International Journal of Information Security (2024) 23:2827–2879
https://doi.org/10.1007/s10207-024-00865-5

REGULAR CONTRIBUTION

IoT cybersecurity in 5G and beyond: a systematic literature review

Sandeep Pirbhulal[1] · Sabarathinam Chockalingam[1,2] · Ankur Shukla[1,2] · Habtamu Abie[1]

Accepted: 4 May 2024 / Published online: 28 May 2024

Abstract

The 5th generation (5G) and beyond use Internet of Things (IoT) to offer the feature of remote monitoring for different applications such as transportation, healthcare, and energy. There are several advantages of 5G and beyond for IoT applications like high speed and low latency. However, they are prone to cybersecurity threats due to networks softwarization and virtualization, thus raising additional security challenges and complexities. In this paper, we conducted a systematic literature review (SLR) of cybersecurity for 5G and beyond-enabled IoT. By developing a taxonomy to classify and characterize existing research, we identified and analyzed strategies, key patterns, mechanisms, performance evaluation, validation parameters and challenges of cybersecurity and resilience for 5G and beyond-enabled IoT in existing studies. We used "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)" recommendations for this SLR. Through our search in scientific databases, 4449 records published between 2017 and 2023 were initially identified, which were then reduced to 558 records after title and abstract screening to be considered for the eligibility check process. After screening the full-text, 79 articles were finalized for thorough analysis. The findings of this study suggest that 35% of the included studies focus on authentication and access control as security aspects, 59% studies are based on combination of both network layer and application layer as main operation layer, and 34% of the included studies use real-time implementation for validation purpose while the remaining studies utilize simulation or theoretical analysis. Our SLR also highlights open research challenges of 5G and beyond-enabled IoT cybersecurity and suggests a tentative solution for each challenge, which can be a focus of future research. Finally, key limitations of our SLR and threats to validity are addressed.

Keywords Cybersecurity · IoT · Resilience · 5G and beyond

1 Introduction

1.1 Overview

Internet of Things (IoT) has received a lot of research attention over the last few decades in addition to being a most important emerging technology [1–3]. A physical perception layer of IoT observes the physical environment through sensors, whereas a network layer connects to other smart things and processes observed data [3]. Finally, an application layer provides a user with application-specific services. With the emergence of IoT, numerous challenges corresponding to personal, businesses, and even governments around the world are addressed. Examples of IoT applications include energy conservation, health and fitness, home automation, pollution control, smart agriculture, smart transport, and supply chain and logistics [2, 3]. IoT is used by over 80% of organizations today to solve business problems. In the future, IoT risks are expected to increase significantly across a wide range of organizations. The number of global IoT connections continues to grow exponentially and will reach 25 billion by 2025. However, security is one of the major concerns of the IoT devices. An IoT-based attack has been identified by 20% of these organizations within the past three years. Less than one-third of Chief Information Security Officers believe that

Sandeep Pirbhulal, Sabarathinam Chockalingam and Ankur Shukla have contributed equally to this work.

✉ Sandeep Pirbhulal
sandeep@nr.no

✉ Sabarathinam Chockalingam
Sabarathinam.Chockalingam@ife.no

✉ Ankur Shukla
Ankur.Shukla@ife.no

[1] Norwegian Computing Center, Blindern, PO Box 114, 0314 Oslo, Norway

[2] Department of Risk and Security, Institute for Energy Technology, 1777 Halden, Norway

there is a reliable risk assessment and mitigation for information security of IoT devices [4]. On the other hand, the tools, entry points, and vulnerabilities available to threat actors have expanded significantly over the past few years. Thus, adversaries might certainly use ever-increasing tactics, techniques, and procedures (TTPs) to attack 5G [5].

The 4th generation (4G) technology is a widely used communication technology for IoT [4, 5]. The next generation of IoT devices demand some of the following key requirements for communication technology: decreased latency, improved data rate, improved security, and massive connectivity [4, 5]. Importantly, the 5th generation (5G) and 6th generation (6G) technologies possess characteristics to address the above-mentioned key requirements for communication technology of next generation IoT devices [6–10]. Some emerging applications of 6G-enabled IoT include healthcare, vehicular, satellite, and industrial [10].

Even though IoT-based applications improve human life, they are also susceptible to cyber-attacks in addition to random failures [11–13]. Therefore, security and resilience of IoT applications is essential in ensuring the proper functioning of our society and businesses [14]. There are different studies which investigated security and/or resilience aspects of 5G and beyond-enabled IoT [15–99]. Syalim et al. analyzed six different existing ID-Based Aggregate Signature (IBAS) schemes [26]. They concluded that the schemes proposed by Gentry et al. [100] and Yuan et al. [101] as the most suitable ones for 5G-enabled massive IoT. Thantharate et al. also explored the security challenges in the 5G network [30]. They proposed a robust network slicing framework that prevents security attacks [30].

1.2 Related work

There are different Systematic Literature Reviews (SLRs) conducted within IoT in general [102, 103], role of IoT in specific domains like agriculture [104, 105], supply chain management [106, 107], healthcare [108, 109], 5G-enabled IoT [5], 6G-enabled IoT [8, 10] and 5G and beyond-enabled IoT [110–117]. Furthermore, there are also SLRs conducted with a focus on security and resilience aspects of IoT [114–121].

Madakam et al. [102] reviewed the definitions, architectures, and technologies of IoT. Li et al. surveyed recent advancements in IoT from the viewpoint of enabling technologies [103]. They highlighted open problems and challenges related to IoT, like security and privacy protection. Farooq et al. identified 67 studies related to IoT in the agriculture domain [104]. They also compared the identified studies in terms of approaches used, sub-application domains within agriculture based on communication protocols, standards in agriculture, and policies in different countries [104]. In addition, Ben-Daya et al. identified studies related to IoT in the supply chain management domain [106]. They analyzed the role of IoT in supply chain management and their impact on delivery processes and delivery decisions and models [106].

Numerous studies have been conducted in recent times to explore various aspects of 5G, 6G, and IoT applications, including their main drivers, requirements, architecture, technologies, design trends, opportunities, and open challenges. For instance, Li et al. reviewed studies related to 5G-enabled IoT and analyzed requirements, key enabling technologies, and research challenges and future trends of 5G-enabled IoT [5]. Mao et al. [120] conducted a survey on security and privacy concerns at the edge of 6G networks. In their survey, Mahmood et al. [122] explored 5G architecture, transformative technologies, and recent design trends that can enable large-scale wireless Industrial Internet of Things (IIoT) deployments. Guo et al. surveyed studies related to 6G-enabled IoT and summarized key drivers and requirements, technologies, applications, and open issues of 6G-enabled IoT [8]. Qadir et al. [111] examined recent advancements, use cases, and open challenges of 6G IoT, while Kim [112] discussed the primary drivers of 6G technology, current research, and potential applications of 6G to IoT technologies and service areas. However, only a few of these studies have focused on both 5G and 6G networks [113, 117, 123], while most of them addressed only one and overlooked the broader impact of the other.

