Review

Systematic Literature Review on 5G-IoT Security Aspects

Dalton Valadares *, Newton Will, Álvaro Sobrinho, Anna Lima, Igor Morais, Danilo Santos

Posted Date: 8 November 2023

doi: 10.20944/preprints202311.0565.v1

Keywords: Internet of Things; 5G Networks; threats; vulnerabilities; mitigations

Article

Systematic Literature Review on 5G-IoT Security Aspects

Dalton Cézane Gomes Valadares[1,2]*, Newton Carlos Will[3], Álvaro Alvares de Carvalho César Sobrinho[4], Anna C. D. de Lima[1], Igor S. de Morais[1] and Danilo Freire de Souza Santos[1]

[1] Federal University of Campina Grande - VIRTUS RDI Center/Embedded Lab, Campina Grande, Paraíba, Brazil; anna.lima@embedded.ufcg.edu.br; igor.morais@embedded.ufcg.edu.br; danilo.santos@virtus.ufcg.edu.brm
[2] Federal Institute of Pernambuco, Caruaru, Pernambuco, Brazil
[3] Federal University of Technology - Paraná, Dois Vizinhos, Paraná, Brazil; will@utfpr.edu.br
[4] Federal University of Agreste of Pernambuco, Garanhuns, Pernambuco, Brazil; alvaro.alvares@ufape.edu.br
* Correspondence: dalton.valadares@embedded.ufcg.edu.br

Abstract: The 5G technology brings many benefits already known: large connection capacity, great transmission velocities, and low latencies with high reliability. One of its core services, the massive Machine Type Communication (mMTC), theoretically allows up to one million devices connected simultaneously in a square kilometer. As the Internet of Things (IoT) devices often have very restricted resources, hampering the adoption of robust security mechanisms, they can be targets for attackers aiming to explore vulnerabilities and gain access to the 5G infrastructure. Given this concern, it is essential to know existent vulnerabilities and possible threats and solutions related to 5G-IoT, the scenarios considering IoT devices connected to 5G infrastructures. For this reason, we carried out a systematic literature review, extracting and analyzing data from 142 selected papers from conferences and journals. As the main results, we present lists with known vulnerabilities, possible threats and solutions, and some recommendations.

Keywords: Internet of Things; 5G Networks; threats; vulnerabilities; mitigations

1. Introduction

One of the pillars of the new services offered by 5G technology is the massive Machine Type Communication (mMTC) [1], which is based on the Low-Power Wide Area Network (LP-WAN) communication standard, suitable for long-distance communication of small amounts of data with energy saving [2]. The mMTC will enable the connection of a large number of devices to the 5G infrastructure, reaching 1 million devices per square kilometer [2], which will favor the deployment of Internet of Things (IoT) services and applications.

IoT applications generally present heterogeneity regarding the different devices, often from different manufacturers and communication technologies. In addition, such applications can also be dynamic when considering the number and status of connected devices. These characteristics allow different combinations of scenarios, which, together with the limitations of computational resources inherent to devices, become attractive for attackers who seek and exploit vulnerabilities. Thus, IoT data can be targets for possible attacks, independently whether they are in devices, transit, or stored in remote servers, such as in the cloud, fog, and edge computing.

Cloud-centric models are more vulnerable to IoT security and privacy due to more user data in the cloud layer accessed by different entities [3]. Considering edge computing, the IoT gateway contains more data than an IoT end device, making it more vulnerable. Besides, a mobile device is at risk when used as a data collection or analysis tool because accessing insecure data sources can make the device vulnerable. An HP report found that 70% of devices have vulnerabilities, and that number reaches 100% when considering the scenario of smart homes [4].

Although many scientific papers and technical reports have addressed security issues, challenges, and recommendations in 5G and IoT environments [5], the lack of security standardization is still a concern [6–10]. Given the different security concerns regarding IoT devices connected in 5G infrastructures, it is important to know the vulnerabilities and threats in these scenarios, as well as possible solutions to mitigate them.

In this sense, considering the context of 5G-IoT, we performed a systematic literature review to investigate what are the known vulnerabilities, what are the possible threats/attacks, and what can be applied to mitigate them. A systematic literature review aims to identify, evaluate, and interpret all available research relevant to a topic of interest, helping to identify gaps in current research, suggest areas for further investigation, and position new research activities. The main advantage of the systematic literature review is the use of a well-defined

 doi:10.20944/preprints202311.0565.v1

methodology that, despite demanding considerably more effort, makes it less likely that the literature results are biased [11].

To perform an SLR, we first must define a protocol considering a specified problem/scenario, the research questions, the inclusion and exclusion criteria, the search string, scientific repositories, the data collection methodology, and the quality assessment method. Thus, following the systematic literature review protocol we defined, after the search and selection phase, we considered 142 papers published in journals and conferences. As a result, we start presenting general information regarding the quantitative analyses of the extracted data. Then, we present the list of vulnerabilities classified into five classes, the main threats to consider, and possible solutions to adopt. Finally, we present some general recommendations related to 5G-IoT security.

The main contributions of this article are:

- we elaborated the SLR protocol, which can be used to replicate or update this study in the future;
- we selected and reviewed 142 papers considering they explore security threats, vulnerabilities, or solutions for 5G-IoT environments;
- we analyzed and presented the information extracted from the selected papers, classifying threats, vulnerabilities, and solutions;
- we present the state-of-the-art related to security issues in 5G-IoT scenarios.

The remainder of this paper is organized as follows: we present the research protocol for the SLR in Section 2; in Section 3, we show the general results from the collected data, considering quantitative information; in Section 4, we describe the threat model applied to our study; in Section 5, we list all the vulnerabilities found in the selected papers; in Section 6, we present all the threats discussed in the selected papers; in Section 7, we describe what security solutions were considered in the relevant works; we present general recommendations in Section 8 and the related work in Section 9; we conclude this work in Section 10.

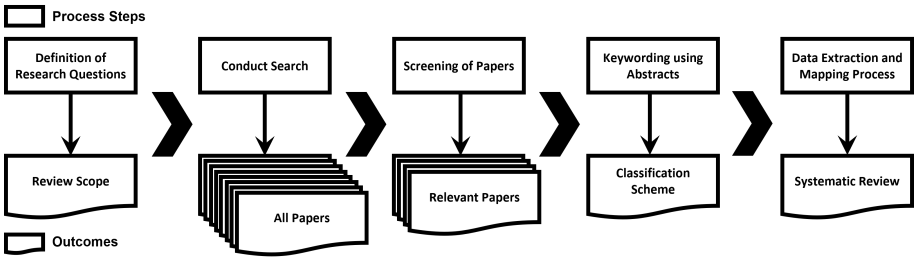

Figure 1. Systematic review process.

2. Research Protocol

To conduct our review, we applied the five steps described by [12], where each process steps has an outcome, as shown in Figure 1. All these steps and their outcomes are detailed in the following sections.

2.1. Research Questions

Research questions must incorporate the purpose of the review performed. The main goal of this review is to investigate threats, vulnerabilities, and possible solutions to mitigate them in Internet of Things applications and services with 5G communication infrastructure. Thus, we defined the following research questions:

- **RQ1:** What are the known vulnerabilities in the 5G-IoT context? *Rationale:* This question seeks to identify the vulnerabilities listed in the literature in the context of 5G-IoT applications.
- **RQ2:** What are the known threats in the 5G-IoT context? *Rationale:* We seek to classify the known threats in the 5G-IoT context and understand how they affect these environments.
- **RQ3:** What are the recommendations and proposed solutions to mitigate the vulnerabilities and threats listed in the literature? *Rationale:* This question aims to present the recommendations and proposed solutions to mitigate the known vulnerabilities and threats in IoT and 5G environments and the best practices to build secure applications in these contexts.

2.2. Search Strategy

We specified the following terms as keywords for the research: 5G, Internet of Things, and security. Then, we applied alternative terms and terms defined by the PICO approach (Population, Intervention, Context, and Outcome), as shown in Table 1.

 doi:10.20944/preprints202311.0565.v1

Table 1. Keywords and PICO terms.

Population	Internet of Things, Internet of Everything, IoT, IoE
Intervention	threat, vulnerability, solution
Context	5G
Outcome	security, privacy, confidentiality, integrity, trustworthiness, protection

For the term solution, we also considered the following words: architecture, framework, platform, and system.

2.3. Search String

With the keywords, alternative terms, and terms defined with the PICO approach, we defined the following search string using the boolean operators AND/OR to link the terms:

("Internet of Everything" **OR** "Internet of Things" **OR** "IoE" **OR** "IoT")
AND
("Solution" **OR** "Architecture" **OR** "Framework" **OR** "Platform" **OR** "System" **OR** "Threat" **OR** "Vulnerability")
AND
("Confidentiality" **OR** "Integrity" **OR** "Privacy" **OR** "Protection" **OR** "Security" **OR** "Trustworthiness")
AND
("5G")

2.4. Search Repositories

To search for relevant articles, we used the six scientific repositories listed in Table 2, which gather articles from different conferences and journals.

Table 2. Selected scientific repositories.

Scientific Repository	URL
ACM Digital Library	http://dl.acm.org
El Compendex	http://www.engineeringvillage.com
IEEE Digital Library	http://ieeexplore.ieee.org
Wiley Online Library	http://onlinelibrary.wiley.com
Scopus	http://www.scopus.com
Springer Link	http://link.springer.com

2.5. Selection Criteria

In order to avoid results that do not help to answer the research questions and improve the probability of selecting relevant articles to answer the research questions, we defined the following inclusion criteria:

- **IC1:** Papers that present vulnerabilities in 5G-IoT context;
- **IC2:** Papers that present threats in 5G-IoT context;
- **IC3:** Papers that present solutions to mitigate vulnerabilities and threats in 5G-IoT context;
- **IC4:** Papers that present recommendations to improve the security of applications in 5G-IoT contexts;
- **IC5:** When several papers show similar studies, only the most recent is included;
- **IC6:** If there are versions of the same paper, the most complete must be included.

Exclusion criteria are important, as they allow greater precision in eliminating studies not relevant to the context of the review. For this reason, during the individual analysis of the studies, we discarded all those that met at least one of the following exclusion criteria:

- **EC1:** Posters, short articles, and expanded abstracts (articles with less than three pages);
- **EC2:** Book chapters;

 doi:10.20944/preprints202311.0565.v1

- **EC3:** Articles not written in English;
- **EC4:** Articles that do not focus on security;
- **EC5:** Duplicate results;
- **EC6:** Articles published before the year 2010 (beginning of work for 5G development).

We did not remove secondary studies because some of them propose specific solutions (e.g., [13]), in addition to summarizing and analyzing the state-of-the-art. The secondary studies are also relevant sources for identifying vulnerabilities and threats regarding 5G-IoT.

2.6. Selection Procedure

To carry out the selection of relevant articles, we used the selection criteria according to the following steps:

- Delete duplicate documents;
- Exclude documents published before the year 2010 or documents not written in English;
- Exclude documents not published in journals or conferences;
- Exclude dissertations and theses, expanded abstracts, summary articles, and posters;
- Exclude irrelevant documents, i.e., documents that do not help to answer the research questions.

To exclude irrelevant documents, we analyzed each article resulting from the search by two reviewers according to the following criteria:

- Each reviewer classifies the document as relevant, irrelevant, or undefined;
- Documents classified as relevant by two reviewers are kept;
- Documents classified as irrelevant by two reviewers are excluded;
- Documents classified as undefined by two reviewers are better analyzed through a quick reading of the complete document, and then they are reclassified as relevant or irrelevant;
- Documents classified as relevant or undefined by one reviewer and irrelevant by another are discussed between both until they reach a consensus on one of the previous classifications.

2.7. Quality Assessment

The paper quality assessment aims to provide more detailed criteria for the inclusion and exclusion of candidate papers and to investigate whether quality differences impact on different results in the studies [14]. To assess the quality of the selected documents, we established the following questions:

1. Is the text well organized and clear (easy to understand)?
2. Are motivation and goals well described?
3. Is the methodology clear (easy to understand and replicate)?
4. Is the document well-referenced, and does it present good related work?
5. Does the document present threats, vulnerabilities, or solutions?
6. Do the authors present a good discussion of the topics covered in the document?
7. Are there any suggestions for future work?

For each article selected, reviewers answer each of the seven questions with possible answers: yes, moderated, or no. Each answer receives a score as described below:

- Yes 1;
- Moderate - 0.5;
- No - 0.

Thus, as there are seven questions, the maximum score for each article is seven, and the minimum is 0, indicating an article's best and worst quality. Depending on the score, we classified the quality level as follows:

- High quality, if the score is 5.5 or higher;
- Medium quality, if the score is between 3.5 and 5.5;
- Low quality if the score is less than or equal to 3.5.

 doi:10.20944/preprints202311.0565.v1

2.8. Data Extraction

The following list contains the data we extracted from the relevant articles:

- Title
- Authors
- Abstract
- Year
- Article type
- Name of Conference/Journal
- Country(s) where the research was performed
- Number of pages
- Number of citations
- Quality
- List of threats
- List of vulnerabilities
- List of solutions
- List of essential definitions/terms

3. General Results

Figure 2 presents an overview of the SLR results. We reviewed 3,012 papers by reading titles and abstracts in the first filtering step. By applying the selection criteria, we rejected 2,015 papers and accepted 159 papers. The remaining papers were automatically removed due to duplication. Afterward, by the full paper reading, we rejected 17 papers and conducted data extraction and quality assessment of 142 papers. As presented in Figure 3, 99 works were published in journals, and 43 were published in conferences.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

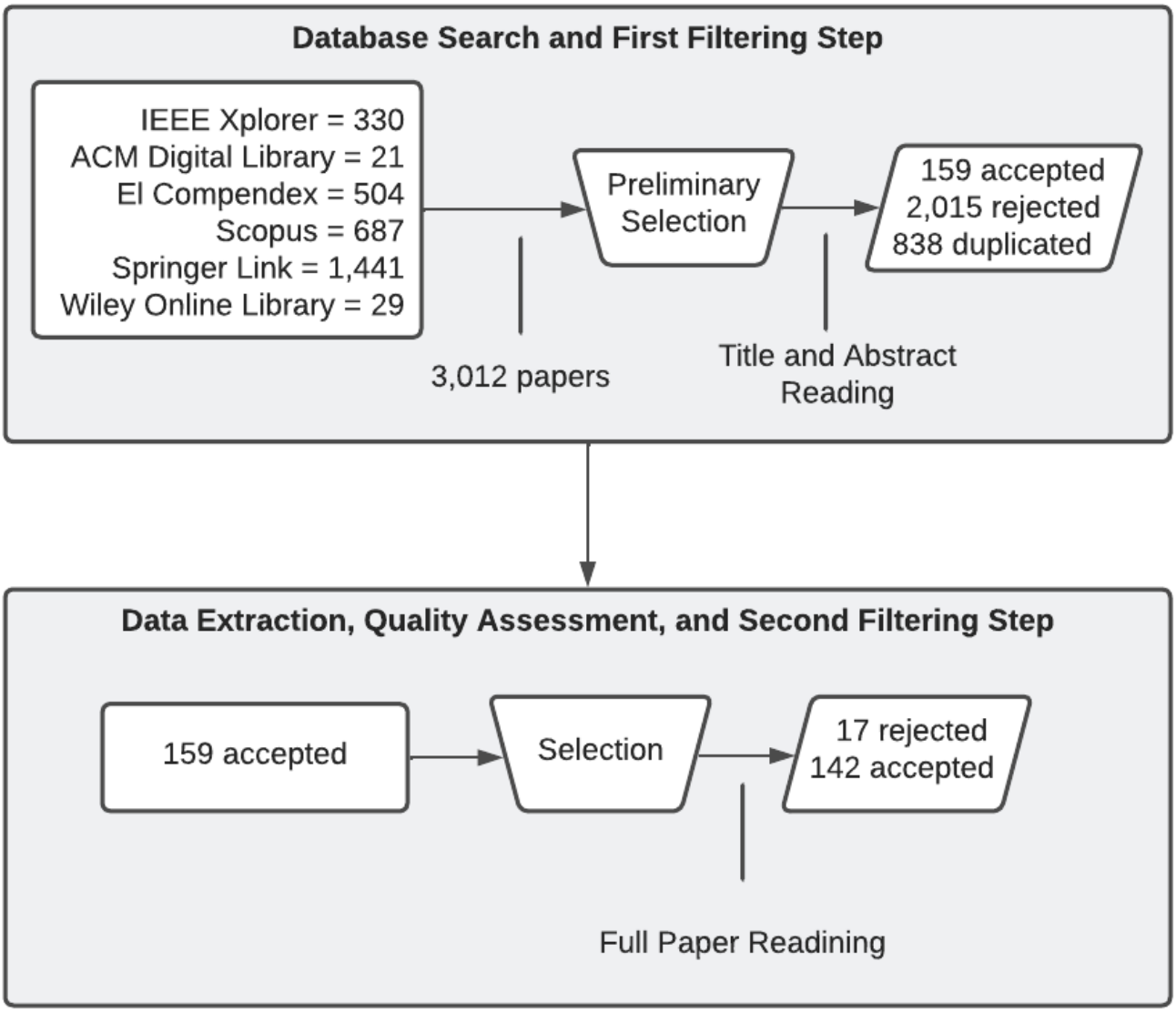

Figure 2. Overview of the SLR results.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

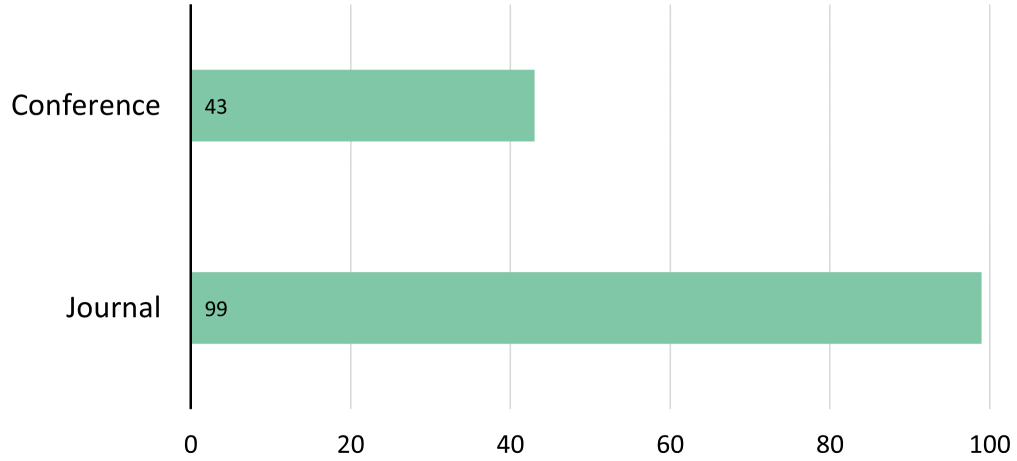

Figure 3. Number of selected papers by publication type.

