of 5G devices, which necessitates longer battery life and backup solutions for IoT devices. Effective collaboration is crucial to create a stable and resilient 5G infrastructure that supports the next generation of IoT-enabled connectivity without compromising user privacy and security.

We believe that with this work we have shed some light on how 5G and IoT are related in terms of remote services, security on mobile devices, and connectivity.

ACKNOWLEDGMENTS

The study was developed under the project A-MoVeR – "Mobilizing Agenda for the Development of Products & Systems towards an Intelligent and Green Mobility", operation n.º 02/C05-i01.01/2022.PC646908627-00000069, approved under the terms of the call n.º 02/C05-i01/2022 – Mobilizing Agendas for Business Innovation, financed by European funds provided to Portugal by the Recovery and Resilience Plan (RRP), in the scope of the European Recovery and Resilience Facility (RRF), framed in the Next Generation UE, for the period from 2021 - 2026, and under the Institute of Electronics and Informatics Engineering of Aveiro (IEETA) Research Unit, funded by National Funds through the FCT – Foundation for Science and Technology, in the context of the project UIDB/00127/2020.

WORKS CITED

G. A. Macriga, S. S. Sakthy, R. Niranjan, and S. Sahu, "An emerging technology: Integrating IoT with 5G cellular network," in 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021, pp. 208–214.

I. Zhou, I. Makhdoom, N. Shariati, M. A. Raza, R. Keshavarz, J. Lipman, M. Abolhasan, and A. Jamalipour, "Internet of things 2.0: Concepts, applications, and future directions," IEEE Access, vol. 9, pp. 70 961–71 012, 2021.

H. Rahimi, A. Zibaeenejad, and A. A. Safavi, "A novel IoT architecture based on 5G-IoT and next generation technologies," in 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 81–88.

M. M. Alsulami and N. Akkari, "The role of 5G wireless networks in the internet-of-things (IoT)," in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, pp. 1–8.

L. Chettri and R. Bera, “A comprehensive survey on internet of things (IoT) toward 5G wireless systems,” IEEE Internet of Things Journal, vol. 7, no. 1, pp. 16–32, 2020.
S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, S. B. Taher, M. Kabir, S. M. Muyeen, and A. H. Gandomi, “Toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities,” IEEE Access, vol. 12, pp. 13 125–13 145, 2024.
M. Fodor and P. Viktor, “IoT devices and 5G network security option from generation aspects,” in 2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC), 2022, pp. 000 265–000 270.
S. Wijethilaka and M. Liyanage, “Survey on network slicing for internet of things realization in 5G networks,” IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 957–994, 2021.
A. Mir, M. F. Zuhairi, S. Musa, T. A. Syed, and A. Alrehaili, “Poster: A survey of security challenges with 5G-IoT,” in 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), 2020, pp. 249–250.
R. M. Haris and S. Al-Maadeed, “Integrating blockchain technology in 5G enabled IoT: A review,” in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 367–371.
L. Tello-Oquendo, S.-C. Lin, I. F. Akyildiz, and V. Pla, “Software-defined architecture for QoS-aware IoT deployments in 5G systems,” Ad Hoc Networks, vol. 93, p. 101911, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518309016
A. Eid, J. Hester, and M. M. Tentzeris, “A scalable high-gain and large-beamwidth mm-wave harvesting approach for 5G-powered IoT,” in 2019 IEEE MTT-S International Microwave Symposium (IMS), 2019, pp. 1309–1312.
A. M. Escolar, J. M. A. Calero, and Q. Wang, “Highly-scalable software firewall supporting one million rules for 5G NB-IoT networks,” in ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6.
G. Su and M. Moh, “Improving energy efficiency and scalability for IoT communications in 5G networks,” in Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication, ser. IMCOM ’18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3164541.3164547
H. Ghorbani, M. S. Mohammadzadeh, and M. H. Ahmadzadegan, “DDoS attacks on the IoT network with the emergence of 5G,” in 2020 International Conference on Technology and Entrepreneurship – Virtual (ICTE-V), 2020, pp. 1–5.
A. Agrawal and P. Baniya, “The internet of things: Security challenges and opportunities,” 04 2024.
S. Sicari, A. Rizzardi, and A. Coen-Porisini, “5G in the internet of things era: An overview on security and privacy challenges,” Computer Networks, vol. 179, p. 107345, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620300827
D.-R. Berte, “Defining the IoT,” Proceedings of the International Conference on Business Excellence, vol. 12, no. 1, pp. 118–128, 2018. [Online]. Available: https://doi.org/10.2478/picbe-2018-0013
N. A. Anagnostopoulos, S. Ahmad, T. Arul, D. Steinmetzer, M. Hollick, and S. Katzenbeisser, “Low-cost security for next-generation IoT networks,” ACM Trans. Internet Technol., vol. 20, no. 3, sep 2020. [Online]. Available: https://doi.org/10.1145/3406280
X. Ge, R. Zhou, and Q. Li, “5G NFV-based tactile internet for mission-critical IoT services,” IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6150–6163, 2020.