On the other hand, there are only a few papers that focused on security concerns of 5G/6G and IoT networks [114, 116, 117, 120, 121, 123]. However, these papers mainly focused on specific components of IoT devices such as the network edge [120], physical layer [123], or particular applications like low-power IoT [117], intrusion detection systems [114], digital forensics [116], and secure network management using blockchain technology [121]. The details of the existing surveys are compared with the main focus, coverage, and limitations of our SLR in Table 1.

1.3 Our contributions

As we previously mentioned, there exist studies which focus on the security and/or resilience aspects of 5G and beyond-enabled IoT. However, the existing SLRs and surveys lack in providing an overview of cybersecurity and resilience for 5G and beyond-enabled IoT applications. Also, current studies do not elaborate in detail about the techniques that are developed for ensuring 5G and beyond-enabled IoT security and resilience. Therefore, this research aims to address these gaps by addressing the Research Questions (RQs) that will be discussed in Sect. 3. The main contributions of this study are:

- A systematic review of the state-of-the-art of cybersecurity and resilience for 5G and beyond-enabled IoT.

Table 1 Comparative analysis of existing surveys

S. no.	Paper [References]	Main focus	5G	6G	IoT	Cybersecurity	Comment
1	Mao et al. [120]	Focused on security and privacy on the 6G network edge	×	✓	×	✓	This paper does not address the impact of the 5G network and focuses only on network edge
2	Mahmood et al. [122]	Reviewed the 5G architecture, transformative technologies, and recent design trends, in the context of enabling large-scale wireless IIoT deployments	✓	×	✓	×	This paper does not address the impact of the 6G network, and it does not provide comprehensive cybersecurity coverage
3	Guo et al. [8]	Discussed 6G-enabled massive IoT considering drivers and requirements, visions, breakthrough technologies, network architecture	×	✓	✓	×	This paper does not address the impact of the 5G network, and it does not provide comprehensive cybersecurity coverage
4	Mahmood et al. [110]	Focused on the convergence of 6G and IoT to explore emerging opportunities in IoT networks and applications	×	✓	✓	×	This paper does not address the impact of the 5G network, and it does not provide comprehensive cybersecurity coverage
5	Qadir et al. [111]	Reviewed the recent advancements, use cases, and open challenges of 6G IoT	×	✓	✓	×	This paper neither addresses the impact of the 5G network nor provides comprehensive cybersecurity coverage
6	Kim [112]	Discussed the main drivers of 6G technology, along with current 6G research and the potential applications of 6G to IoT technologies and service areas	×	✓	✓	×	This paper discusses applications of 6G to IoT technologies and does not cover the impact of 5G or cybersecurity comprehensively
7	Hakak et al. [113]	Explored advancements in autonomous vehicles, focusing on automation levels, enabling technologies, and the essential role of 5G networks	✓	✓	×	×	This paper is limited to autonomous vehicles and does not cover cybersecurity comprehensively
8	Irram et al. [123]	Mainly considered the physical layer security for beyond 5G/6G networks	✓	✓	×	✓	This paper is limited to the security of the physical layer
9	Jahid et al. [121]	Focused on IoT and blockchain convergence for intelligent distribution in IIoT and 6G network technical model: potential, opportunities, challenges, and research roadmap	×	✓	✓	✓	This paper focuses only on blockchain technology in the context of security. It addresses 6G and IoT but not 5G
10	Alotaibi et al. [114]	Explored the security aspects of massive IoT towards 6G networks, specifically in regards to IDS	×	✓	✓	✓	This paper does not consider the 5G network and mainly focuses on IDS systems
11	Bodkhe et al. [115]	Addressed the potential of blockchain technology to provide secure network management for the IoTs	×	✓	✓	✓	This paper does not consider the 5G network and mainly focuses on blockchain technology and network management for IoT systems

Table 1 (continued)

S. no.	Paper [References]	Main focus	5G	6G	IoT	Cybersecurity	Comment
12	Akinbi [116]	Discussed the digital forensic challenges and associated issues within 6G IoT networks	×	✓	✓	✓	This paper does not consider the 5G networks and focuses only on the digital forensic challenges and related issues
13	Cook et al. [117]	Focused on security and privacy for low power IoT devices on 5G and beyond networks	✓	✓	✓	✓	This paper does not focus on cybersecurity comprehensively but is mainly limited to privacy of low-power personal IoT devices and confidentiality of the data. Also, their search query to find the relevant records from scientific databases is different in addition to RQs and comparison criteria for detailed analysis compared to our SLR
14	Our SLR	Focused on a systematic literature review of cybersecurity challenges, security considerations, standards, methods, focused layers, application domains, open challenges, and tentative solutions for IoT cybersecurity in 5G and beyond	✓	✓	✓	✓	This paper aims to systematically and comprehensively review IoT cybersecurity in 5G and beyond

✓: This aspect is *addressed in the study*, ×: This aspect is *not addressed in the study*

- A taxonomy for 5G and beyond-enabled IoT cybersecurity based on included studies.
- Identification and comparative analysis of strategies, mechanisms, performance evaluation, and validation parameters for cybersecurity and resilience for 5G and beyond-enabled IoT.
- Categorize open challenges and propose their tentative solutions.

1.4 Structure

The rest of this paper is structured as follows: Sect. 2 provides a background on IoT and 5G and beyond and their security challenges followed by the research methodology including limitations and threat to validity of our SLR in Sect. 3. Section 4 describes the findings from the comparative analysis of the included studies based on security considerations and standards followed by the discussion on security methods and tools in Sect. 5. Section 6 describes the application domains and focused layers of the included studies. The open research challenges and tentative solutions proposed are elaborated in Sect. 7. Conclusions and future works are described in Sect. 8.

2 Background

In contrast with 1G to 3G, 4G networks facilitate machine-to-machine (M2M) communication and establish integration with other networks through IoT, which introduces different vulnerabilities and easy accessibility to attackers using core network servers [124]. 1G and 2G networks were susceptible to single infrastructure attacks, whereas cross infrastructure attacks were common for 3G and 4G networks. Main security threats for 1G, 2G, 3G were eavesdropping, brute force attacks, network congestion attacks, respectively. In the transition from 1 to 4G, different security measures have been introduced [124, 125]. However, 4G networks had several other security issues than 3G due to their high connectivity with the internet and IoT. Some of key threats for 4G are user privacy, unsecured radio communication, lack of protection in network control, and security architecture limitations [126]. The migration to the 5G and beyond brings several

security gaps and new risks. This necessitates updated strategies and policies for ensuring security. 63% of enterprises deploying IoT services encounter more security challenges since they did not update their security policies as per new emerging technologies [126].