Figure 4 presents a heatmap representing the distribution of publications by the authors' country of the 142 accepted papers. We considered the country of all authors of the papers. For instance, a paper with four authors from China and one from India increased the total number of counts for both countries. Researchers from China and India more frequently authored papers, appearing 110 and 83 times, respectively. This information indicates the current high research interest of such countries in 5G-IoT security.

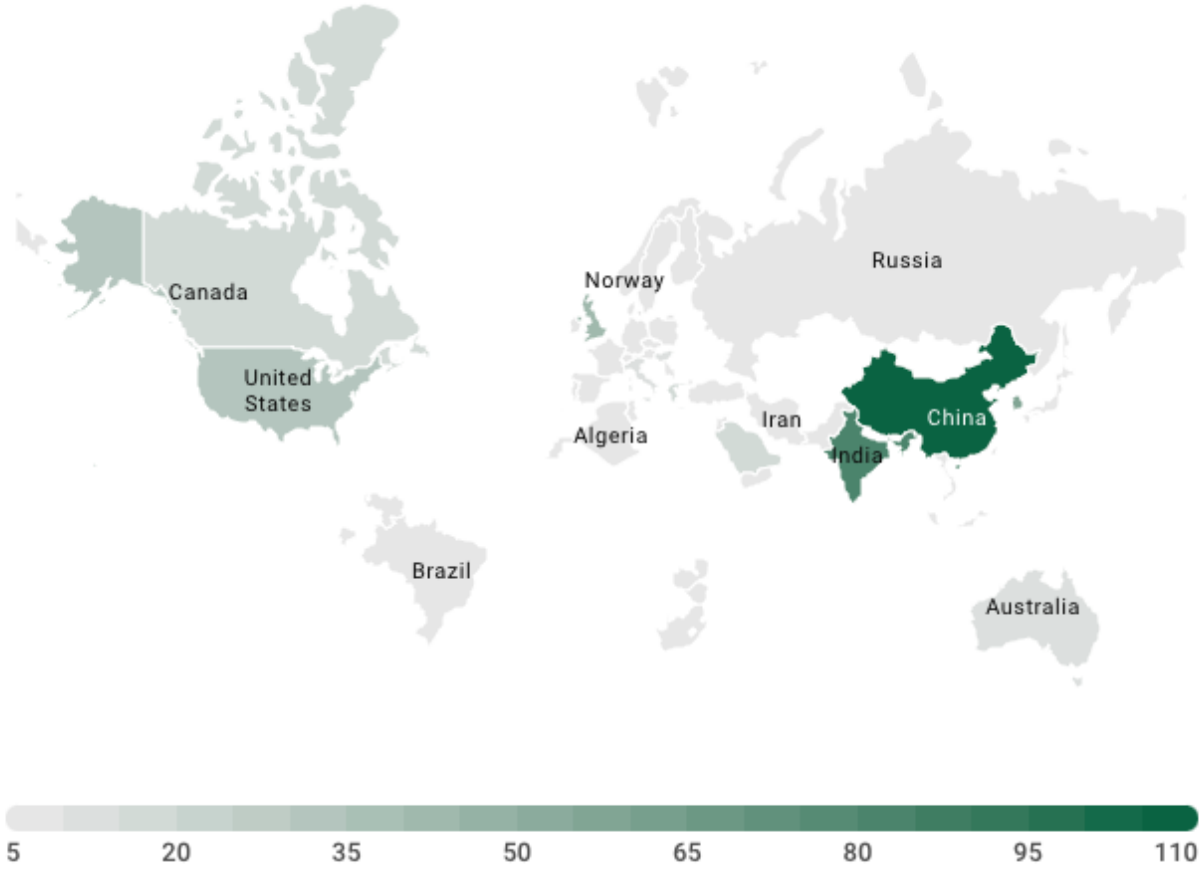

Figure 4. Heatmap for the distribution of authors per country.

 doi:10.20944/preprints202311.0565.v1

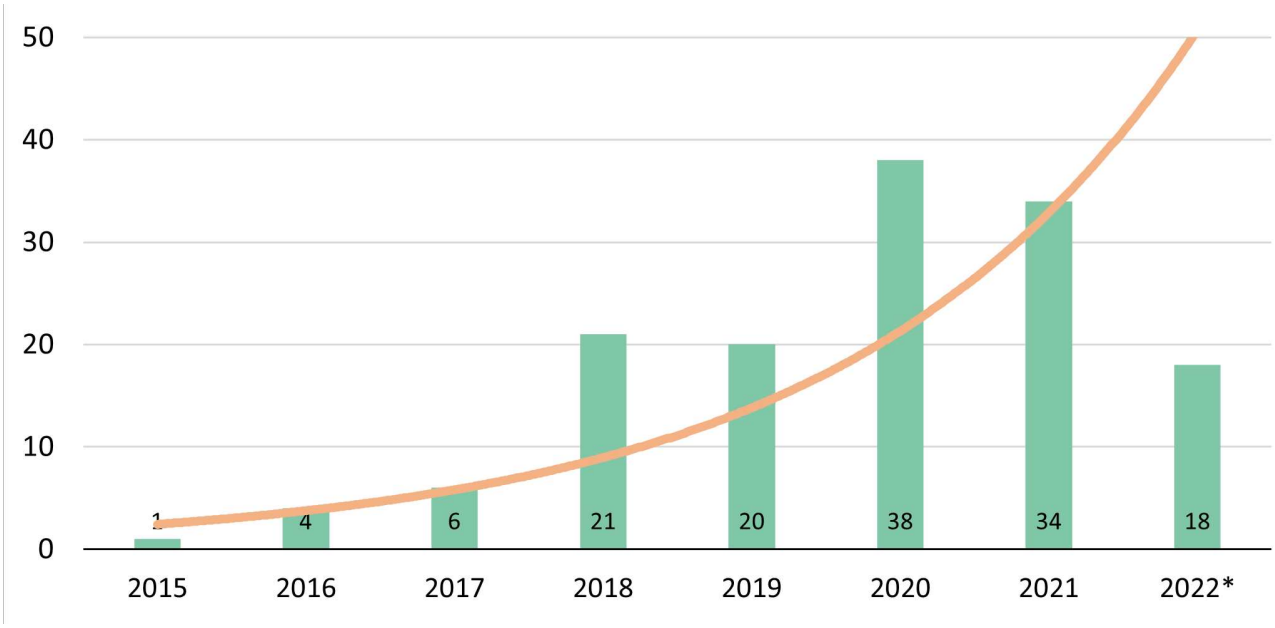

Figure 5. Number of selected papers per year.

When we analyze the number of publications per year, we can see that the studies regarding the 5G-IoT context increased, as shown in Figure 5. It is important to note that the year 2022 may not include the totality of papers since the search in the digital repositories was carried out in May 2022.

Another relevant piece of information is the number of citations for selected papers. Figure 6 illustrates the number of citations for selected papers from Google Scholar in February 2023. Most papers were cited by at most 21 other documents, and only 10 of the 142 papers were cited more than 99 times.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

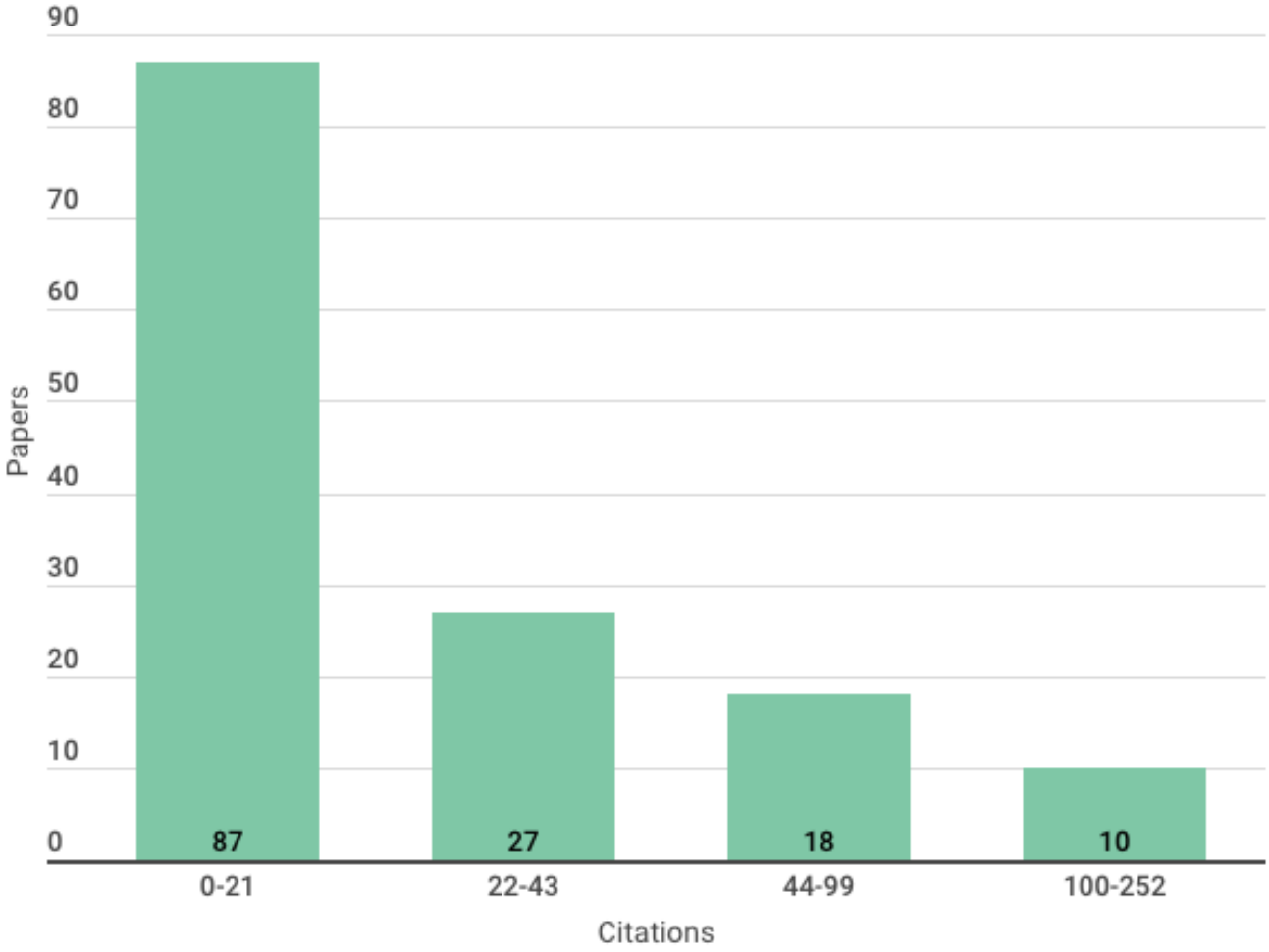

Figure 6. Number of citations for selected papers.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

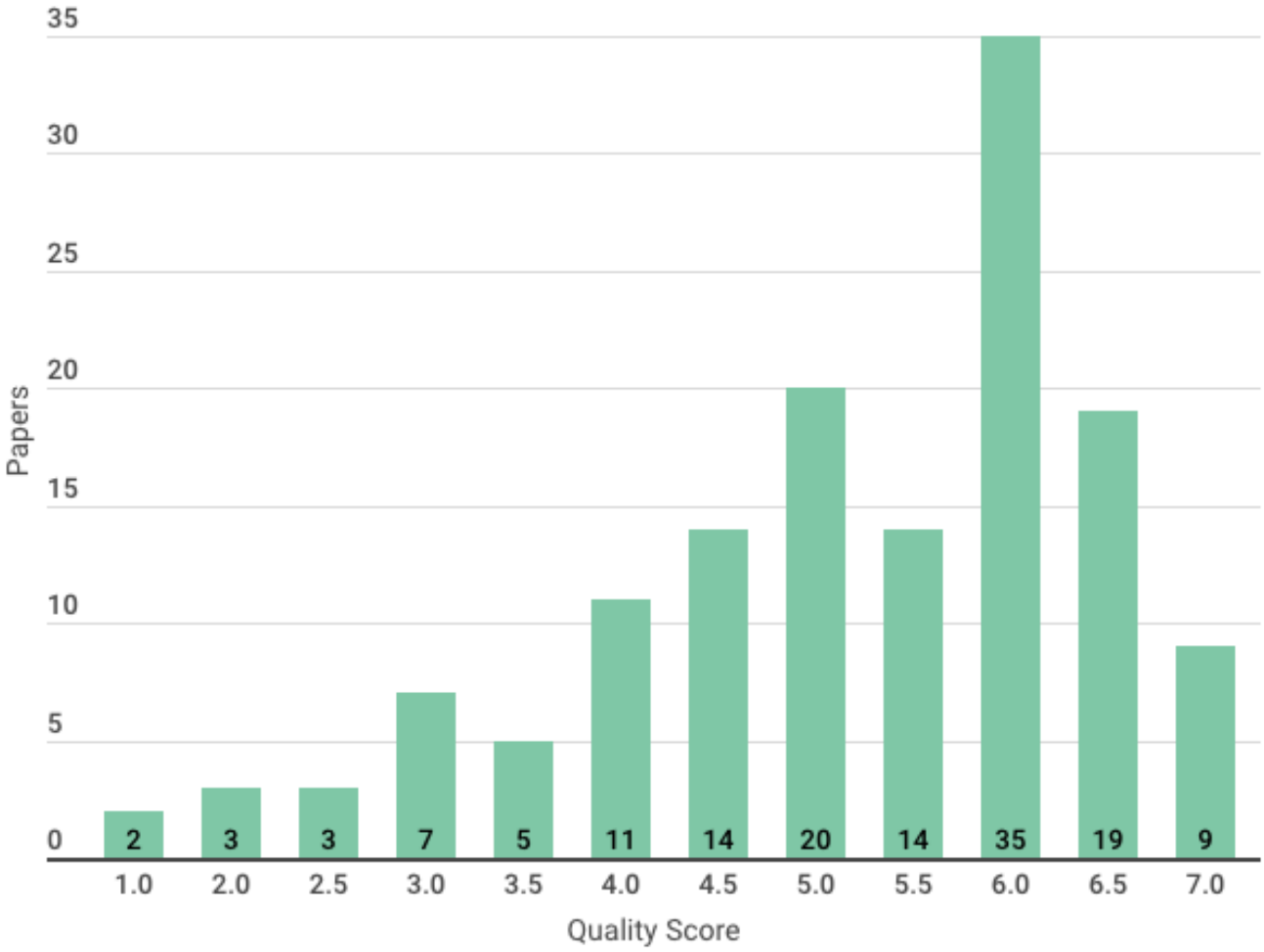

Figure 7. Quality assessment score for selected papers.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