2.1 5G technology and security challenges

5G is the fifth generation of communication technology that connects everyone and everything together virtually. 5G is more evolved than 4G mobile communication, comprising protocol, speed, and network configurations. Network Function Virtualisation (NFV) and Software-Defined Networking (SDN) concepts have been introduced in 5G to provide lower latency, higher network capacity, greater availability, better connectivity, enhanced bandwidth, higher speed and throughput, and uniform user experiences [127, 128]. 5G networks combine licensed and unlicensed wireless technologies to support converged heterogeneous networks. This makes more bandwidth available to users.

The advantages of 5G are enormous, but the use of SDN and NFV come with additional security challenges and complexities in different scenarios. 5G needs robust security solutions since it combines several real-time applications with communication networks. The essential security challenges in 5G are investigated and pinpointed in [129]. The main security challenges in 5G are as follows [129, 130]:

- *User plane integrity:* The user plane carries the end-user's data. Protecting the integrity of the user plane is essential for smooth communications between 5G devices and networks.
- *Flash network traffic and signaling storms:* In 5G networks, several devices are connected, which may yield flash network traffic by compromising vulnerable devices. In an environment, where a huge number of devices are connected, it may pose a considerable threat to the 5G signaling network.
- *Roaming security:* Secure roaming in 5G networks is important for mobile operators to protect subscribers and network infrastructures.
- *Decentralized security:* 5G communication based on blockchain technology requires more traffic routing points. Thus, it will be important to create trustworthy communication.
- *Denial of Service (DoS) attacks on end-user devices and infrastructures:* DoS attacks could make devices or networks or infrastructures inaccessible to the envisioned users by flooding the target with traffic.
- *Compatibility:* 5G devices will have more bandwidth requirements. Thus, it may have high pressure on the current security monitoring tools to process in a smooth manner.
- *IoT device security:* Many IoT devices are designed in a way that they do not have built-in security. Therefore, device security might be considered separately.
- *Lack of early encryption in connection process:* Receiving unciphered information of the 5G device by an attacker allows it to launch cyber-attacks.

Due to the introduction of virtualization and softwarization in addition to adoption of open-source software in 5G, there can be many other security requirements for NFVs including access control, secure communication within virtual and physical systems. It is essential to address the security issues and to focus on instilling more robust security and privacy in 5G NFV systems in the following areas [131]:

- *Virtualisation or Containerisation:* SDNs' poses major security challenges because they are susceptible to attacks such as forwarding device attacks, control plane threats, API vulnerabilities, counterfeit traffic flows and more.
- *Orchestration and Management:* Security challenges such as vulnerabilities within orchestration protocols, Management and Orchestration (MANO) single point of failure, orchestration compromise and policy violations can occur due to a lack of consistency on how to manage and orchestrate the network services.
- *Administration and Access Control:* 5G NFV network architecture offers openness and programmability relying on the expanded use of APIs. Network functions and sensitive parameters with inaccurate access control rules may be exposed due to improperly designed or configured API.
- *New and Legacy Technologies:* The communication between physical and virtual environments in 5G may also raise several security challenges at management and orchestration layers which need to be considered.
- *Adoption of Open Source:* Another security challenge related to the use of lower cost, commercial off-the-shelf (COTS) hardware for network functions based on NFV technologies which may impact security and performance.
- *Supply Chain:* The 5G NFV supply chain is susceptible to risks such as malicious software and hardware, counterfeit components, poor designs, manufacturing processes, and maintenance procedures.
- *Lawful Interception (LI):* Another security challenge is securing and hiding LI functions from other functions in an NFV environment.

The security threats in 5G [131] can be classified layer wise such as core network, radio access, network virtualisation or generic infrastructure component as follows:

- *Core Network Threats:* These threats are related to SDN, NVF, NS and MANO, and lie in the categories

of Nefarious Activity/Abuse (NAA) and Eavesdropping/Interception/Hijacking (EIH).
- *Access Network Threats:* These threats are related to radio access technology, radio access network and non-3GPP access technologies, and lie in the categories of EIH.
- *Multi-edge Computing Threats:* These threats are also related to NAA and EIH categories but mostly associated with components located at the edge of the network.
- *Virtualisation Threats:* These threats are associated with NFVs and VNFs operations and functions.
- *Physical Infrastructure Threats:* These threats affect IT infrastructures that support the network and lie in the categories of physical attacks, damage or loss of equipment, disruption of services, and disasters.
- *Generic Threats:* These threats such as Denial of Service (DoS) typically affect any ICT system or network.
- *SDN Threats:* These threats are related to the softwarization functions that are the backbone of 5G.

2.2 5G and beyond technology and security challenges

The commercial deployment of 5G is underway worldwide, but academia and industry have already started focusing on 5G and beyond to meet the expectation of ICT in 2030. There are ongoing discussions within the wireless community about whether 5G and beyond, i.e., 6G is needed or not. More specifically, whether counting generations should stop at 5 or not [132, 133]. Some studies have indicated that 5G may not fulfill the market requirements in the post-2030 era due to several issues, including deployment costs, security, reliability and hardware complexity, so 6G has the potential to fill the gap between 5G and the market demands [134–138]. As per a study [135], 6G communication KPI targets include 1 Tbps peak data rates, 0.1 ms radio latency, a 20-year battery life, 100/m^3 device connectivity, an increase in traffic of 1000 times, 10 times increase in energy efficiency, 1 outage out of 1 million, and a precision of 10 cm indoors and 1 m outdoors. It is expected that 6G will revolutionize society by using modern technologies such as quantum computing, molecular communication, AI, blockchain, teraHertz technology, and edge computing. However, 6G is prone to complex security risks. The main challenges of 6G security are [130, 139–141]:

- *Security Function Virtualization (SFV)*: In place of NFV, SFV is introduced which offers better security measures, but it brings up more security management and security overheads which need proper attention.
- *Self-evolving network*: 6G came up with the concept of self-evolving network. It is important that 6G networks must be able to deal with varying security threats by offering adaptive protection measures.
- *Automation of vulnerabilities management*: The static vulnerabilities management will not be sufficient for 6G networks due to their self-sustenance and evolution nature. The dynamic and real-time vulnerabilities management will be key for 6G.
- *Privacy Preserving in Edge*: Edge computing is the main pillar of 5G and beyond, thus it is required to safeguard the edge device data privacy to avoid potential threats.
- *AI security*: using AI in 5G and beyond can be a double-edged sword such as an attacker may alter the training dataset or manipulate the testing result, which may give inaccurate models.
- *Secure quantum communication*: Secure quantum key distribution is vital for 6G so that only valid users can get keys to get into the infrastructure.

2.3 5G and beyond-enabled IoT

The advance in wireless technology promises new groundbreaking capabilities and unlocks the potential of IoT technologies. The 5G and beyond network is set to enhance IoT devices' performance, availability, and connectivity by using THz communication, edge intelligence and distributed AI. 5G and beyond technology can significantly expand the Industrial Internet of Things (IIoT) capability, such as factory vehicles, industrial robots, and wearable technologies, which cannot be achieved with the current technology. However, IoT applications based on modern wireless communication require a high level of security and reliability due to more openness in their architecture [4]. IoT is enormously complex to deploy in large-scale deployment in critical sectors because of data privacy and security challenges [142, 143].

The 5G and beyond-enabled IoT communications environment faces some conventional and new security, privacy, and other challenges. Along with the main security challenges identified in Sects. 2.1 and 2.2, the followings are additional issues for IoT security in context of 5G and beyond [144, 145]:

- *Efficiency of Security Protocols*: 5G and beyond-enabled IoT networks contain devices with restricted computational capability, fixed storage, and tiny battery size. Thus, developing efficient security protocols that could provide a balance between resource consumption and security is one of the critical challenges in 5G and beyond-enabled IoT.
- *Heterogeneity of End-users' Devices:* In 5G and beyond-enabled IoT, different types of devices, including servers, mobile devices, and other digital types of equipment, are used with varying communication protocols, storage, and capacity. Thus, designing heterogeneous security

protocols will be vital to deal with different devices, technologies, and mechanisms.
- *Data Privacy and Data Security*: Data privacy and security are obligatory conditions for 5G and beyond-enabled IoT so that sensitive information is not leaked for illegal purposes. Since various users are communicating with IoT via cloud and open-source software, it is essential that authorized users get their respective data.
- *Optimal Access Control*: Another key challenge is to provide optimal access control to the 5G and beyond-IoT applications so that only valid users can access the critical infrastructures.
- *Effective Authentication:* IoT devices with 5G and beyond capabilities must have efficient authentication processes to guarantee a trustworthy environment. Blockchain-based trust execution environment development ensures a unique identity to be given to each device to increase trust level in critical sectors.

3 Study design

The study design of this SLR followed the recommendations of the PRISMA statement [146], and F. Weidt et al. [147] guidelines to conduct a systematic review.

3.1 Research questions (RQs)

A total of six RQs are addressed in this SLR:

RQ1. What are the security/resilience aspects considered for ensuring end-to-end security/resilience in 5G and beyond-enabled IoT?

RQ2. What are the current techniques/methods/tools that are developed for ensuring 5G and beyond-enabled IoT security and resilience? What are the underlying approaches used for this development?

RQ3. What are the security standards and guidelines used in 5G and beyond-enabled IoT?

RQ4. What are the application domains, development lifecycle phases and operational layers, and corresponding security goals addressed in each application domain of 5G and beyond-enabled IoT security?

RQ5. What are the performance evaluation metrics of developed techniques/mechanisms/tools?

RQ6. What are the validation approaches used in the development of identified techniques/mechanisms/tools? How are they validated?

3.2 Records searching process

The following search query is used to conduct systematic searches from different scientific databases to identify articles on 5G and beyond-enabled IoT cybersecurity/resilience [147].

("5G" OR "6G") AND ("IoT" OR "internet of things") AND ("security" OR "cybersecurity" OR "cyber") AND ("resilience" OR "resilient")

Note: A few databases only accept eight logical operators (For example: Science Direct). Therefore, in our search query, only eight operators are included.

3.3 Exclusion and inclusion criteria

Exclusion Criteria for our SLR are:

- studies that have not emphasized on development of cybersecurity or resilience for 5G and beyond-enabled IoT applications were excluded.
- studies that develop an approach only for 5G security/resilience or IoT security/resilience were excluded.
- studies that merely provide basic overview of 5G and beyond-enabled IoT applications were excluded.

Inclusion criteria for our SLR are:

- Must be published in a journal/conference indexed in databases.
- Published between January 2017 and November 2023. The rationale behind this range is that there are not many articles before 2017 since 5G technology was not mature at that point and the search study was conducted in 2021 and then updated in November 2023.
- Designed or proposed an approach for cybersecurity or resilience of 5G and beyond-enabled IoT applications.
- Scientific databases are included based on [147]. These scientific databases are extensively used for searching articles in the field of computer science and technology.

Figure 1 shows that 4449 papers published between 2017 and 2023 were initially recognized based on the search query process. Moreover, after deleting duplicates and performing abstract/title/keywords screening and then full screening based on the exclusion and inclusion criteria, only 79 articles are included for detailed analysis.

3.4 Taxonomy

Figure 2 outlines our taxonomy to assist us in classifying the included studies related to 5G and beyond-enabled IoT