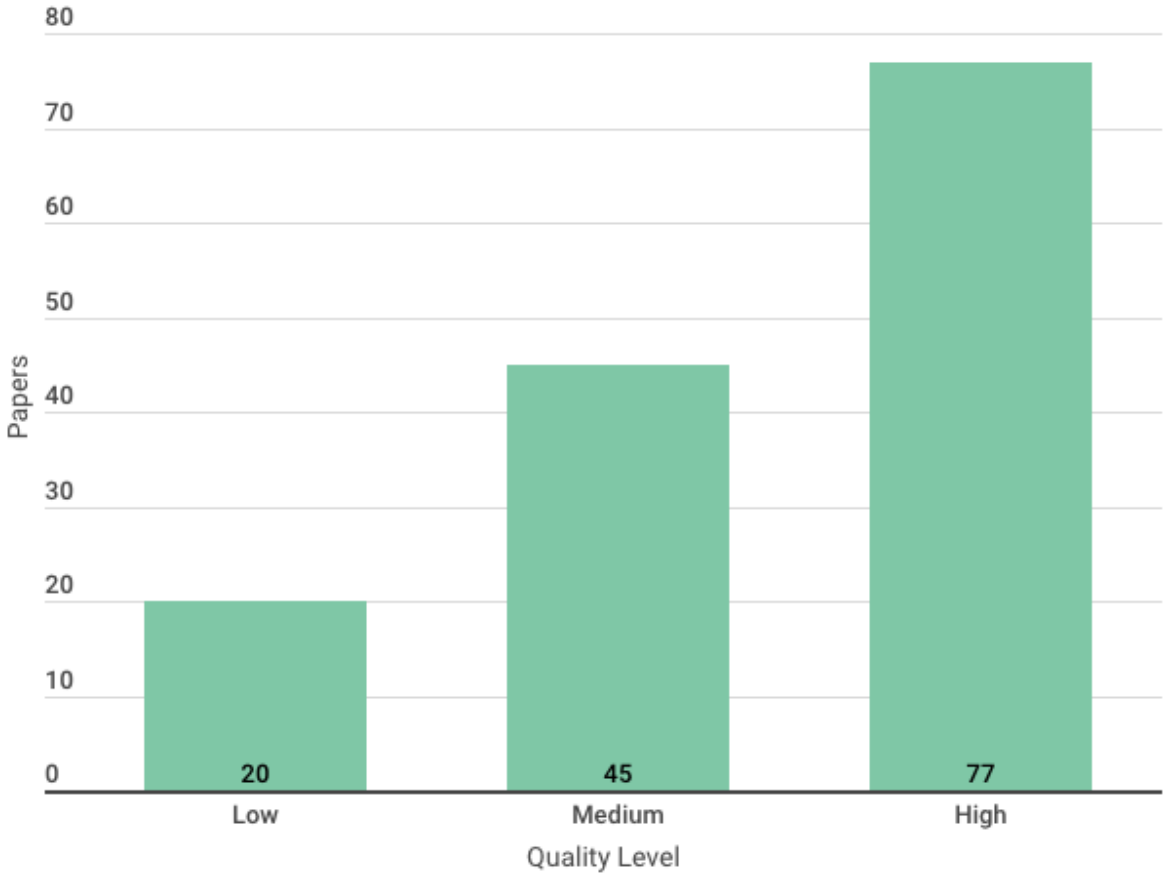

Figure 8. Quality levels for selected papers.

Finally, Figure 7 presents the quality assessment score for selected papers. Our quality assessment score ranges from 0.0 to 7.0 points. Most papers achieved an assessment score of 6.0 points. Besides, Figure 8 presents the quality levels for the 142 papers. Therefore, most papers achieved a high-quality level. Only 14.08% of the selected papers presented low quality according to our classification (i.e., $score \leq 3.5$). The 85.92% of medium or high-quality classifications evidence the relevance of the papers included in this revision.

4. Threat Model

Although there is no single universally accepted IoT architecture, the most basic and most widely accepted one considers three layers, as described in Figure 9. The three-layer approach was proposed in the early stages of the Internet of Things research and fulfills the basic idea of IoT [15]. In this paper, we use this architecture to analyze the threats in the 5G-IoT environment, and each of these layers has specific security challenges [16].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

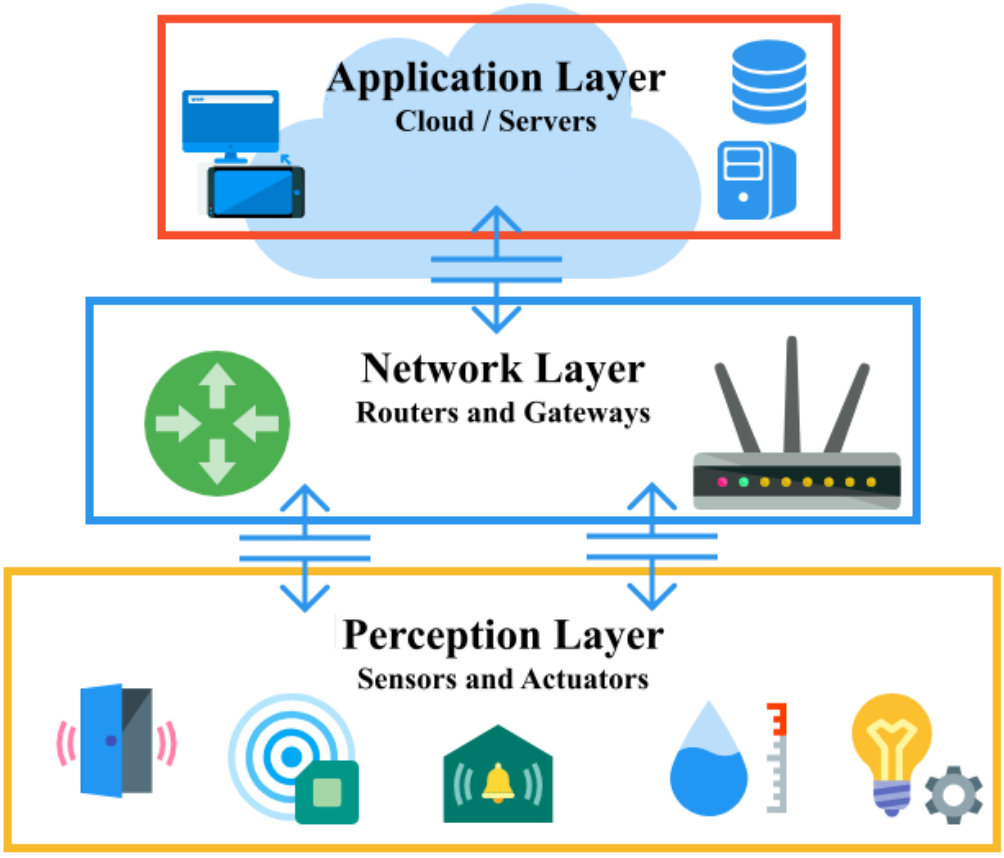

Figure 9. Three layer IoT architecture.

The perception layer, also known as the sensors layer, is where the sensors and connected devices are and is responsible for collecting various amounts of data. Due to its importance in the IoT environment, this layer is the main target of attackers that aim to replace the devices with their own, collect sensitive data from the system or the user, or even generate fake data to be sent to the server.

The network or transmission layer connects the sensor to other devices, gateways, and servers. It is responsible for transmitting all the data and acts as a bridge between the perception and application layers. This layer is sensitive to attacks that target the service availability, and data integrity and confidentiality.

The third layer, named application layer, delivers application-specific services to the user. These services may vary depending on the data collected by the sensors and the application goal. This layer introduces inside and outside threats, and its security is a key issue.

Considering the three-layer architecture, we defined the threat model shown in Figure 10, considering the possible attack surfaces in IoT applications with 5G infrastructure. The defined threat model considers six attack surfaces, as follows.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

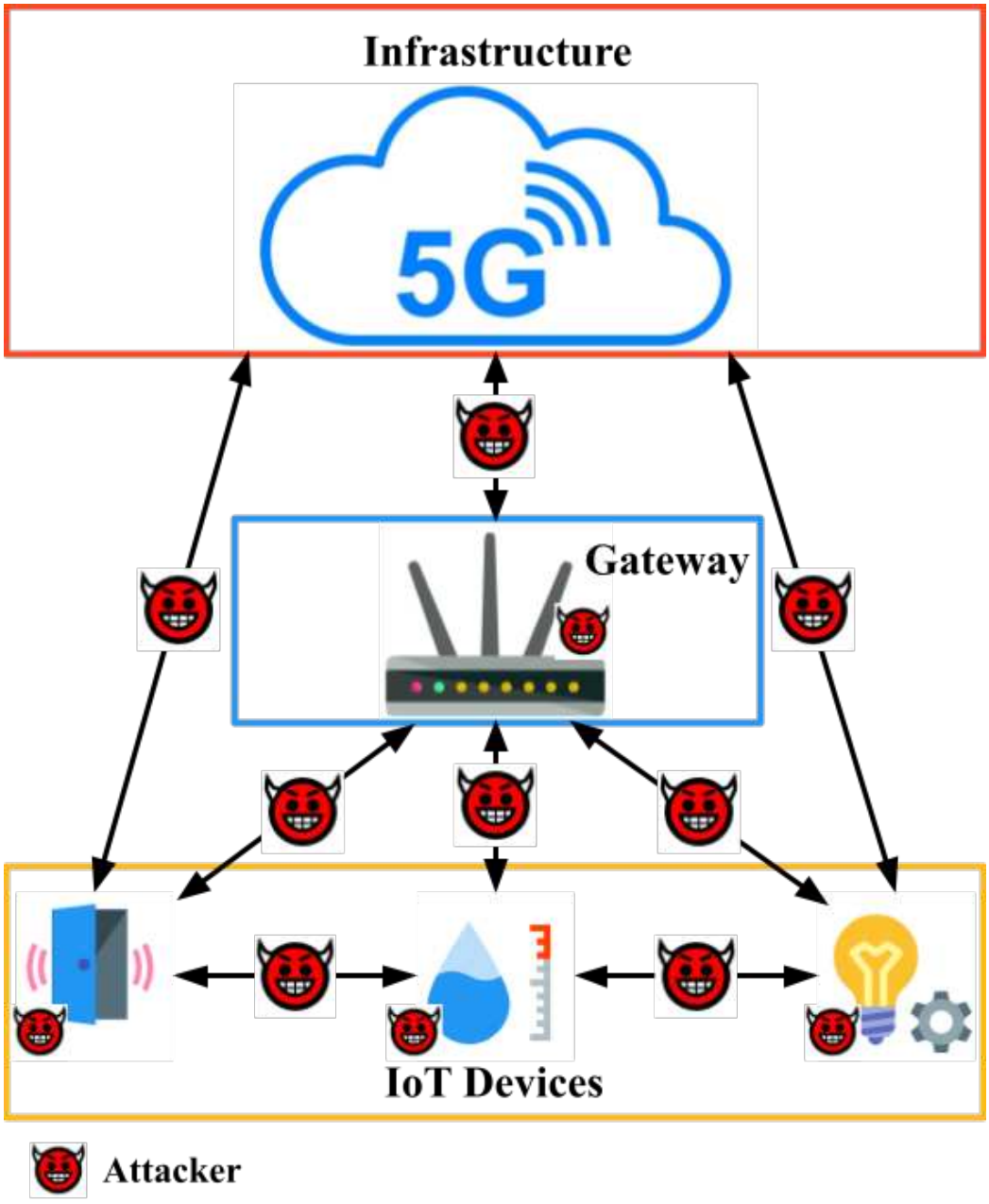

Figure 10. The considered threat model.

- **Device:** Each device can be targeted by attackers and, when compromised, allows communication with the 5G infrastructure or gateways, expanding the attack surface to other targets. The attacker can co-opt the device into a botnet frequently used for DDoS attacks. The captured device can also be used to listen to communication, extract sensitive information from the system, or even send fake data.
- **Gateway:** Gateways concentrate communication in IoT systems, enabling communication with devices and the 5G infrastructure. If an attacker takes control of the gateway, all the devices connected to it can be targeted to be co-opted. The gateway can also become unavailable due to a successful attack, and the devices connected to it will be unreachable. Finally, since gateways serve as an aggregation point in IoT systems, sensitive information can be leaked or even manipulated by the attacker.
- **Communication Between Device and Gateway:** Since IoT devices have computational constraints, the communication between devices and gateways can be targeted by eavesdroppers, who can steal sensitive

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

data. Even when using encryption, the attacker can derive the original data by collecting enough encrypted data in transmission [17].

- **Communication Between Gateway and Infrastructure:** Attackers can exploit the communication channel between gateways and the 5G infrastructure.
- **Communication Between Device and Infrastructure:** Attackers can exploit the communication channel between the devices and the 5G infrastructure in the case of direct connection of the devices (e.g., using the 5G mMTC).
- **Device-to-Device Communication:** An important feature in 5G is the Device-to-Device (D2D) communication, which increases network coverage by enabling direct communication between devices without traversing the core network. This feature opens the door to propagating attacks in a multi-hop scenario, i.e., hop by hop to reach a vulnerable device. Using a compromised device, the attacker can access critical parts of the infrastructure [18].

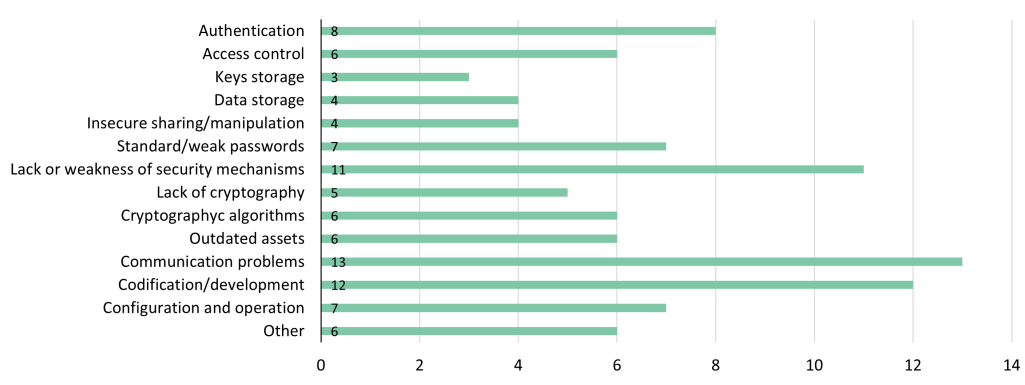

Figure 11. Main vulnerabilities

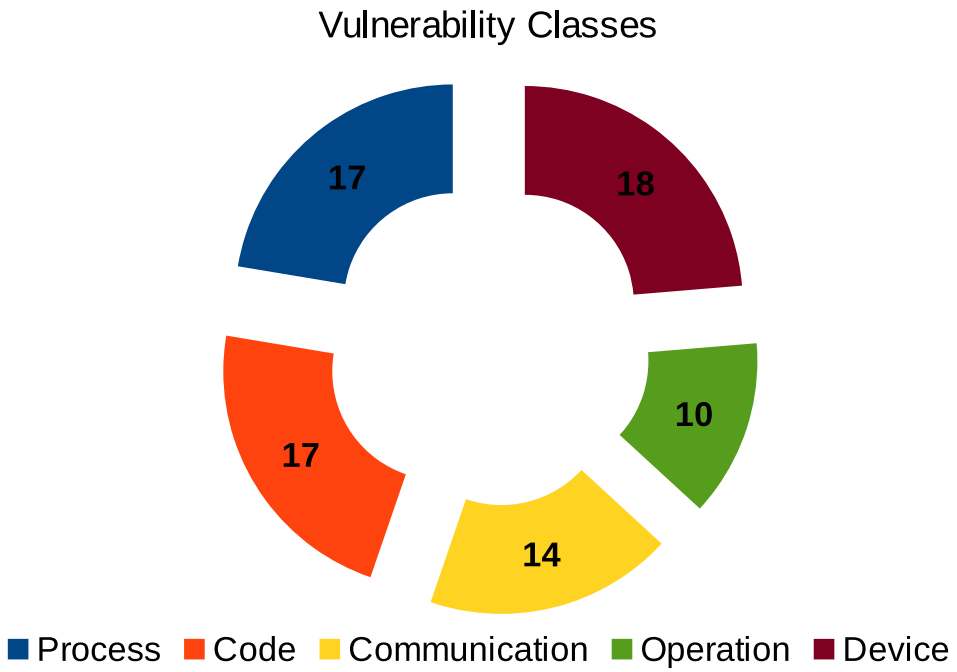

Figure 12. Vulnerabilities number by class.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

5. Known Vulnerabilities

Considering all the vulnerabilities extracted from the selected papers, we can classify them into the following classes:

- **process**, when related to common processes such as authentication, attestation, or manipulation;
- **code**, when related to development processes, including code practices and used technologies;
- **communication**, when related to protocols and data transmission;
- **operation**, when related to the device's use or configuration by the user;
- and **device**, when related to some characteristic of the devices.