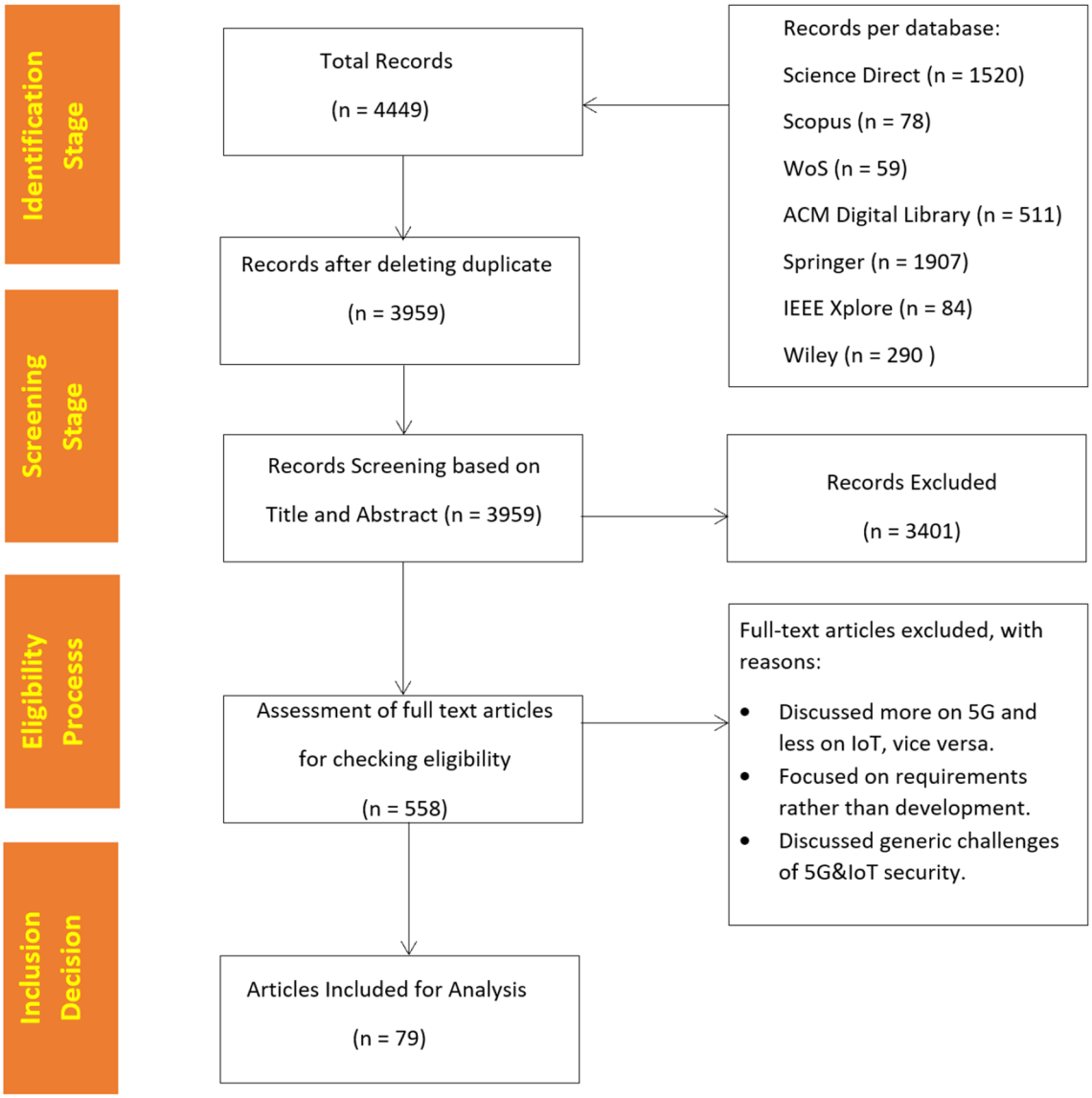

Fig. 1 An overview of literature screening process

cybersecurity. The application of the developed taxonomy is also described in Sects. 4, 5, and 6.

3.5 Limitations and threats to validity

This section highlights limitations of our SLR which mainly corresponds to completeness and publication bias. In general, this SLR followed the PRISMA process, which in turn helped to minimize/reduce the threats to the validity of our study. In this section, we also discuss threats to the validity of our study, and even steps taken to minimize or mitigate them in some cases.

a. *Completeness* The articles for in-depth analysis are identified through selected seven different scientific databases. These scientific databases are high-quality and well-known (as elaborated in Sect. 3). Although we cannot completely rule out the existence of other articles that fulfill our inclusion criteria from other scientific databases, the review methodology that we adopted helped to ensure the acceptable level of completeness in the selection of these articles. Furthermore, the choice of our scientific databases is determined by the nature of our topic area. These scientific databases are extensively used for searching articles in the field of computer science and technology [147]
Furthermore, this SLR includes the studies, which are written in the English language. This means that the studies on *"5G and beyond-enabled IoT applications", which are* written in other languages are not considered. Finally,

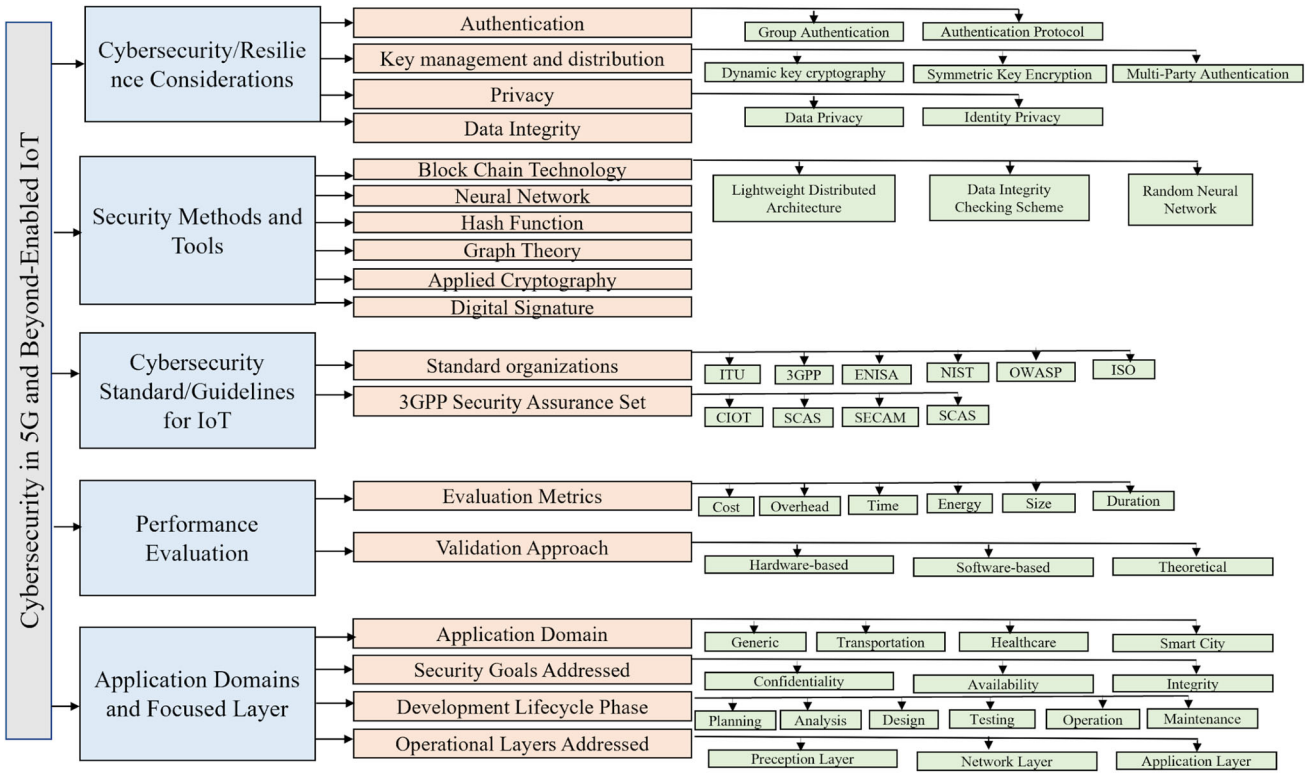

Fig. 2 Taxonomy for 5G and beyond-enabled IoT cybersecurity

there might be some studies which are not publicly available, due to confidentiality and privacy issues.

b. *Publication Bias* We relied on published studies in scientific literature and did not consider unpublished work, findings presented in books and at conferences. The published studies in scientific literature might only discuss positive aspects/results, while negative or controversial aspects/results might not be published. It is not possible to completely remove this bias. However, in order to address this limitation to some extent, we have a dedicated section on open challenges and tentative proposed solutions, which mainly focus on the current open challenges in this area of *"5G and beyond-enabled IoT applications"*.

We also consider construct, internal, and external threats to validity.

a. *Construct Validity* Construct validity assesses whether the SLR represents the degree to which it measures what it asserts. Our first threat is the search query's phrasing. Scientific databases are robust tools to conduct literature search. However, they are also sensitive to a search query's phrasing, where even the slightest change of keywords can lead to very different search results. The completeness of the search strings is difficult to determine because it is based on randomized controlled trials. However, the search query which we used in this paper is appropriately derived from our research questions and has been thoroughly discussed among the authors. We also generated a search strategy where we conducted trial search queries using different combinations of search terms and checked the trial search queries against some already known studies.

Our second threat corresponds to the selection of primary studies especially with selection bias in specific. We minimized this selection bias through defining study selection criteria (i.e., inclusion and exclusion criteria), which were also discussed among the co-authors to ensure the quality of the defined criteria.

b. *Internal Validity* Internal validity shows the incomplete relationship between results, which may lead to structural errors. Subjectivity bias could be one of our internal threats to validity especially during the study selection and data extraction process. However, we have minimized it by including random quality controls mainly during the study selection and data extraction process.

In this study, the search and screening process results in a number of studies considering different technologies in different domains. There are differences between these studies regarding architecture, mechanisms, deployment

process, and frameworks. It is therefore almost impossible to compare all the aspects across the included studies. Therefore, we defined and used criteria, where it is comparable and can lead to meaningful results corresponding to our RQs.

c. *External Validity* Typically, the validity of SLR results heavily depend on the external validity of the included studies. We attempted to minimize or mitigate this issue to some extent by adopting conservative exclusion criteria, excluding studies that have not emphasized on the development of cybersecurity or resilience for 5G and beyond-enabled IoT applications, development of an approach only for 5G security/resilience or IoT security/resilience, and merely provides basic information or theoretical analysis.

In this study, we focused on cybersecurity for 5G and beyond-enabled IoT applications only since, based on findings, it is anticipated to carry out developing tools or models in this research direction. However, cybersecurity is a substantial domain, it may be applied in fields other than 5G and beyond-enabled IoT, but it was not considered in this SLR.

4 Security considerations and standards

In this section, we discuss cybersecurity aspects and standards. Table 2 elaborates which security/resilience aspects are considered for ensuring end-to-end security/resilience in 5G and beyond-enabled IoT applications.

4.1 Security considerations

The different aspects of security and resilience in the context of 5G and beyond-enabled IoT are illustrated in Fig. 3 and Table 2 (RQ 1). As observed in this table, an emphasis is placed by most researchers on authentication [15, 16, 19, 21, 26, 29, 34, 45, 49, 53, 57–60, 65, 68, 79, 81, 84, 85, 89, 91, 93, 98]. Furthermore, Table 2 also covers a wide range of other aspects, such as dynamic key cryptography [15], key agreement [16, 45, 49, 57, 68, 85], key-secrecy [56], key exposure restriction [17], aggregate signature [26], multiparty authentication [34], multi-factor authentication [53, 89], mutual authentication [68], group authentication [26], cryptography [92], and access control [21].

Furthermore, the studies explore various aspects of security such as data security [66, 67, 73, 74, 94], data integrity [20, 22, 65, 71], privacy [17, 18, 35, 36, 43, 66, 87, 93] including identity management [70], security resilience [24, 27, 32, 47, 54, 75, 95], network security [28, 30, 37, 38, 40, 42, 82] including intrusion detection [28, 40], network slicing security [30, 31], forensics security [76], security threat detection and prevention including intrusion detection [80, 86], anomaly detection [63], botnet detection [61], malware detection [55], attack prevention [48], self-protection system [83], and security moving targets [90]. There is also some focus on security and risk management including risk management [22], trust management [96], and threat modeling [97]. Other aspects considered in this paper are decentralized security (adversarial effects) [23], security vulnerabilities [25, 44], security architecture [39], and mobile system security [46].

4.2 Security standards

The purpose of this section is to analyze the security policies, standards, and best practices for 5G and beyond-enabled IoT. Identifying and implementing appropriate cybersecurity standards and best practices can aid organizations in protecting their systems and data from cyber threats. Security standards lay the foundation for cybersecurity strategies and help organizations to determine what their needs are. There have been several standards, specifications, and guidelines developed to ensure that 5G networks and IoT services are deployed, operated, and used safely by ITU, 3GPP, ENISA, NIST, OWASP, and ISO ETSI, as shown in Tables 3 and 4. However, these standards, specifications, and guidelines either focus on 5G security or IoT security and do not provide security recommendations for 5G and beyond-enabled IoT. As 6G is predicted to be deployed around 2030 [63], 6G standards are expected to be rolled out shortly after that. However, some researchers have begun investigating the architecture, security, privacy, and trust requirements of 6G technology and its challenges [148–151]. On the other hand, standardization of 5G is expected to advance rapidly soon.

A focus group FG IMT-2020 has been created by the International Telecommunication Union (ITU) to identify shortcomings in wireless standards for those improvements that are needed in the development of IMT (International Mobile Telecommunications) for 2020 and 5G development beyond that. A 3GPP consortium (3rd Generation Partnership Project) was built, which designed the 3G and 4G standards and is currently developing the 5G standard, has already defined the 5G security architecture [16]. The 3GPP has defined three broad services of 5G under ITU-R (Radiocommunication Sector), which are eMBB (enhanced Mobile Broadband), mMTC (massive machine type communication), and URLLC (Ultra Reliable and Low Latency Communications) [18, 23, 31, 152]. A prominent application of 5G is IoT, utilizing mMTC and URLLC types of services. 3GPP working group SA3 have defined 5G security specifications for security mechanisms for the 5G system as shown in Table 3 (relates to RQ3).