From the 142 selected papers, only 47 presented vulnerabilities. We could classify some vulnerabilities in more than one class even though we classified them in only one. For example, we list the "lack of encryption" in the "device" class, but it could also apply to "communication" or "code" classes. Furthermore, many of the vulnerabilities are not directly related to IoT devices and applications but are listed in this section because they are mentioned in the selected articles. In Figure 11 and Figure 12, we show, respectively, the main vulnerability types with the number of mentions and number of vulnerabilities in each of the five classes.

To exemplify, the "access control" type refers to the existence of backdoors [10,19,20], easy physical access [21], and the lack of certificate validation [22] and access control [23]. The "outdated assets" relate to software [6,20], firmware [10], technologies, and services that are not updated [19,24,25], while "communication problems" consider infrastructure [26], network topology [27], protocols [19,24,25,28–30], and message exchange [22,23,31,32]. The "other" type includes device management [26], insecure deserialization [23], lack of integrity verification [7], SIM card modification [33], node interruption [26], device failure, and unauthorized access [10].

We list the mentioned vulnerabilities for each of the five classes in the following subsections.

5.1. Process

The list below contains all the vulnerabilities related to processes:

- diversity of authentication modes may generate high network traffic [34];
- lack of authentication facilitates access [34–36];
- lack of authentication and authorization in SDN [13];
- weak/broken or inadequate authentication (e.g., single-factor authentication method using a username and password) [8,23,26,37,38];
- broken access control [23];
- Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol is vulnerable to several well-known attacks, such as man-in-the-middle (MITM) and denial of service (DoS), and suffers from the disclosure of user identity on first access to the network [39];
- 5G-AKA allows for replay attacks since authentication and synchronization failure messages are sent to the device in plain text [40];
- other messages, such as RRC (Radio Resource Control) and NAS (Non-access stratum), are sent to the device in plain text, which can generate DoS and other attacks that compromise the confidentiality, as already happens with 4G [40];
- lack of attestation to know if a device is compromised [13];
- storage of keys in non-volatile memory (security chips, e.g., integrated circuits and smart cards) [7,29,41];
- lack of certificate validation or incorrect validation [22];
- lack of data integrity verification [7];
- information sharing with unsecured clouds [26,42];
- data manipulation/exposure [23,26];
- unprotected storage [7,19,36,43];
- insecure deserialization [23];
- management of large numbers of devices [26].

5.2. Code

The list below presents the vulnerabilities regarding code:

- outdated or insecure protocols [24,25];
- code vulnerabilities such as fragile programming processes, without good secure coding practices, and buffer overflow [25,26];
- vulnerable code allowing memory leak, code injection, and buffer overflow [6,7,23,44];

- memory buffer overflow can crash the system, allow control of program execution flow, or execute arbitrary code [22];
- XML external entity (XXE) injection [23];
- processing overload can facilitate replay attacks and RPL (routing protocol for low power and lossy networks) routing [26];
- non-standard protocol stacks, easily accessed physically or remotely [29];
- insecure encryption algorithms or outside the recommended standards (e.g., 3DES is vulnerable to collision attacks, RSA is vulnerable to side-channel attacks, and random probability approximation) [22,37,45];
- insecure pseudo-random generators [22];
- symmetric key algorithms are vulnerable to cryptographic attacks (e.g., known text, chosen text, and cryptanalysis) [46];
- asymmetric key algorithms are vulnerable to MitM and chosen text attacks [46];
- classic encryption algorithms, such as those based on the elliptic curve, are easily compromised when considering eventual advances in quantum computing [46];
- Diffie-Hellman (DH) algorithm is vulnerable to man-in-the-middle (MITM) attacks when exchanging public DH values between two devices [47];
- RSA algorithm (supports point-to-point communication and multicast routing in low power networks) is vulnerable to attacks such as forwarding, sinkhole, Sybil, Hello flooding, wormhole, black hole, and DoS [23];
- vulnerable web interfaces [48];
- single master key for software update [37];
- use of third-party libraries without proper security [43].

5.3. Communication

Below, we present the vulnerabilibies related to the communication mechanisms and processes:

- lack of security mechanisms (e.g., resistance to tampering) facilitates connection intrusion [10,27];
- vulnerabilities in infrastructure and edge devices [26];
- unreliable communication channel and medium access collisions [31];
- wireless communication can be exploited if not properly secured [29,49];
- wireless sensor networks allow for easier device duplication [44];
- massive access is susceptible to eavesdropping due to the broadcast nature of wireless channels [50];
- TLS and SSL are vulnerable to attacks such as resource exhaustion, flooding, replay, amplification attacks, BEAST (Browser Exploit Against SSL/TLS), CRIME (Compression Ratio Info-leak Made Easy), Heartbleed, and RC4 (Rivest Cipher 4) [23];
- insecure TLS/SSL version or configuration [22];
- cross-site scripting (XSS) [23];
- Access Stratum (AS) keys' stream reuse and NAS null encryption [28];
- 5G NSA (non-standalone) inherits vulnerabilities from 4G (network core) [30];
- simple HTTP communication [32];
- unencrypted communications [19,48];
- insecure pairing procedures [19].

5.4. Operation

The list below exhibits the vulnerabilities related to the operations:

- standard or weak passwords/credentials [4,6,20,24,30,37,51];
- incorrect OS and software configuration [26];
- outdated services and devices [19,24];
- lack of firmware/software update [6,10,20,25];
- node interruption [26];
- deployment site exposure can facilitate attacks [29];
- translation between security protocols of different networks can be a weakness [49];
- misconfiguration of security or standard configuration [7,23,36];
- bad user practices [30];
- frequent topology change in the Internet of Vehicles (IoV) networks [27].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

5.5. Device

Finally, we list the vulnerabilities related to the devices' characteristics:

- vulnerable hosts can create multi-host and multi-stage vulnerabilities [24];
- weak physical security and insecure communication interfaces - given the resource restrictions - can lead to spoofing and sleep deprivation attacks [26];
- lack of sophisticated/robust security mechanisms due to limitations of computational resources [6,20,49,52];
- easy device access enables malicious code execution [44];
- lack of identity privacy protection [53,54];
- lighter security technologies due to resource constraints [29];
- lack of encryption [4,28,35];
- weak encryption [4];
- wearable devices have a high probability of losing confidential information in case of theft or loan [55];
- device identity can be spoofed due to the lack of identity privacy protection [56,57];
- device location can be changed [57];
- rogue or compromised edge nodes and log files can be monitored by attackers [58];
- private keys can be compromised due to node security flaw [59];
- SIM card contents and functions can be remotely modified by sending a text message through OTA (Over-The-Air) technology [33];
- easy access to devices that do not require human interaction [21];
- lack of digital identity on devices [32];
- poorly designed devices allow easy execution of commands that can cause failures, or unauthorized access [10];
- existence of backdoors [10,19,20].

6. Threats In 5G-IoT Environments

To better understand the main threats in the 5G-IoT environment, we classified them into five categories, described in the following subsections.

6.1. Attacks on Data

Since information is the most valuable commodity, a wide range of attacks aims to retrieve sensitive data exchanged among devices and servers. These types of attacks can affect the confidentiality and integrity of data. Passive attacks can stay undetected for a long time since the data are not modified and nothing suspicious would be noticed by the users or devices. On the other hand, if the attacker acts actively on the communication channel by modifying, re-sending, or creating fake messages, the data integrity will be affected, and the results generated from these data may not be reliable [60].

Man-in-the-middle attacks are the main threat in the network layer. In these attacks, the adversary intercepts the connection between two connected devices, without being detected, and actively acts to change and forge the data that is sent between them. The attacker can also read and redirect the data in the communication channel, extracting sensitive information and harming the privacy of users and data. Fake data added by the attacker may also compromise the aggregation results and lead to wrong or harmful decisions by the system [61].

The connection between devices can also be intercepted and data passively retrieved in eavesdropping or sniffing attacks. The adversary will sniff the network and obtain the packets for further analysis. This attack is a major security flaw, compromising privacy and confidentiality [61]. The attacker can use the collected data to perform a traffic analysis [47], track the user behavior or location [62], or disclose sensitive information [63]. After eavesdropping on the communication, the adversary can also modify the data and forward them to the target, performing a replay attack [64].

The perception layer is also targeted when performing attacks on data since an attacker can subvert data aggregation by injecting false data or suppressing legitimate data through node replication, clone or injection. In node replication attacks, the adversary adds nodes to the network that mimics other existing legitimate nodes, aiming to obtain valuable information from the system. Similarly, node clone attacks create clones from existing nodes and use them for malicious purposes [44,65,66].

Node injection attacks are used to control data flow, by dropping a malicious node between the connection of two legitimate nodes, with the attacker acquiring control of the processing of any data. Another attack related to the perception layer is node tampering when the attacker changes the whole hardware or gains access to the node and acts to manipulate sensitive data generated or received by it [66–69].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

6.2. Access Attacks

In this type of attack, the adversary aims to gain unauthorized access to the IoT device, to the network, or to the service. Access attacks can affect all three layers of the IoT architecture [60].

If an attacker takes the smart card or the authentication device of a legitimate user, he or she may have the opportunity to impersonate the user's identity to perform other attacks, by stealing this smart card. Another possibility is skimming attacks, which aim to copy the physical credentials of a legitimate user, such as an ID card or chip. The attacker needs to have physical access to the device to be cloned, to install the skimming device, or to steal the physical credentials [70].

In the network layer, session hijacking attacks allow the attacker to take control over a valid session between the user or device and the server, pretending to be an authentic user and potentially sending fake data or collecting sensitive information [71]. Relay attacks are used to resend a legitimate user's authentication signal to gain network access without decrypting the message content. The attacker may succeed when no protection or additional checks are implemented [72].

The application layer is also susceptible to access attacks, such as stolen verifier attacks, where the attacker steal or modifies verification data, such as plain-text or hash passwords, biometric data, certificates, and others, which are stored in the server [73]. User or device credentials can also be retrieved by attackers through brute force attacks, guessing default passwords, or trying every possible encryption key, to gain access to the IoT network. This attack may affect also the perception layer since the attacker can target the sensors [47].

6.3. Masquerade Attacks

The attacker uses masquerade attacks to pretend to be someone else by using forged certificates or someone else's credentials, taking advantage of weak or nonexistent authentication protocols, to gain unauthorized access to the system or data through legitimate access identification. For example, an adversary can steal the key used in the authentication during the handshake response [38]. These attacks affect the perception and network layers since the attackers use node identities to access network traffic [60].

Forgery attacks are carried out aiming to forge node identities and obtain system authorization. The attacker can also impersonate an authenticated user or device in the network. Forged nodes and impersonation attacks can be used to perform counterfeiting attacks, where the adversary intercepts network data for analysis and tampering, and can change and replicate the contents of many IoT devices [61,74].

Forged network addresses can also be used to perform spoofing attacks, compromising both wired and wireless networks. This attack can be used by an adversary to get authentication credentials that belong to other users, and the attacker can use these data to gain access to a device or restrict service by impersonating a legitimate user [7].

Another threat is when an attacker creates a large number of pseudonymous identities to gain a large influence and subverts the service's reputation system. This attack, called Sybil, targets fault-tolerant schemes, such as distributed storage and multipath routing [71].

6.4. Routing Attacks

Routing attacks can control or even block the communication between nodes, affecting the network layer. The network's performance is degraded by compromising its resources, topology, and traffic, and may force the network to reorganize itself many times. These attacks include selective forwarding, wormhole, sinkhole, and flooding.

Selective forwarding attacks prevent the propagation of messages by refusing to forward them and simply dropping the messages. To reduce the suspicion of the wrongdoing, the attacker can drop the packets of a few selected nodes, or a group of nodes, and forward the remaining traffic, causing a denial of service for that node or group. The attacker can also subvert a node and neglect to route some messages. When the malicious node drops all the packets, the attack is called *black hole*, and when only some packets are forwarded and others dropped, it is called *grey hole* [31]. The grey hole variation is more difficult to detect, since there are several reasons for packet dropping, including packet collision and unreliable communication channels, and a careful analysis is required to detect the attack.

Wormhole is a passive attack that creates a communication tunnel between the target nodes, by using high-power transmission, encapsulation or out-of-band channels, to pipe data and performs a traffic analysis. The malicious node is located in a strategic place in the network, providing the shortest route for exchanging messages between the other devices. This attack can be used to make the two communication parties believe

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

they are close when they are not [31,75]. The attacker can also drop some of data or control packets to cause a denial of service.

The goal of a sinkhole attack is to attract the largest amount of traffic, being one of the most severe attacks that can be launched by a compromised node and can be used by the attacker to run selective forward, denial of service, and other related attacks. By using sinkhole, the attacker can prevent the server and other nodes to obtain correct data by misrounting legitimate packets and also by sending fabricated information. This attack can also be used to collect sensitive information from the network [76].

Finally, a flooding attack aims to flood the network with a large amount of packets, generating useless traffic or requests. This attack can slow down the server response or the network performance, and even cause a denial of service, preventing legitimate users from accessing services provided [77].

6.5. Availability Attacks

Availability attacks aim to degrade the service quality, making the service unavailable for legitimate users. This attack is especially dangerous to IoT devices since they have limited hardware resources and are optimized for low-power consumption and long-life operation [60]. These attacks target the network layer, with denial of service and desynchronization attacks, and the perception layer, with jamming and exhaustion attacks.

The main goal of denial-of-service attacks is to partially or completely avoid the access of legitimate users to one or more services or resources, by flooding the network traffic or sending a large amount of requests to the servers. Due to their computational constraints and weak security, IoT devices are often targeted to malware injection in order to build "botnets" and carry out distributed denial of service attacks, by using these devices in a coordinated manner to generate a large amount of traffic [20].

Desynchronization attacks aim to disconnect a valid tag from an identification system, by eavesdropping and replaying public messages. This attack does not reveal any tag's information to the adversary and can be considered a kind of denial of service attack since the tag cannot authenticate itself to the other entities [8].

In the perception layer, jamming attacks are used to block and disturb legitimate communications. This attack forces IoT devices to repeat the transmission over and over again, and can also knock out sensor network communications. Jamming is an easy attack to apply, as all wireless communication technology is vulnerable to it [78,79].

Exhaustion attacks intentionally consume device resources, such as battery lifespan, memory, and processing power, to disable the device and the network as a whole. This attack can exhaust the resources of the device in a relatively short period of time and it is stealthy enough for an attack target, making it difficult to detect [69].

6.6. Summary

As the previous sections demonstrate, the vast majority of threats in 5G-IoT environments are concentrated in the perception and network layers. Although the application layer is extremely relevant for the IoT context, threats directed at this layer cover a broader context, beyond the scope of this work, but should also be considered for the security assessment of IoT systems.

Threats to IoT systems at the network layer can be minimized by using secure communication protocols and encryption algorithms. Similarly, solutions can also be applied to the perception layer. Such solutions are discussed in the next section.