Security guidelines and baselines for IoT are being developed by the European Network and Information Security

Table 2 Cybersecurity/resilience aspects in 5G and beyond-enabled IoT applications

S. no.	Authors [References]	Security/resilience aspects
1	Raghu et al. [15]	Dynamic key cryptography, communication security, authentication
2	Jorge et al. [16]	Authentication and key agreement protocol, symmetric-key encryption
3	B.D. et al. [17]	Authentication, key exposure restriction, data privacy
4	Hiten [18]	Identity privacy
5	Minahil et al. [19]	Authentication protocol
6	Huaqun et al. [20]	Data integrity
7	Will [21]	Access control, authentication
8	Alberto et al. [22]	Intentional risk management, data integrity
9	Mohammed et al. [23]	Adversarial effects, decentralized security
10	Sultan et al. [24]	Self-adaptiveness, resilience
11	Raluca et al. [25]	Security vulnerabilities
12	Amril et al. [26]	Aggregate signature, group authentication
13	Mehdi et al. [27]	Secret key generation, jamming-resiliency
14	Prabhakar et al. [28]	Network intrusion detection
15	Vishal et al. [29]	Key exchange and authentication protocol
16	Anurag et al. [30]	Network slicing security
17	Zbigniew et al. [31]	End-to-end secure slice isolation
18	Amir et al. [32]	System-level resilience
19	Kubra et al. [33]	Secure key distribution, secure clustering
20	Hussain et al. [34]	Multiparty authentication
21	Md. Ashraf et al. [35]	Secure communication, data privacy
22	Lewis et al. [36]	Privacy-preserving, aggregate signcryption
23	Nilupulee et al. [37]	Cryptography
24	Amir et al. [38]	Network connectivity
25	Rasheed et al. [39]	High-level security architecture
26	Bocu et al. [40]	Network intrusion detection
27	Abdellah et al. [42]	Network security
28	Mishra et al. [43]	Data privacy and security
29	Dzogovic et al. [44]	Security vulnerabilities
30	Kisung et al. [45]	Key agreement, authentication
31	Zhixin et al. [46]	Mobile systems security
32	Suleyman et al. [47]	Resilient services
33	Christian et al. [48]	Ranks attack prevention
34	Deebak, et al. [49]	Authentication, key agreement
35	Prabhakar et al. [50]	Secure communication
36	Awaneesh et al. [53]	Multi factor authentication
37	Yuanjie et al. [54]	Resilience to failures and threats
38	Valerian et al. [55]	Malware detection
39	Shubham et al. [56]	Key-secrecy
40	Mustafa et al. [57]	Authentication, session key agreement
41	Vibha et al. [58]	Authentication
42	Vincent [59]	Authentication
43	Awaneesh et al. [60]	Authentication

Table 2 (continued)

S. no.	Authors [References]	Security/resilience aspects
44	Mattia et al. [61]	Botnet detection
45	Reshmi [63]	Anomaly detection
46	Sankar et al. [65]	Data integrity, authentication
47	Rahman et al. [66]	Data security, data privacy
48	Dakshita [67]	Data security
49	Ismaila et al. [68]	Mutual authentication, key agreement
50	Aruna et al. [70]	Self-sovereign identity
51	Jinwen et al. [71]	Data integrity
52	Fábio et al. [72]	Secure communication
53	Rao et al. [73]	Data security
54	Pronaya et al. [74]	Secure data exchange
55	Xianjun et al. [75]	Resilience of network coverage
56	Deepashika et al. [76]	Forensics security
57	Guilin et al. [77]	Data sharing and security
58	Nilesh et al. [78]	Secure message exchange
59	Vincent et al. [79]	Authentication
60	Lilhore et al. [80]	Intrusion detection
61	Borgohain et al. [81]	Authentication
62	Jesus Martins et al. [82]	Network slicing security
63	Benlloch-Caballero et al. [83]	Self-protection system
64	Ge et al. [84]	Authentication
65	Singh [85]	Authentication, key agreement
66	Alotaibi et al. [86]	Intrusion detection
67	Alamer et al. [87]	Privacy-preserving
68	Rajawat et al. [88]	Device security
69	Deebak et al. [89]	Multi-factor authentication
70	Escaleira et al. [90]	Securing moving targets
71	Nyangaresi et al. [91]	Authentication
72	Kaushik et al. [92]	Post-quantum cryptography
73	Patruni et al. [93]	Privacy-preserving, authentication
74	Alcaraz et al. [94]	Device and data security
75	Xu et al. [95]	Resilient and secure communication
76	Babu et al. [96]	Trust management
77	Valadares et al. [97]	Threat modeling
78	Kumar et al. [98]	Authentication
79	Rajawat et al. [99]	Secure communication

Agency (ENISA), a center for cybersecurity expertise in Europe [153]. The National Institute of Standards and Technology (NIST) has also developed several reports on the security of IoT devices, including NISTIR 8259 [154], SP 800-213 Series [155], and Executive Order 14028 [156]; several of which are drafts. NISTIR 8259 provides guidance for manufacturers and the third parties who support them as they design, develop, test, sell, and support IoT devices. The NISTIR 8259 series has three final documents, (1) NISTIR 8259 [157]: it is a report of foundational activities of recommendations for IoT device manufacturers, (2) NISTIR 8259A [158]: it is the report of core device cybersecurity capability baseline; and (3) NISTIR 8259B [159]: it is a report of IoT non-technical supporting capability core baseline. The Open Web OWASP [160] has developed an IoT project to help manufacturers, developers, and consumers better understand IoT security issues and help users make better security decisions when developing, deploying, or assessing IoT solutions, no matter what context they are in. ISO/IEC developed