7. Proposed Solutions

Figure 13 presents an overview of the proposed solutions for IoT security identified in the research papers. The proposals included architectures, methodologies/methods, testbed, models, algorithms, protocols, schemes, approaches/mechanisms, and frameworks. Most of the solutions are related to approaches/mechanisms. Of the 142 papers, 47 did not present the proposal of specific solutions for IoT security.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

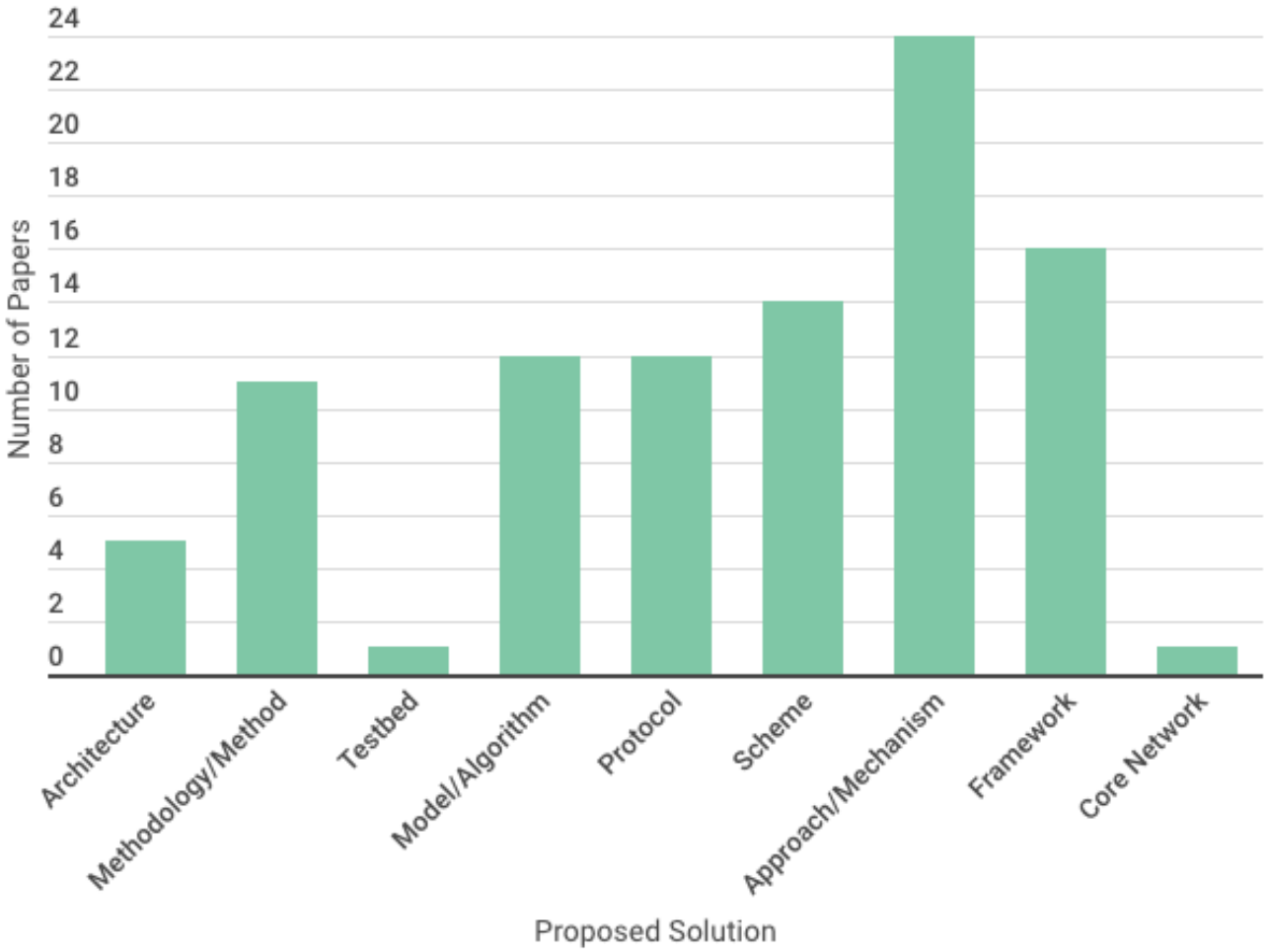

Figure 13. Proposed solutions identified in the research papers.

Each proposed solution focus on different threats (e.g., DDoS, eavesdropping, replay, MITM, and malware) or specific threats (e.g., APT). Figure 14 presents the relations between the purpose (i.e., detect/mitigate, planning, mitigate, or detect) of solutions identified in the research papers and threats. The bubble size relates to the number of papers focusing on the threats with specific purposes. The greater the size, the greater the number of research papers identified.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

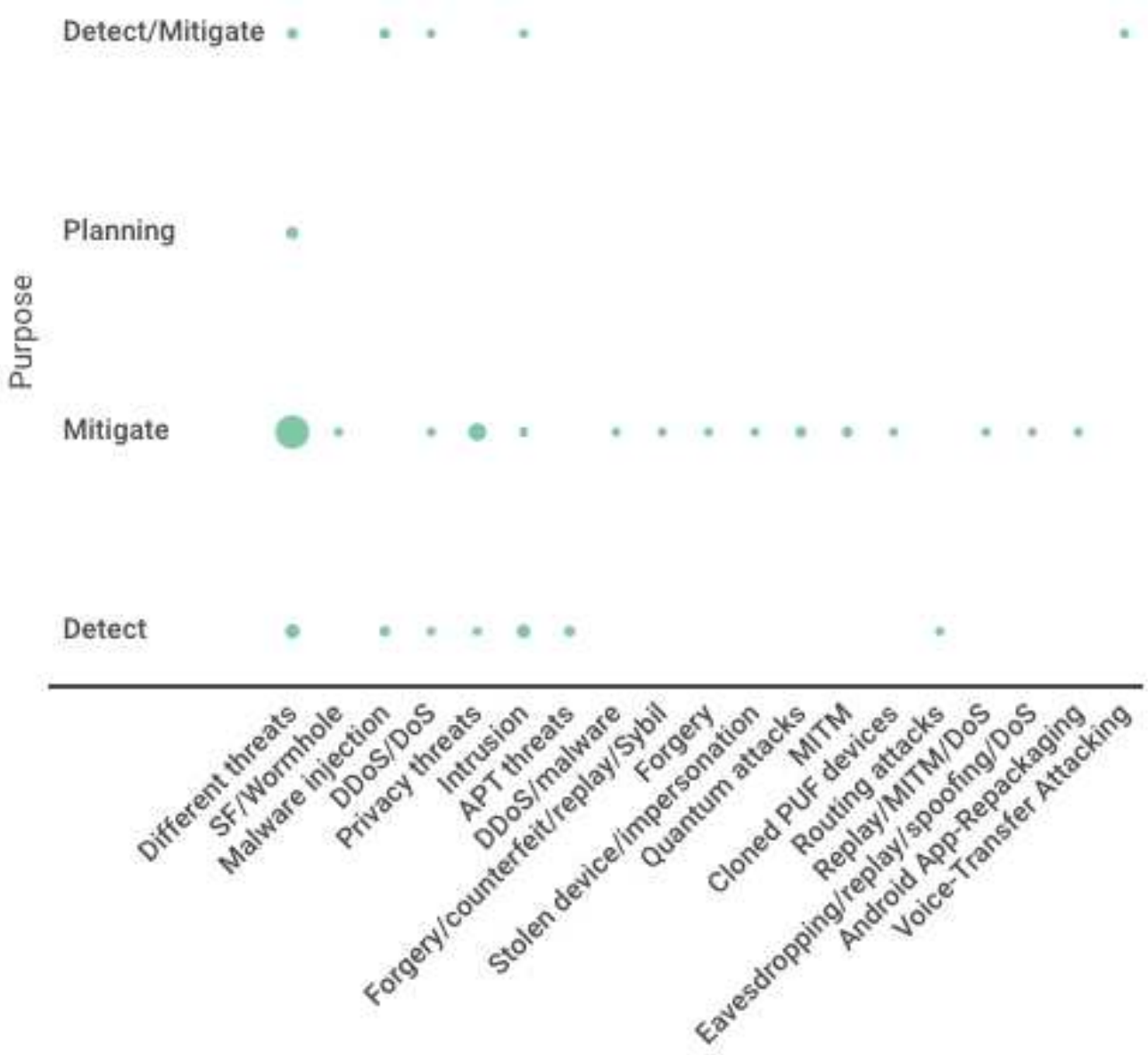

Figure 14. Proposed solutions identified in the research papers.

The solutions addressing different threats focused on design, implementation, security analysis, and security assurance frameworks [13,24,32,50,67,80–84]; systems for security assurance [47], intrusion detection [29] and security incident management [85]; approaches/mechanisms for security [7,25,28,40,41,43,45,48,86–91] and remote diagnostics [92]; schemes for security assurance [72,73,93–95]; protocols for security assurance [8,16,39,53,62,63,96–101]; algorithms for security assurance [102]; models/algorithms for security assurance [35,103], testbed for security experimentation [104]; methodology for development [66]; method for privacy and security [21,60,105]; design of core network [106], and architecture for security [23,42,59,107,108]. Some of the solutions rely on perception layer security, blockchain, embedded SIM, fuzzy logic, network slicing, deep learning, SDN/NFV, machine learning, federated learning, differentially private federated learning, chaotic digital watermarking, field programmable gate arrays, chaotic map zero-knowledge proof, and Boltzmann machine keys generation.

Regarding specific solutions, the authors focused on frameworks for security against Selective Forwarding (SF) and wormhole attacks [31], malware injection [109,110], DDoS attacks [111,112], and privacy threats [113]; systems for security against intrusion [27,114,115]; approaches/mechanisms for security against forgery, counterfeit, replay, and Sybil attacks [74], Advanced Persistent Threat (APT) [51], and DDoS and malware

 doi:10.20944/preprints202311.0565.v1

injection [58]; schemas for security against Stolen device and impersonation attacks [116], forgery [57], privacy threats [117,118], quantum attacks [54,56].

Besides, some solutions consider specific vertical applications smart health [31,32,45,64,66], Industrial IoT [29,35,82,91,105,106,119,120], smart cities [25,57,84,101], smart agriculture [108], public services [87], and smart transportation [27,121]. The remaining solutions do not address specific vertical applications, only focusing on IoT [3,8,13,24,39,43,50,51,58,63,74,83,85,86,99,109,112,116,117,122–125] or 5G-IoT [16,21,40,41,47,56,56,59,60, 60,62,67,72,73,77,80,81,88–90,92–95,97,98,100,102,104,105,107,110,111,113–115,115,118,126–132]. Tables 3 and 4 present a summary of the 95 proposed solutions identified in the selected papers.

Table 3. Summary of proposed solutions (Part 1).

Reference	Problem	Main Objective	Proposed Solution
Qiao et al. [50]	IoT security in the context of massive spectrum sharing.	Secure massive access.	A framework for securing cellular IoT networks.
Qadri et al. [31]	SF and wormhole in the context of healthcare-IoT.	Secure patients' data.	A blockchain-based cryptographic framework.
Ozdemir et al. [32]	Security of social assistive robotics.	Secure implementation.	A framework of social assistive robotics.
Vassilakis et al. [80]	Security in the context of multi-tenant MEC services.	Security analysis for virtualized small cell networks.	A framework for MEC in virtualised small cell networks.
Dib et al. [109]	Emergence of IoT malware.	IoT malware classification.	A multi-dimensional deep learning framework.
Ni et al. [67]	Security of network slicing and fog computing for 5G-IoT.	Authentication	Service-oriented authentication framework.
Mohammed et al. [81]	Security in the context of 5G IoT HetNets.	Preserve security.	A framework based on deep reinforcement learning.
Li et al. [82]	Security in the context of 5G-IoT systems.	Authentication.	Blockchain enabled zero-trust security framework.
Krishnan et al. [111]	Security in the context of fog-to-things computing.	Detecting attacks.	An autonomic multilayer security framework.
Huang et al. [83]	Security in the context of IoT.	Provide robust and transparent security protection.	A security framework.
Lagkas et al. [84]	Security in the context of UAV.	Protect drones as things.	UAV IoT framework.
Lawal et al. [112]	DDoS attacks in the context of IoT.	DDoS mitigation.	A framework for IoT using fog computing.
Jaiswal et al. [113]	Security in the context of IoT.	Maximize the secrecy rate of IoT systems.	A secure framework.
Rey et al. [110]	Malware in the context of IoT.	Malware detection.	A framework based on federated learning.
Ramezan et al. [13]	Security in the context of multi-hop cellular networks.	Compare secure routing protocols.	An evaluation framework.
Yadav et al. [24]	Vulnerabilities in the context of IoT.	Discover ways an attacker can breach a system.	A penetration testing framework.
Lee et al. [29]	Security in the context of industrial IoT.	Improve security.	A method for a secure cryptographic system on a chip.
Miloslavskaya et al. [85]	Security in the context of IoT ecosystems.	Information security incident management.	A blockchain-based system.
Kwon et al. [28]	Eavesdropping in the context of 5G-IoT.	Detection of eavesdropping.	An intrusion detection system
Miloslavskaya et al. [7]	Security in the context of IoT.	Improve security.	Applying the security intelligence approach.
Sharma et al. [92]	Security in remote diagnosis of IoT devices.	Secure validation of IoT devices.	Fuzzy logic for safety decisions and remote diagnosis.
Rim et al. [48]	DoS attacks in the context of 5G-IoT.	Detection and mitigation.	A system for defending and blocking attacks.
Anisetti et al. [43]	Security in the context of IoT.	Security assessment.	IoT security checker.
Mansour et al. [86]	Security in the context of smart interconnected networks.	Improve security.	Multi-layer security mechanism.
Jain et al. [114]	Security in the context of IoT ecosystem.	Improve security.	An intrusion detection system and network slicing.
Chitroub et al. [41]	Security in the context of IoT.	Secure mobile IoT deployment.	A solution based on the blind source separation method.
Ahmed et al. [51]	APT in the context of IoT.	Detection of APT.	A data-driven approach to detecting APT stages.
Rathee et al. [87]	Security of e-voting within IoT-oriented smart cities.	Improve security.	A secure e-voting mechanism based on blockchain.
Srinivasu et al. [45]	Security in the context of 5G-IoT.	Secured healthcare data communication.	A blockchain-based approach.
Shen et al. [58]	Security in the context of edge-assisted IoT.	Improve security.	A solution for the tradeoff between security and energy.
Osman et al. [25]	Security in the context of smart home IoT networks.	Reduce the attack surface.	A microsegmentation-based approach.
Hellaoui et al. [88]	Security in the context of 5G-IoT.	Provide optimized security levels.	An end-to-end adaptive approach.
Yujia et al. [74]	Security in the context of IoT.	Improve security.	An authentication mechanism.
Bordel et al. [89]	Security in the context of 5G-IoT.	Improve security.	A security mechanism.
Garcia et al. [90]	Security in the context of heterogeneous IoT networks.	Improve security.	A handover roaming mechanism.
Behrad et al. [40]	Security in the context of 5G-IoT.	Improve authentication and access control.	An authentication and access control mechanism.
Aqrabi et al. [91]	Security in the context of industrial IoT.	Improve authentication.	Physically unclonable function and a multi-layer approach.
Jung et al. [47]	Security in the context of IoT.	Improve security.	A secure gatekeeper system.
He et al. [27]	Security of intelligent transportation systems.	Improve access control.	An access control mechanism based on risk prediction.
Azad et al. [93]	Security in the context of IoT.	Improve authentication.	A self-enforcing authentication schema.
Tang and Keoh [57]	Security in the context of home area networks.	Improve security.	A scheme to secure data.
Lee et al. [116]	Security in the context of IoT.	Improve authentication.	A three-factor anonymous user authentication scheme.
Ambareen et al. [72]	Security in the context of 5G-IoT D2D communication.	Protect user information and data.	A secure authentication scheme.
Li et al. [117]	Security in the context of IoT applications.	Protect data.	Privacy preserving data aggregation scheme.
Shin et al. [73]	Security in the context of 5G-IoT.	Improve security.	Authentication, authorization, and key agreement scheme.
Yu et al. [56]	Security in the context of 5G NB-IoT.	Improve security.	Authentication and data transmission scheme.
Choudhury [118]	Identity privacy.	Protect identity.	A lightweight scheme.
Shin et al. [94]	Security of 5G and wireless sensor networks.	Improve security.	Two-factor authentication and key agreement scheme.
Cao et al. [54]	Security in the context of 5G NB-IoT.	Improve security.	Authentication and data distribution scheme.
Liu et al. [95]	Authentication in the context of crowdsourcing IoT.	Improve authentication.	Remote multi-factor authentication scheme.
Lu et al. [132]	Security in the context of MTC and 5G-IoT.	Improve security.	Traffic-driven intrusion detection scheme.
Kang et al. [122]	MITM attack in IoT networks.	Improve the detection.	A scheme using a hybrid routing mechanism.
Wu et al. [62]	Authentication in the context of 5G-IoT.	Improve authentication.	An authentication protocol.
Fan et al. [97]	Security in the context of 5G-IoT.	Improve authentication.	Ultralightweight NFC mutual authentication protocol.
Zhang et al. [123]	Security in the context of mobile IoT.	Improve security.	Security trusted protocol model.

 doi:10.20944/preprints202311.0565.v1

Table 4. Summary of proposed solutions (Part 2).

Reference	Problem	Main Objective	Proposed Solution
Khumalo et al. [53]	Security in the context of IoT and D2D communication.	Improve security.	Group-based authentication and key agreement protocol.
Fan et al. [98]	Authentication in the context of 5G-IoT.	Improve authentication.	RFID mutual authentication protocol.
Das [99]	Security in the context of IoT.	Improve security.	Secure protocol for constrained environments.
Lopes et al. [39]	Security in the context of MTC and IoT.	Improve security.	Authentication and key agreement protocol.
Duguma et al. [100]	Security in the context of D2D and 5G.	Improve security.	Lightweight D2D security protocol.
Xiao et al. [63]	Authentication in the context of 5G-IoT.	Improve authentication.	RFID lightweight authentication protocol.
Shin et al. [101]	Security in the context of smart home IoT networks.	Improve security.	Security protocol for route optimization.
Khalid et al. [8]	Authentication in the context of IoT.	Improve authentication.	Ultralightweight authentication protocol.
Khalid et al. [96]	Authentication in the context of IoT.	Improve authentication.	Advance strong authentication strong integrity protocol.
Sharma et al. [16]	Authentication in the context of IoT.	Improve authentication.	Secure authentication protocol.
Nie et al. [131]	Security in the context of SDN-based IoT.	Improve security.	A differentially private tensor computing model.
Anand et al. [64]	Malware attacks in 5G-IoT healthcare applications.	Malware detection.	CNN-based deep learning model.
Zhang et al. [119]	Security in the context of industrial IoT.	Improve security.	Federated learning and transfer learning model.
Rajawat et al. [102]	Security in the context of 5G-IoT.	Improve security.	Boltzmann machine-based encryption algorithm.
Fu et al. [124]	Security in the context of 5G-IoT.	Improve detection.	Automata-based intrusion detection method.
Laguduva et al. [125]	IoT edge node security.	Improve security.	A model to identify an original or cloned PUF.
Mo [35]	Security in the context of industrial 5G-IoT.	Improve security.	A model for abnormal traffic detection.
Krundyshev et al. [120]	Security in the context of smart infrastructures.	Cyber attack detection.	Artificial neural network models.
Sadique et al. [3]	Data privacy in the context of IoT.	Protect data.	A model for data privacy enhancement.
Rawal et al. [103]	Security in the context of IoT.	Improve security.	An interstitial model.
Baniata et al. [130]	Security of fog-enabled mobile cloud computing.	Improve security.	A privacy-preserving model.
Rezvy et al. [77]	Security in the context of 5G-IoT.	Intrusion classification and prediction.	A deep learning model.
Ravi et al. [104]	Security in the context of 5G-IoT.	Analyze security aspects.	A testbed for security.
Taimoor et al. [66]	Security of IoT-based personalized healthcare services.	Improve security.	A methodology for developing health services.
Wang et al. [105]	Voice-transfer attack in industrial 5G-IoT.	Detection and mitigation.	A method for addressing voice-transfer attacks.
Wang et al. [133]	Binary black-box adversarial attacks.	Improve malware detection.	An adversary sample generation method.
Khan [115]	Security in the context of 5G-IoT.	Improve security.	ElGamal with public key infrastructure techniques.
Sankar et al. [129]	Security in the context of beyond 5G and IoT.	Improve security.	Private blockchain in SDN and an authentication method.
Catania et al. [128]	Privacy threats in the context of 5G-IoT.	Protect privacy.	An analysis methodology.
Lee et al. [127]	Security of online identification process in 5G-IoT.	Improve security.	Transaction linkage technique.
Sarac et al. [21]	Cyber-attacks on IoT devices.	Improve security.	Integrate security gateway architecture and blockchain.
Holik [60]	Security in the context of IoT.	Improve security.	Protection techniques based on SDN.
Lee et al. [121]	Android app-repackaging attacks on in-vehicle networks.	Mitigate the Android app-repackaging attacks.	A security technology as a countermeasure.
Cheng et al. [126]	APT in the context of 5G-IoT.	Predict APT.	Method based on differentially private federated learning.
Deebak et al. [107]	Security and privacy in the context of 5G-IoT.	Security and privacy preservation.	A blockchain-based lightweight distributed architecture.
Alvarenga et al. [59]	Security in the context of IoT.	Secure management.	A hybrid distributed ledger architecture.
Chopra et al. [42]	Security in the context of ultra-dense networks.	Improve security.	An architecture for security in ultra-dense networks.
Mrabet et al. [23]	Security in the context of IoT.	Improve security.	An optimized architecture for IoT.
Vangala et al. [108]	Security in IoT-enabled smart agriculture.	Improve security.	An architecture for smart farming.
Szymanski [106]	Security in the context of industrial-tactile IoT.	Improve security.	A secure deterministic industrial-tactile IoT core network.

8. Recommendations

Most of the reviewed papers addressing recommendations presented secondary studies (e.g., [69,134]). Examples of general recommendations are listed below:

- users should not use default passwords;
- users should keep software updated;
- developers should ensure secure communication;
- developers should simplify the installation and maintenance of devices;
- developers should ensure software integrity;
- developers should ensure that personal data protection; and
- developers should prevent interruptions.

Other recommendations include the usage of intrusion detection systems [6,20,36,135–137], threat detection systems [65], early warning systems [138], anomaly detection systems [61], code clone detection [44], post-quantum cryptography [69], lightweight cryptography [37,68,134,139,140], temporary identity [141], authentication [4,7,9,49,52,70,79,108,142], authorization [78], blockchain [30,38,76,143–145], perception layer security [10,146,147], covert timing channels [148], end-to-end security [149], key management [34], secure exchanging data [26], and frequent key update [150].

The following sections highlight the most frequent recommendations identified in the reviewed papers. Specifically, we highlight machine learning-based solutions, blockchain-based solutions, lightweight solutions (e.g., lightweight cryptography and protocols), and perception layer security.

8.1. Machine Learning

The usage of machine learning is a trend in the context of 5G-IoT security. Implementing intrusion detection systems based on deep learning can increase security, for instance, of vehicular networks in a distributed architecture [135]. Examples of specific usage scenarios include attack detection (e.g., DDoS [6]), anomaly detection, malware IoT detection, and botnet detection. These systems can rely on techniques such as deep neural networks, convolutional neural networks, Recurrent Neural Networks (RNN), long short term memory RNN, and gated recurrent unit RNN.

In addition to deep learning solutions, less complex supervised learning approaches are also relevant [20]. Thus, algorithms such as k-nearest neighbors, random forest, and decision trees, can be trained to implement detection, classification, and mitigation models to improve 5G-IoT security [61].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 November 2023 doi:10.20944/preprints202311.0565.v1

We highlight some of the proposed solutions identified in the previous section to exemplify possible implementation. Dib et al. [109] proposed a framework based on deep learning techniques for classifying IoT malware. The solution can identify new malware families in the context of 5G-IoT. Lawal et al. [112] presented a framework for DDoS attacks mitigation based on machine learning. The framework relies on fog computing to address processing and storage problems. Rey et al. [110] proposed a security framework based on federated learning to detect malware affecting IoT devices. Anand et al. [64] proposed a convolutional neural network for detecting malware attacks in 5G-IoT.

8.2. Blockchain

Another recommended solution to increase security and privacy in 5G-IoT is the usage of blockchain [145]. Blockchain-based solutions can be part of frameworks to secure IoT applications [144]. Blockchain enables the decentralization of security resources in 5G-IoT environments.

Assuring trust, confidentiality, and integrity is a relevant issue in the context of 5G-IoT. Therefore, blockchain can assist in tracking, organizing, and supporting communications. Besides, such technology can ensure transparency and improve confidence in IoT applications (and services) such as smart e-voting in the context of smart cities [87].

For instance, Miloslavskaya and Tolstoy [85] proposed a blockchain-based system for information security incident management. Srinivasu et al. [45] propose a blockchain-based approach to secure healthcare data communication in the context of 5G-IoT. Deebak and AL-Turjman [107] proposed a lightweight and robust blockchain-based distributed architecture for 5G-IoT.

8.3. Lightweight Solutions

Given the resource constraints of IoT devices, it is essential to provide lightweight solutions such as lightweight cryptographic algorithms. Cryptography is a popular and relevant solution in the context of IoT. Lightweight cryptographic algorithms relate to block ciphers and stream ciphers. S-AES, ICEBERG, and DES are examples of block ciphers; while GRAIN and Trivium are examples of stream ciphers [140]. There are also proposals of hybrid ciphers (e.g., Hummingbird).

Besides, authentication is recommended to increase the security of IoT devices. For instance, Ambareen et al. [72] presented an authentication scheme for in 5G-IoT in the context of D2D communications. Fan et al. [97] proposed an ultralight mutual authentication protocol for near field communication.

8.4. Perception Layer Security

Perception layer security can also support in ensuring the security (e.g., confidentiality) of resource-constrained IoT devices. For instance, 5G-IoT devices with full-duplex capability can be exploited to prevent jamming attacks [147]. Besides, perception layer security schemes are recommended to present eavesdropping by increasing the secrecy rate. Other examples of possible solutions include, but are not limited to perception layer authentication (e.g., preventing pilot contamination attacks) and frequency-hopping spread spectrum (e.g., preventing interference attacks). As a specific solution, Qi et al. [50] presented a secure massive access framework for the 5G-IoT, exploiting the inherent co-channel interference.

9. Related Work

A wide range of papers covers security and privacy issues in 5G networks. The security aspects in 3GPP 5G networks are presented by [151] and [152]. The authors stated that security requirements should be standardized and all vendors and operators must ensure they are enforceable and verifiable. Research issues in slice authentication mechanisms are discussed by [152]. The paper [151] also points out that IoT integration may raise more security concerns, particularly regarding privacy. Security risks in 5G-IoT environments are analyzed by [33], and security requirements are proposed for IoT control and management.

An overview of challenges in 5G-IoT systems is provided by [153], with security threats and approaches to mitigate them. The paper addresses the challenges in communications between devices and with the cloud, presenting protocols and techniques to improve it and provide scalability. The paper [154] points out that the concerns about security and privacy are the centerpiece in 5G-IoT environments, and a systematic security strategy is required in 5G-IoT environments.

10. Conclusions

We presented a trusted and general IoT architecture, proposing the application of TEEs to core components of a distributed architecture commonly employed for cloud/fog-based IoT applications. We used HCPN to formally model the architecture and verify security aspects, considering the communication between all the architecture components and the authentication, authorization, and encryption processes. We defined 14 security properties and performed model checking, enabling the generation of other project artifacts (e.g., test cases) to increase confidence in the trusted architecture's correct usage. As all properties are satisfied through the model checking, we have evidence that the trusted architecture assures data confidentiality and integrity, preserving data's security and privacy. We answered our defined RQs by presenting the generic, modular, executable, and parametric specification, supported by model checking and MBT with the MBT/CPN tool. As future work, we envision the modeling and model checking of the remote attestation protocol, also considering security aspects. Our model can be extended to include, for instance, time information based on experiments, allowing the verification regarding scalability and performance properties.

Author Contributions:

Funding:

Acknowledgments: We thank the National Telecommunications Agency (Agência Nacional de Telecomunicações - ANATEL) for supporting this research. We also thank the VIRTUS Research, Development, and Innovation Center, and the Embedded and Pervasive Computing Laboratory, Federal University of Campina Grande.

Conflicts of Interest:

References

1. Bockelmann, C.; Pratas, N.K.; Wunder, G.; Saur, S.; Navarro, M.; Gregoratti, D.; Vivier, G.; De Carvalho, E.; Ji, Y.; StefanoviC, C.; Popovski, P.; Wang, Q.; Schellmann, M.; Kosmatos, E.; Demestichas, P.; Raceala-Motoc, M.; Jung, P.; Stanczak, S.; Dekorsy, A. Towards Massive Connectivity Support for Scalable mMTC Communications in 5G Networks. *IEEE Access* **2018**, *6*, 28969–28992. doi:10.1109/ACCESS.2018.2837382.
2. Chen, Y.; Sambo, Y.A.; Onireti, O.; Imran, M.A. A Survey on LPWAN-5G Integration: Main Challenges and Potential Solutions. *IEEE Access* **2022**, *10*, 32132–32149. doi:10.1109/ACCESS.2022.3160193.
3. Sadique, K.M.; Rahmani, R.; Johannesson, P. Enhancing Data Privacy in the Internet of Things (IoT) Using Edge Computing. Proceedings of the 2nd International Conference on Computational Intelligence, Security and Internet of Things; Springer: Agartala, India, 2020; pp. 231–243. doi:10.1007/978-3-030-66763-4_20.
4. Ghorbani, H.; Mohammadzadeh, M.S.; Ahmadzadegan, M.H. DDoS Attacks on the IoT Network with the Emergence of 5G. Proceedings of the International Conference on Technology and Entrepreneurship; IEEE: San Jose, CA, USA, 2020; pp. 1–5. doi:10.1109/ICTE-V50708.2020.9113779.
5. Valadares, D.C.G.; Will, N.C.; Sobrinho, A.A.C.C.; Lima, A.C.D.; Morais, I.S.; Santos, D.F.S. Security Challenges and Recommendations in 5G-IoT Scenarios. To appear in AINA 2023 Proceedings.
6. Lohachab, A.; Karambir, B. Critical Analysis of DDoS — An Emerging Security Threat over IoT Networks. *Journal of Communications and Information Networks* **2018**, *3*, 57–78. doi:10.1007/s41650-018-0022-5.
7. Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information Security Challenges and Solutions. *Cluster Computing* **2019**, *22*, 103–119. doi:10.1007/s10586-018-2823-6.
8. Khalid, M.; Mujahid, U.; ul Islam Muhammad, N. Ultralightweight RFID Authentication Protocols for Low-Cost Passive RFID Tags. *Security and Communication Networks* **2019**, *2019*, 1–25. doi:10.1155/2019/3295616.
9. Borgaonkar, R.; Anne Tøndel, I.; Zenebe Degefa, M.; Gilje Jaatun, M. Improving Smart Grid Security Through 5G Enabled IoT and Edge Computing. *Concurrency and Computation: Practice and Experience* **2021**, *33*, e6466. doi:10.1002/cpe.6466.
10. Mogadem, M.M.; Li, Y.; Meheretie, D.L. A Survey on Internet of Energy Security: Related Fields, Challenges, Threats and Emerging Technologies. *Cluster Computing* **2021**, *25*, 2449–2485. doi:10.1007/s10586-021-03423-z.
11. Kitchenham, B.A.; Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, 2007.

12. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic Mapping Studies in Software Engineering. Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering; British Computer Society: Bari, Italy, 2008.
13. Ramezan, G.; Leung, C.; Wang, Z.J. A Survey of Secure Routing Protocols in Multi-Hop Cellular Networks. *IEEE Communications Surveys & Tutorials* **2018**, *20*, 3510–3541. doi:10.1109/COMST.2018.2859900.
14. Kitchenham, B.A.; Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Technical Report EBSE 2007-001, School of Computer Science and Mathematics, Keele University, 2007.
15. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796.
16. Sharma, S.; Satapathy, S.; Singh, S.; Sahu, A.K.; Obaidat, M.S.; Saxena, S.; Puthal, D. Secure Authentication Protocol for 5G Enabled IoT Network. Proceedings of the 5th International Conference on Parallel, Distributed and Grid Computing; IEEE: Solan Himachal Pradesh, India, 2018; pp. 621–626. doi:10.1109/PDGC.2018.8745799.
17. Liao, C.H.; Shuai, H.H.; Wang, L.C. Eavesdropping Prevention for Heterogeneous Internet of Things Systems. Consumer Communications & Networking Conf; IEEE: Las Vegas, NV, USA, 2018; pp. 1–2. doi:10.1109/CCNC.2018.8319297.
18. Nieto, A.; Acien, A.; Fernandez, G. Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation. *Mob. Netw. Appl.* **2019**, *24*, 881–889. doi:10.1007/s11036-018-1146-4.
19. Shim, J.P.; Sharda, R.; French, A.M.; Syler, R.A.; Patten, K.P. The Internet of Things: Multi-faceted Research Perspectives. *Communications of the Association for Information Systems* **2020**, pp. 511–536. doi:10.17705/1cais.04621.
20. Salim, M.M.; Rathore, S.; Park, J.H. Distributed Denial of Service Attacks and its Defenses in IoT: A Survey. *The Journal of Supercomputing* **2020**, *76*, 5320–5363. doi:10.1007/s11227-019-02945-z.
21. Šarac, M.; Pavlović, N.; Bacanin, N.; Al-Turjman, F.; Adamović, S. Increasing Privacy and Security by Integrating a Blockchain Secure Interface Into an IoT Device Security Gateway Architecture. *Energy Reports* **2021**, *7*, 8075–8082. doi:10.1016/j.egyr.2021.07.078.
22. Mathas, C.M.; Vassilakis, C.; Kolokotronis, N.; Zarakovitis, C.C.; Kourtis, M.A. On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids. *Energies* **2021**, *14*, 2818. doi:10.3390/en14102818.
23. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* **2020**, *20*, 3625. doi:10.3390/s20133625.
24. Yadav, G.; Paul, K.; Allakany, A.; Okamura, K. IoT-PEN: A Penetration Testing Framework for IoT. Proceedings of the International Conference on Information Networking; IEEE: Barcelona, Spain, 2020; pp. 196–201. doi:10.1109/ICOIN48656.2020.9016445.
25. Osman, A.; Wasicek, A.; K¨opsell, S.; Strufe, T. Transparent Microsegmentation in Smart Home IoT Networks. Proceedings of the 3rd USENIX Workshop on Hot Topics in Edge Computing; USENIX Association: Virtual Event, 2020; pp. 1–6.
26. Saleem, K.; Alabduljabbar, G.M.; Alrowais, N.; Al-Muhtadi, J.; Imran, M.; Rodrigues, J.J.P.C. Bio-Inspired Network Security for 5G-Enabled IoT Applications. *IEEE Access* **2020**, *8*, 229152–229160. doi:10.1109/ACCESS.2020.3046325.
27. He, Y.; Kong, M.; Du, C.; Yao, D.; Yu, M. Communication Security Analysis of Intelligent Transportation System Using 5G Internet of Things From the Perspective of Big Data. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 2199–2207. doi:10.1109/TITS.2022.3141788.
28. Kwon, S.; Park, S.; Cho, H.; Park, Y.; Kim, D.; Yim, K. Towards 5G-based IoT Security Analysis Against Vo5G Eavesdropping. *Computing* **2021**, *103*, 425–447. doi:10.1007/s00607-020-00855-0.
29. Lee, B.; Lee, I.G.; Kim, M. Design and Implementation of Secure Cryptographic System on Chip for Internet of Things. *IEEE Access* **2022**, *10*, 18730–18742. doi:10.1109/ACCESS.2022.3151430.
30. Vaezi, M.; Azari, A.; Khosravirad, S.R.; Shirvanimoghaddam, M.; Azari, M.M.; Chasaki, D.; Popovski, P. Cellular, Wide-Area, and Non-Terrestrial IoT: A Survey on 5G Advances and the Road Toward 6G. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 1117–1174. doi:10.1109/COMST.2022.3151028.
31. Qadri, Y.A.; Ali, R.; Musaddiq, A.; Al-Turjman, F.; Kim, D.W.; Kim, S.W. The Limitations in the State-of-the-Art Counter-Measures Against the Security Threats in H-IoT. *Cluster Computing* **2020**, *23*, 2047–2065. doi:10.1007/s10586-019-03036-7.

32. Ozdemir, D.; Cibulka, J.; Stepankova, O.; Holmerova, I. Design and Implementation Framework of Social Assistive Robotics for People with Dementia - A Scoping Review. *Health and Technology* **2021**, *11*, 367–378. doi:10.1007/s12553-021-00522-0.
33. Qiu, Q.; Du, X.; Yu, S.; Wang, C.; Liu, S.; Zhao, B.; Chang, L. Research on IoT Security Technology and Standardization in the 5G Era. Proceedings of the International Conference on Security and Privacy in New Computing Environments; Springer: Virtual Event, 2021; pp. 77–90. doi:10.1007/978-3-030-66922-5_5.
34. Rahimi, H.; Zibaeenejad, A.; Rajabzadeh, P.; Safavi, A.A. On the Security of the 5G-IoT Architecture. Proceedings of the International Conference on Smart Cities and Internet of Things; ACM: Mashhad, Iran, 2018. doi:10.1145/3269961.3269968.
35. Mo, X. The Development Direction of Industrial Internet of Things based on 5G Communication. *Journal of Physics: Conference Series* **2020**, *1648*, 042121. doi:10.1088/1742-6596/1648/4/042121.
36. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart Home Security: Challenges, Issues and Solutions at Different IoT Layers. *The Journal of Supercomputing* **2021**, *77*, 14053–14089. doi:10.1007/s11227-021-03825-1.
37. Gong, G. Securing Internet-of-Things. Proceedings of the 11th International Symposium on Foundations and Practice of Security; Springer: Montreal, Canada, 2018; pp. 3–16. doi:10.1007/978-3-030-18419-3_1.
38. Xingzhong, J.; Qingshui, X.; Haifeng, M.; Jiageng, C.; Haozhi, Z. The Research on Identity Authentication Scheme of Internet of Things Equipment in 5G Network Environment. Proceedings of the 19th International Conference on Communication Technology; IEEE: Xi'an, China, 2019; pp. 312–316. doi:10.1109/ICCT46805.2019.8947126.
39. Lopes, A.P.G.; Hilgert, L.O.; Gondim, P.R.; Lloret, J. Secret Sharing-Based Authentication and Key Agreement Protocol for Machine-Type Communications. *International Journal of Distributed Sensor Networks* **2019**, *15*, 1550147719841003. doi:10.1177/1550147719841003.
40. Behrad, S.; Bertin, E.; Tuffin, S.; Crespi, N. A New Scalable Authentication and Access Control Mechanism for 5G-Based IoT. *Future Generation Computer Systems* **2020**, *108*, 46–61. doi:10.1016/j.future.2020.02.014.
41. Chitroub, S.; Blaid, D.; Aouadia, H.; Laouar, R. Securing Mobile IoT Deployment Using Embedded SIM: Concerns and Solutions. Proceedings of the International Conference on Internet of Things, Embedded Systems and Communications; IEEE: Tunis, Tunisia, 2019; pp. 75–79. doi:10.1109/IINTEC48298.2019.9112138.
42. Chopra, G.; Kumar Jha, R.; Jain, S. A Survey on Ultra-Dense Network and Emerging Technologies: Security Challenges and Possible Solutions. *Journal of Network and Computer Applications* **2017**, *95*, 54–78. doi:10.1016/j.jnca.2017.07.007.
43. Anisetti, M.; Asal, R.; Ardagna, C.A.; Comi, L.; Damiani, E.; Gaudenzi, F. A Knowledge-Based IoT Security Checker. Proceedings of the European Conference on Parallel Processing; Springer: Turin, Italy, 2018; pp. 299–311. doi:10.1007/978-3-030-10549-5_24.
44. Zhang, H.; Sakurai, K. A Survey of Software Clone Detection From Security Perspective. *IEEE Access* **2021**, *9*, 48157–48173. doi:10.1109/ACCESS.2021.3065872.
45. Srinivasu, P.N.; Bhoi, A.K.; Nayak, S.R.; Bhutta, M.R.; Woźniak, M. Blockchain Technology for Secured Healthcare Data Communication Among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics* **2021**, *10*, 1437. doi:10.3390/electronics10121437.
46. Althobaiti, O.S.; Dohler, M. Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World. *IEEE Access* **2020**, *8*, 157356–157381. doi:10.1109/ACCESS.2020.3019345.
47. Jung, Y.; Agulto, R. Virtual IP-Based Secure Gatekeeper System for Internet of Things. *Sensors* **2021**, *21*, 38. doi:10.3390/s21010038.
48. Rim, K.; Lim, D. DoS Attack Control Design of IoT System for 5G Era. *Journal of Information and Communication Convergence Engineering* **2018**, *16*, 93–98. doi:10.6109/JICCE.2018.16.2.93.
49. Chen, S.; Ma, R.; Chen, H.H.; Zhang, H.; Meng, W.; Liu, J. Machine-to-Machine Communications in Ultra-Dense Networks — A Survey. *IEEE Communications Surveys & Tutorials* **2017**, *19*, 1478–1503. doi:10.1109/COMST.2017.2678518.
50. Qi, Q.; Chen, X.; Zhong, C.; Zhang, Z. Physical Layer Security for Massive Access in Cellular Internet of Things. *Science China Information Sciences* **2020**, *63*, 1–12. doi:10.1007/s11432-019-2650-4.
51. Yussuf Ahmed, A.Taufiq Asyhari, M.A.R. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Computers, Materials & Continua* **2021**, *67*, 2497–2513. doi:10.32604/cmc.2021.014223.

52. Wazid, M.; Das, A.K.; Shetty, S.; Gope, P.; Rodrigues, J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access* **2021**, *9*, 4466–4489. doi:10.1109/ACCESS.2020.3047895.
53. Khumalo, P.; Nleya, B.; Gomba, A.; Mutsvangwa, A. Services and Applications Security in IoT Enabled Networks. Proc. of the Intl. Conf. on Intelligent and Innovative Computing Applications; IEEE: Mon Tresor, Mauritius, 2018. doi:10.1109/ICONIC.2018.8601298.
54. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H. Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System. *IEEE Internet of Things Journal* **2019**, *6*, 9794–9805. doi:10.1109/JIOT.2019.2931724.
55. Uddin, H.; Gibson, M.; Safdar, G.A.; Kalsoom, T.; Ramzan, N.; Ur-Rehman, M.; Imran, M.A. IoT for 5G/B5G Applications in Smart Homes, Smart Cities, Wearables and Connected Cars. Proceedings of the 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks; IEEE: Limassol, Cyprus, 2019; pp. 1–5. doi:10.1109/CAMAD.2019.8858455.
56. Yu, P.; Cao, J.; Ma, M.; Li, H.; Niu, B.; Li, F. Quantum-Resistance Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks. Proceedings of the Wireless Communications and Networking Conference; IEEE: Marrakesh, Morocco, 2019; pp. 1–7. doi:10.1109/WCNC.2019.8885686.
57. Tang, Z.; Keoh, S.L. An Efficient Scheme to Secure Data Provenance in Home Area Networks. Proceedings of the 3rd 5G World Forum; IEEE: Bangalore, India, 2020; pp. 115–120. doi:10.1109/5GWF49715.2020.9221402.
58. Shen, S.; Zhang, K.; Zhou, Y.; Ci, S. Security in edge-assisted Internet of Things: challenges and solutions. *Science China Information Sciences* **2020**, *63*, 1–14. doi:10.1007/s11432-019-2906-y.
59. Alvarenga, I.D.; Camilo, G.F.; De Souza, L.A.C.; Duarte, O.C.M.B. DAGSec: A Hybrid Distributed Ledger Architecture for the Secure Management of the Internet of Things. Proceedings of the International Conference on Blockchain; IEEE: Melbourne, Australia, 2021; pp. 266–271. doi:10.1109/Blockchain53845.2021.00043.
60. Holik, F. Protecting IoT Devices with Software-Defined Networks. Proceedings of the International Conference on Intelligent Technologies and Applications; Springer: Grimstad, Norway, 2021; pp. 41–52. doi:10.1007/978-3-030-71711-7_4.
61. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of Machine Learning and Deep Learning in Securing 5G-Driven Industrial IoT Applications. *Ad Hoc Networks* **2021**, *123*, 102685. doi:10.1016/j.adhoc.2021.102685.
62. Wu, T.Y.; Lee, Z.; Obaidat, M.S.; Kumari, S.; Kumar, S.; Chen, C.M. An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks. *IEEE Access* **2020**, *8*, 28096–28108. doi:10.1109/ACCESS.2020.2969986.
63. Xiao, L.; Xu, H.; Zhu, F.; Wang, R.; Li, P. SKINNY-Based RFID Lightweight Authentication Protocol. *Sensors* **2020**, *20*, 1366. doi:10.3390/s20051366.
64. Anand, A.; Rani, S.; Anand, D.; AljahThe Development Direction ofdali, H.M.; Kerr, D. An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications. *Sensors* **2021**, *21*, 6346. doi:10.3390/s21196346.
65. Gafurov, K.; Chung, T.M. Comprehensive Survey on Internet of Things, Architecture, Security Aspects, Applications, Related Technologies, Economic Perspective, and Future Directions. *Journal of Information Processing Systems* **2019**, *15*, 797–819. doi:10.3745/JIPS.03.0125.
66. Taimoor, N.; Rehman, S. Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey. *IEEE Access* **2022**, *10*, 535–563. doi:10.1109/ACCESS.2021.3137364.
67. Ni, J.; Lin, X.; Shen, X.S. Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. *IEEE Journal on Selected Areas in Communications* **2018**, *36*, 644–657. doi:10.1109/JSAC.2018.2815418.
68. Qiu, Q.; Wang, D.; Du, X.; Yu, S.; Liu, S.; Zhao, B. Security Standards and Measures for Massive IoT in the 5G Era. *Mobile Networks and Applications* **2022**, *27*, 392–403. doi:10.1007/s11036-021-01841-2.
69. Seyhan, K.; Nguyen, T.N.; Akleylek, S.; Cengiz, K. Lattice-Based Cryptosystems for the Security of Resource-Constrained IoT Devices in Post-Quantum World: A Survey. *Cluster Computing* **2022**, *25*, 1729–1748. doi:10.1007/s10586-021-03380-7.
70. Ferrag, M.A.; Shu, L.; Choo, K.K.R. Fighting COVID-19 and Future Pandemics With the Internet of Things: Security and Privacy Perspectives. *IEEE/CAA Journal of Automatica Sinica* **2021**, *8*, 1477–1499. doi:10.1109/JAS.2021.1004087.
71. Zidková, N.; Maryska, M. Threat Analysis of 5G Technology Within IIoT Sensors. Proceedings of the Future Technologies Conference; Springer: Vancouver, BC, Canada, 2022; pp. 389–402. doi:10.1007/978-3-030-89906-6_26.

72. Ambareen, J.; Prabhakar, M.; Ara, T. LEES: A Hybrid Lightweight Elliptic ElGamal-Schnorr-Based Cryptography for Secure D2D Communications. *Journal of Telecommunications and Information Technology* **2021**, *2*, 24–30. doi:10.26636/jtit.2021.146020.
73. Shin, S.; Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. doi:10.1109/ACCESS.2020.2985719.
74. Yujia, H.; Yongfeng, H.; Fu, C. Research on Node Authentication of MQTT Protocol. Proceedings of the 11th International Conference on Software Engineering and Service Science; IEEE: Beijing, China, 2020; pp. 405–410. doi:10.1109/ICSESS49938.2020.9237678.
75. Zenger, C.T.; Zimmer, J.; Pietersz, M.; Driessen, B.; Paar, C. Constructive and Destructive Aspects of Adaptive Wormholes for the 5G Tactile Internet. Proceedings of the 9th Conference on Security & Privacy in Wireless and Mobile Networks; ACM: Darmstadt, Germany, 2016; pp. 109–120. doi:10.1145/2939918.2939923.
76. Montaño-Blacio, M.; Briceño-Sarmiento, J.; Pesántez-Bravo, F. 5G Network Security for IoT Implementation: A Systematic Literature Review. Proceedings of the International Conference on Innovation and Research; Springer: Sangolquí, Ecuador, 2021; pp. 28–40. doi:10.1007/978-3-030-60467-7_3.
77. Rezvy, S.; Luo, Y.; Petridis, M.; Lasebae, A.; Zebin, T. An Efficient Deep Learning Model for Intrusion Classification and Prediction in 5G and IoT Networks. Proceedings of the 53rd Annual Conference on Information Sciences and Systems; IEEE: Baltimore, MD, USA, 2019; pp. 1–6. doi:10.1109/CISS.2019.8693059.
78. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzere, D.; Maliosz, M.; Toka, L. 5G Support for Industrial IoT Applications — Challenges, Solutions, and Research Gaps. *Sensors* **2020**, *20*, 828. doi:10.3390/s20030828.
79. Sharma, A.; Balasubramanian, V.; Jolfaei, A. Security Challenges and Solutions for 5G HetNet. Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications; IEEE: Guangzhou, China, 2020; pp. 1318–1323. doi:10.1109/TrustCom50675.2020.00177.
80. Vassilakis, V.; Chochliouros, I.P.; Spiliopoulou, A.S.; Sfakianakis, E.; Belesioti, M.; Bompetsis, N.; Wilson, M.; Turyagyenda, C.; Dardamanis, A. Security Analysis of Mobile Edge Computing in Virtualized Small Cell Networks. Proceedings of the International Conference on Artificial Intelligence Applications and Innovations; Springer: Thessaloniki, Greece, 2016; pp. 653–665. doi:10.1007/978-3-319-44944-9_58.
81. Mohammed, T.; Albeshri, A.; Katib, I.; Mehmood, R. UbiPriSEQ — Deep Reinforcement Learning to Manage Privacy, Security, Energy, and QoS in 5G IoT HetNets. *Applied Sciences* **2020**, *10*, 7120. doi:10.3390/app10207120.
82. Li, S.; Iqbal, M.; Saxena, N. Future Industry Internet of Things with Zero-Trust Security. *Information Systems Frontiers* **2022**. doi:10.1007/s10796-021-10199-5.
83. Huang, X.; Craig, P.; Lin, H.; Yan, Z. SecIoT: A Security Framework for the Internet of Things. *Security and Communication Networks* **2016**, *9*, 3083–3094. doi:10.1002/sec.1259.
84. Lagkas, T.; Argyriou, V.; Bibi, S.; Sarigiannidis, P. UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors* **2018**, *18*, 4015. doi:10.3390/s18114015.
85. Miloslavskaya, N.; Tolstoy, A. IoTBlockSIEM for Information Security Incident Management in the Internet of Things Ecosystem. *Cluster Computing* **2020**, *23*, 1911–1925. doi:10.1007/s10586-020-03110-5.
86. Mansour, C.; Chasaki, D. Multi-layer Security Mechanism for Networked Embedded Devices. Proceedings of the 11th International Conference on Ubiquitous Computing and Ambient Intelligence; Springer: Philadelphia, PA, USA, 2017; pp. 3–14. doi:10.1007/978-3-319-67585-5_1.
87. Rathee, G.; Iqbal, R.; Waqar, O.; Bashir, A.K. On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities. *IEEE Access* **2021**. doi:10.1109/ACCESS.2021.3061411.
88. Hellaoui, H.; Koudil, M.; Bouabdallah, A. Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach. *IEEE Internet of Things Journal* **2020**, *7*, 6589–6602. doi:10.1109/JIOT.2020.2974618.
89. Bordel, B.; Alcarria, R.; Robles, T.; Iglesias, M.S. Data Authentication and Anonymization in IoT Scenarios and Future 5G Networks Using Chaotic Digital Watermarking. *IEEE Access* **2021**, *9*, 22378–22398. doi:10.1109/ACCESS.2021.3055771.
90. Torroglosa-Garcia, E.M.; Calero, J.M.A.; Bernabe, J.B.; Skarmeta, A. Enabling Roaming Across Heterogeneous IoT Wireless Networks: LoRaWAN Meets 5G. *IEEE Access* **2020**, *8*, 103164–103180. doi:10.1109/ACCESS.2020.2998416.
91. Al-Aqrabi, H.; Johnson, A.P.; Hill, R.; Lane, P.; Alsboui, T. Hardware-Intrinsic Multi-Layer Security: A New Frontier for 5G Enabled IIoT. *Sensors* **2020**, *20*, 1963. doi:10.3390/s20071963.

92. Sharma, V.; Kim, J.; Kwon, S.; You, I.; Chen, H.C. Fuzzy-Based Protocol for Secure Remote Diagnosis of IoT Devices in 5G Networks. Proceedings of the International Conference on Internet of Things as a Service; Springer: Taichun, Taiwan, 2018; pp. 54–63. doi:10.1007/978-3-030-00410-1_8.
93. Azad, M.A.; Bag, S.; Perera, C.; Barhamgi, M.; Hao, F. Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. *IEEE Transactions on Industrial Informatics* **2020**. doi:10.1109/TII.2019.2941724.
94. Shin, S.; Kwon, T. Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 11229–11241. doi:10.1109/ACCESS.2018.2796539.
95. Liu, W.; Wang, X.; Peng, W. Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access* **2020**, *8*, 8754–8767. doi:10.1109/ACCESS.2019.2962912.
96. Khalid, M.; Khokhar, U.; Najam-ul Islam, M. Advance Strong Authentication Strong Integrity (ASASI) Protocol for Low Cost Radio Frequency Identification. Proceedings of the International Conference on Smart Computing and Electronic Enterprise; IEEE: Shah Alam, Malaysia, 2018; pp. 1–6. doi:10.1109/ICSCEE.2018.8538436.
97. Fan, K.; Song, P.; Yang, Y. ULMAP: Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G. *Mobile Information Systems* **2017**, *2017*, 1–7. doi:10.1155/2017/2349149.
98. Fan, K.; Gong, Y.; Liang, C.; Li, H.; Yang, Y. Lightweight and Ultralightweight RFID Mutual Authentication Protocol with Cache in the Reader for IoT in 5G. *Security and Communication Networks* **2016**, *9*, 3095–3104. doi:10.1002/sec.1314.
99. Das, M.L. Privacy and Security Challenges in Internet of Things. Proceedings of the 11th International Conference on Distributed Computing and Internet Technology; Springer: Bhubaneswar, India, 2015; pp. 33–48. doi:10.1007/978-3-319-14977-6_3.
100. Duguma, D.G.; Kim, J.; Lee, S.; Jho, N.S.; Sharma, V.; You, I. A Lightweight D2D Security Protocol with Request-Forecasting for Next-Generation Mobile Networks. *Connection Science* **2022**, *34*, 362–386. doi:10.1080/09540091.2021.2002812.
101. Shin, D.; Yun, K.; Kim, J.; Astillo, P.V.; Kim, J.N.; You, I. A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. *IEEE Access* **2019**, *7*, 142531–142550. doi:10.1109/ACCESS.2019.2943929.
102. Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Shukla, P.K.; Jamal, S.S.; Alharbi, A.R.; Aljaedi, A. Securing 5G-IoT Device Connectivity and Coverage Using Boltzmann Machine Keys Generation. *Mathematical Problems in Engineering* **2021**, *2021*, 1–10. doi:10.1155/2021/2330049.
103. Rawal, B.S.; Peter, A. Introduction of Interstitial Model and a Sumkey to Address the Key Challenges with Blockchain. Proceedings of the IEEE Globecom Workshops; IEEE: Waikoloa, HI, USA, 2019. doi:10.1109/GCWkshps45667.2019.9024692.
104. Ravi, N.; Selvaraj, M.S. TeFENS: Testbed For Experimenting Next-Generation-Network Security. Proceedings of the IEEE 5G World Forum; IEEE: Silicon Valley, CA, USA, 2018; pp. 204–209. doi:10.1109/5GWF.2018.8516708.
105. Wang, K.; Liu, X.; Chen, C.M.; Kumari, S.; Shojafar, M.; Hossain, M.S. Voice-Transfer Attacking on Industrial Voice Control Systems in 5G-Aided IIoT Domain. *IEEE Trans. on Industrial Informatics* **2021**. doi:10.1109/TII.2020.3023677.
106. Szymanski, T.H. Securing the Industrial-Tactile Internet of Things With Deterministic Silicon Photonics Switches. *IEEE Access* **2016**. doi:10.1109/ACCESS.2016.2613512.
107. Deebak, B.; AL-Turjman, F. A Robust and Distributed Architecture for 5G-Enabled Networks in the Smart Blockchain Era. *Computer Communications* **2022**, *181*, 293–308. doi:10.1016/j.comcom.2021.10.015.
108. Vangala, A.; Das, A.K.; Chamola, V.; Korotaev, V.; Rodrigues, J.J.P.C. Security in IoT-Enabled Smart Agriculture: Architecture, Security Solutions and Challenges. *Cluster Computing* **2022**. doi:10.1007/s10586-022-03566-7.
109. Dib, M.; Torabi, S.; Bou-Harb, E.; Assi, C. A Multi-Dimensional Deep Learning Framework for IoT Malware Classification and Family Attribution. *IEEE Transactions on Network and Service Management* **2021**, *18*, 1165–1177. doi:10.1109/TNSM.2021.3075315.
110. Rey, V.; Sánchez Sánchez, P.M.; Huertas Celdrán, A.; Bovet, G. Federated Learning for Malware Detection in IoT Devices. *Computer Networks* **2022**, *204*, 108693. doi:10.1016/j.comnet.2021.108693.
111. Krishnan, P.; Duttagupta, S.; Achuthan, K. SDN/NFV Security Framework for Fog-to-Things Computing Infrastructure. *Software: Practice and Experience* **2020**, *50*, 757–800. doi:10.1002/spe.2761.
112. Lawal, M.A.; Shaikh, R.A.; Hassan, S.R. A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing. *Procedia Computer Science* **2021**, *182*, 13–20. doi:10.1016/j.procs.2021.02.003.

113. Jaiswal, A.; Kumar, S.; Kaiwartya, O.; Kumar, N.; Song, H.; Lloret, J. Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications. *IEEE Systems Journal* **2021**, *15*, 2810–2821. doi:10.1109/JSYST.2020.3036417.
114. Jain, A.; Singh, T.; Sharma, S.K.; Prajapati, V. Implementing Security in IoT Ecosystem Using 5G Network Slicing and Pattern Matched Intrusion Detection System: A Simulation Study. *Interdisciplinary Journal of Information, Knowledge, and Management* **2021**, *16*, 001–038. doi:10.28945/4675.
115. Khan, N.A. PKI-Based Security Enhancement for IoT in 5G Networks. Proceedings of the 3rd International Conference on Inventive Computation and Information Technologies; Springer: Virtual Event, 2022. doi:10.1007/978-981-16-6723-7_16.
116. Lee, H.; Kang, D.; Ryu, J.; Won, D.; Kim, H.; Lee, Y. A Three-Factor Anonymous User Authentication Scheme for Internet of Things Environments. *Journal of Information Security and Applications* **2020**. doi:10.1016/j.jisa.2020.102494.
117. Li, X.; Liu, S.; Wu, F.; Kumari, S.; Rodrigues, J.J.P.C. Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications. *IEEE Internet of Things Journal* **2019**, *6*, 4755–4763. doi:10.1109/JIOT.2018.2874473.
118. Choudhury, H. HashXor: A Lightweight Scheme for Identity Privacy of IoT Devices in 5G Mobile Network. *Computer Networks* **2021**, *186*, 107753. doi:10.1016/j.comnet.2020.107753.
119. Zhang, P.; Sun, H.; Situ, J.; Jiang, C.; Xie, D. Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing. *IEEE Access* **2021**, *9*, 98630–98638. doi:10.1109/ACCESS.2021.3095078.
120. Krundyshev, V.; Kalinin, M. Hybrid Neural Network Framework for Detection of Cyber Attacks at Smart Infrastructures. Proceedings of the 12th International Conference on Security of Information and Networks; ACM: Sochi, Russia, 2019; pp. 1–7. doi:10.1145/3357613.3357623.
121. Lee, Y.; Woo, S.; Lee, J.; Song, Y.; Moon, H.; Lee, D.H. Enhanced Android App-Repackaging Attack on In-Vehicle Network. *Wireless Communications and Mobile Computing* **2019**, *2019*, 1–13. doi:10.1155/2019/5650245.
122. Kang, J.J.; Fahd, K.; Venkatraman, S.; Trujillo-Rasua, R.; Haskell-Dowland, P. Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks. Proceedings of the 29th International Telecommunication Networks and Applications Conference; IEEE: Auckland, New Zealand, 2019; pp. 1–6. doi:10.1109/ITNAC46935.2019.9077977.
123. Zhang, B.; Li, J.; Zheng, X.; Ge, J.; Sun, J. A Blockchain-Based Mobile IoT Network Interconnection Security Trusted Protocol Model. Proceedings of the 11th International Symposium on Cyberspace Safety and Security; Springer: Guangzhou, China, 2019; pp. 372–381. doi:10.1007/978-3-030-37352-8_33.
124. Fu, Y.; Yan, Z.; Cao, J.; Koné, O.; Cao, X. An Automata Based Intrusion Detection Method for Internet of Things. *Mobile Information Systems* **2017**, *2017*, 1–13. doi:10.1155/2017/1750637.
125. Laguduva, V.R.; Katkoori, S.; Karam, R. Machine Learning Attacks and Countermeasures for PUF-based IoT Edge Node Security. *SN Computer Science* **2020**, *1*. doi:10.1007/s42979-020-00303-y.
126. Cheng, X.; Luo, Q.; Pan, Y.; Li, Z.; Zhang, J.; Chen, B. Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT Scenarios Based on Differentially Private Federated Learning. *Security and Communication Networks* **2021**, *2021*, 1–14. doi:10.1155/2021/8814068.
127. Lee, K.; Yim, K. Study on the Transaction Linkage Technique Combined with the Designated Terminal for 5G-Enabled IoT. *Digital Communications and Networks* **2022**, *8*, 124–131. doi:10.1016/j.dcan.2020.12.003.
128. Catania, E.; La Corte, A. IoT Privacy in 5G Networks. Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security; SciTePress: Funchal, Madeira, Portugal, 2018; pp. 123–131. doi:10.5220/0006710501230131.
129. Sankar, S.P.; Subash, T.D.; Vishwanath, N.; Geroge, D.E. Security Improvement in Blockchain Technique Enabled Peer to Peer Network for Beyond 5G and Internet of Things. *Peer-to-Peer Networking and Applications* **2020**, *14*, 392–402. doi:10.1007/s12083-020-00971-w.
130. Baniata, H.; Almobaideen, W.; Kertesz, A. A Privacy Preserving Model for Fog-Enabled MCC Systems Using 5G Connection. Proceedings of the 5th International Conference on Fog and Mobile Edge Computing; IEEE: Paris, France, 2020; pp. 223–230. doi:10.1109/FMEC49853.2020.9144814.
131. Nie, X.; Yang, L.T.; Feng, J.; Zhang, S. Differentially Private Tensor Train Decomposition in Edge-Cloud Computing for SDN-Based Internet of Things. *IEEE Internet of Things Journal* **2020**, *7*, 5695–5705. doi:10.1109/JIOT.2019.2960293.
132. Lu, N.; Du, Q.; Sun, L.; Ren, P. Traffic-Driven Intrusion Detection for Massive MTC Towards 5G Networks. Proceedings of the IEEE Conference on Computer Communications Workshops; IEEE: Honolulu, HI, USA, 2018; pp. 426–431. doi:10.1109/INFCOMW.2018.8406976.

133. Wang, F.; Lu, Y.; Wang, C.; Li, Q. Binary Black-Box Adversarial Attacks with Evolutionary Learning Against IoT Malware Detection. *Wireless Communications and Mobile Computing* **2021**. doi:10.1155/2021/8736946.
134. Celik, A.; Tetzner, J.; Sinha, K.; Matta, J. 5G Device-to-Device Communication Security and Multipath Routing Solutions. *Applied Network Science* **2019**, *4*, 1–24. doi:10.1007/s41109-019-0220-6.
135. Tsimenidis, S.; Lagkas, T.; Rantos, K. Deep Learning in IoT Intrusion Detection. *Journal of Network and Systems Management* **2022**. doi:10.1007/s10922-021-09621-9.
136. Sicari, S.; Rizzardi, A.; Coen-Porisini, A. 5G In the Internet of Things Era: An Overview on Security and Privacy Challenges. *Computer Networks* **2020**, *179*, 107345. doi:10.1016/j.comnet.2020.107345.
137. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors* **2021**. doi:10.3390/s21113901.
138. Ahmad, A.; Bhushan, B.; Sharma, N.; Kaushik, I.; Arora, S. Importunity & Evolution of IoT for 5G. Proc. of the Intl. Conf. on Comm. Systems and Network Technologies; IEEE: Gwalior, India, 2020. doi:10.1109/CSNT48778.2020.9115768.
139. Pahlevanzadeh, B.; Koleini, S.; Fadilah, S.I. Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions. Proc. of the 2nd Intl. Conference on Advances in Cyber Security; Springer: Penang, Malaysia, 2021. doi:10.1007/978-981-33-6835-4_18.
140. Sallam, S.; Beheshti, B.D. A Survey on Lightweight Cryptographic Algorithms. TENCON 2018 - 2018 IEEE Region 10 Conference; IEEE: Jeju, South Korea, 2018; pp. 1784–1789. doi:10.1109/TENCON.2018.8650352.
141. Zhang, S.; Wang, Y.; Zhou, W. Towards Secure 5G networks: A Survey. *Computer Networks* **2019**, *162*, 106871. doi:10.1016/j.comnet.2019.106871.
142. Atharvan, G.; Koolikkara Madom Krishnamoorthy, S.; Dua, A.; Gupta, S. A Way Forward Towards a Technology-Driven Development of Industry 4.0 Using Big Data Analytics in 5G-Enabled IIoT. *International Journal of Communication Systems* **2022**, *35*, e5014. doi:10.1002/dac.5014.
143. Liang, W.; Ji, N. Privacy Challenges of IoT-Based Blockchain: A Systematic Review. *Cluster Computing* **2022**, *25*. doi:10.1007/s10586-021-03260-0.
144. Sathish, C.; Rubavathi, C.Y. A survey on Blockchain Mechanisms (BCM) Based on Internet of Things (IoT) Applications. *Multimedia Tools and Applications* **2022**, *81*, 33419–33458. doi:10.1007/s11042-022-12784-5.
145. Hewa, T.M.; Kalla, A.; Nag, A.; Ylianttila, M.E.; Liyanage, M. Blockchain for 5G and IoT: Opportunities and Challenges. Proceedings of the 8th International Conference on Communications and Networking; IEEE: Hammamet, Tunisia, 2020; pp. 1–8. doi:10.1109/ComNet47917.2020.9306082.
146. Rath, D.K.; Kumar, A. A Primer on Internet of Things Ecosystem and 5G Networks. Proceedings of the International Conference on Information Technology; IEEE: Bhubaneswar, India, 2018. doi:10.1109/ICIT.2018.00055.
147. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal* **2019**. doi:10.1109/JIOT.2019.2927379.
148. Tan, Y.a.; Zhang, X.; Sharif, K.; Liang, C.; Zhang, Q.; Li, Y. Covert Timing Channels for IoT over Mobile Networks. *IEEE Wireless Communications* **2018**, *25*, 38–44. doi:10.1109/MWC.2017.1800062.
149. Akhunzada, A.; Islam, S.u.; Zeadally, S. Securing Cyberspace of Future Smart Cities with 5G Technologies. *IEEE Network* **2020**. doi:10.1109/MNET.001.1900559.
150. Gupta, S.; Parne, B.L.; Chaudhari, N.S. Security Vulnerabilities in Handover Authentication Mechanism of 5G Network. Proc. of the Intl. Conf. on Secure Cyber Computing and Communication; IEEE: Jalandhar, India, 2018. doi:10.1109/ICSCCC.2018.8703355.
151. Ziani, A.; Medouri, A. A Survey of Security and Privacy for 5G Networks. In *Emerging Trends in ICT for Sustainable Development*; Springer: Cham, Switzerland, 2021; pp. 201–208. doi:10.1007/978-3-030-53440-0_22.
152. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 170–195. doi:10.1109/COMST.2019.2951818.
153. Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE IoT Journal* **2020**. doi:10.1109/JIOT.2019.2948888.
154. Li, S.; Xu, L.D.; Zhao, S. 5G Internet of Things: A Survey. *Journal of Industrial Information Integration* **2018**, *10*, 1–9. doi:10.1016/j.jii.2018.01.005.

 doi:10.20944/preprints202311.0565.v1