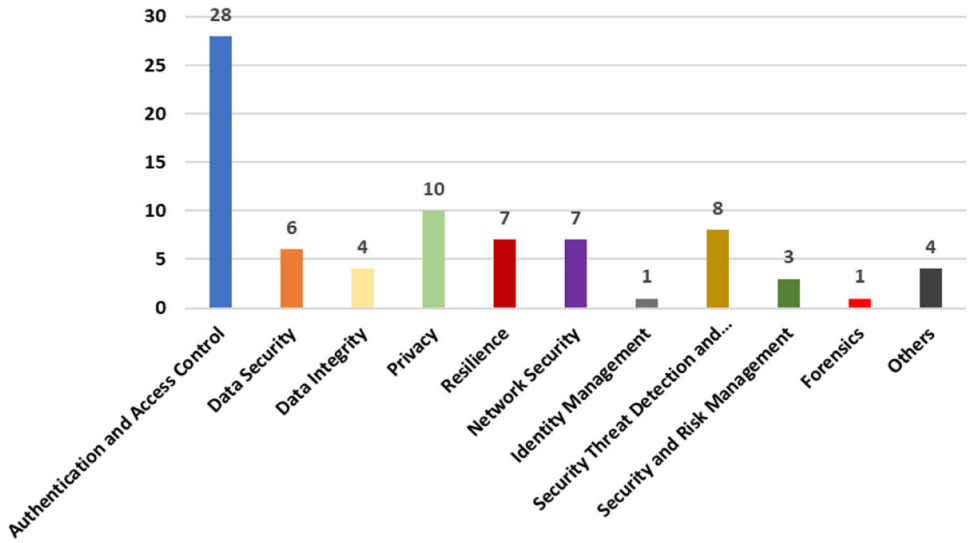

Fig. 3 Security/resilience aspects for 5G-enabled IoT in the included studies

Table 3 3GPP security assurance specification set: 5G

References	Title	Type	Radio technology
33.861	Study on evolution of Cellular Internet of Things (CIoT) security for the 5G System	Technical report	5G
33.117	Catalog of general security assurance requirements	Technical specification	3G, LTE and 5G
33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class	Technical specification	5G
33.512	5G SCAS: Access and Mobility management Function (AMF)	Technical specification	5G
33.513	5G SCAS; User Plane Function	Technical specification	5G
33.514	5G SCAS for the Unified Data Management network product class	Technical specification	5G
33.515	5G SCAS for the Session Management Function network product class	Technical specification	5G
33.516	5G SCAS for the Authentication Server Function network product class	Technical specification	5G
33.517	5G SCAS for the Security Edge Protection Proxy network product class	Technical specification	5G
33.518	5G SCAS for the Network Repository Function network product class	Technical specification	5G
33.519	5G SCAS for the Network Exposure Function network product class	Technical specification	5G
33.916	Security Assurance Methodology for 3GPP network products	Technical report	3G, LTE and 5G
33.926	SCAS threats and critical assets in 3GPP network product classes	Technical report	LTE and 5G

Table 4 Cybersecurity standard/guidelines for IoT

Standard/guidelines/report	Number	Organization/trade associations/industry groups	Security aspect/focus	Current version
NISTIR 8259 Series	NISTIR 8259	NIST	Recommendations for IoT Device Manufacturers: Foundational Activities	Final documents (May 29, 2020)
	NISTIR 8259A	NIST	Core Device Cybersecurity Capability Baseline	Final documents (May 29, 2020)
	NISTIR 8259B	NIST	IoT Non-Technical Supporting Capability Core Baseline	Final documents (August 25, 2021)
	NISTIR 8259C	NIST	Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline	Draft
SP 800-213 Series	SP 800-213 Series	NIST	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	–
Executive Order 14028	NIST's response to E.O. 14028 on improving Consumer IoT cybersecurity	NIST	Baseline Security Criteria for Consumer IoT Devices	Draft (August 31, 2021)
White Paper	NIST recommendation	NIST	Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products	February 4, 2022
OWASP ISVS	The OWASP IoT Security Verification Standard	OWASP	A framework of security requirements for IoT applications	–
ISO/IEC 27400:2022	Cybersecurity—IoT security and privacy—Guidelines	ISO/IEC	Guidelines on risks, principles and controls for security and privacy of IoT solutions	Published June, 2022
Guidelines for Securing the IoT	–	ENISA	Guidelines for securing the supply chain for IoT	November 09, 2020
Baseline Security Recommendations for IoT	–	ENISA	Baseline Security Recommendations for IoT in the context of critical information infrastructures	November 20, 2017

Table 4 (continued)

Standard/guidelines/report	Number	Organization/trade associations/industry groups	Security aspect/focus	Current version
GSMA IoT Security Guidelines and Assessment	–	Global System for Mobile Communications (GSMA)	Best practice for the secure design, development, and deployment of IoT services, and providing a mechanism to evaluate security measures Best practice for designing, developing, and deploying IoT services in a secure manner, as well as a mechanism for evaluating security measures	–
ETSI EN 303 645	–	European Telecommunications Standards Institute (ETSI)	It lays the foundation for future IoT certifications and sets a security baseline for connected consumer products	June 2020
Assessment specification (ETSI EN 303 645)	TS 103 701	ETSI	Specifies baseline conformance assessments for assessing consumer IoT products against the provisions of ETSI EN 303 645	August 2021
Implementation guide (ETSI EN 303 645)	TR 103 621	ETSI	Provides easy-to-follow guidance so manufacturers and other stakeholders can comply with consumer IoT requirements in ETSI EN 303 645	June 2020
ETSI EN 303 645	–	ETSI	Security baseline that applies to a variety of consumer IoT devices	June, 2020

guidelines for the security and privacy of IoT (ISO/IEC 27400:2022) [161] that provides guidelines on risks, principles, and controls. The details of security standards and guidelines are mentioned in Table 4 (relates RQ3).

5 Security methods and tools

In this section, we discuss the cybersecurity methods and tools for 5G and beyond-enabled IoT applications from the included studies. Table 5 (RQ2) describes the current techniques/mechanisms/tools that are developed for ensuring 5G and beyond-enabled IoT security and resilience and their underlying approaches used for their development.

Table 5 describes tools/techniques/mechanisms developed for ensuring security/resilience of 5G and beyond-enabled IoT in addition to the underlying approaches used for its development. Firstly, B.D. et al. [17], Huaqun et al. [20], Will [21], Alberto et al. [22], Sankar et al. [65], Dakshita [67], Jinwen et al. [71], Rao et al. [73], Pronaya et al. [74], Deepashika et al. [76], Kumar et al. [98], and Rajawat et al. [99] used blockchain technology along with the graph, AI models, neural network, and hash functions for their development. For instance, B.D. et al. [17] used blockchain to

Table 5 Cybersecurity methods for 5G and beyond-enabled IoT applications

S. no.	Authors [References]	Development (techniques/tools)	Underlying approach
1	Raghu et al. [15]	Dynamic key generation scheme	Entropy to build a large set of unique keys
2	Jorge et al. [16]	Lightweight authentication scheme	Symmetric key Cryptography
3	B.D. et al. [17]	Lightweight decentralized architecture for 5G and beyond	Blockchain technology
4	Hiten [18]	Lightweight scheme for privacy management	Hash functions and Xor operations
5	Minahil et al. [19]	5G enabled IoT authentication protocol for eHealth cloud	Biometrics Features
6	Huaqun et al. [20]	Remote data integrity checking scheme	Blockchain, RSA and hash function
7	Will [21]	Physical and digital cybersecurity user authentication method	Blockchain technology, and neural networks
8	Alberto et al. [22]	Intentional risk-based strategy	Blockchain technology, and visibility graph
9	Mohammed et al. [23]	Methodology for integrating of IoT and AI with 5G and beyond	Blockchain technology, and machine learning
10	Sultan et al. [24]	Fog and edge computing architecture	Cloud computing strategies
11	Raluca et al. [25]	Remote healthcare system	AI and autonomous activities
12	Amril et al. [26]	Architecture of the authentication system	Aggregate signature
13	Mehdi et al. [27]	Jamming-resistant scheme	Frequency hopping spread spectrum techniques
14	Prabhakar et al. [28]	Distributed threat analysis	SDN
15	Vishal et al. [29]	Authentication protocol	Secure handover in mobile terminals
16	Anurag et al. [30]	Neural Network based 'Secure5G' Network Slicing model	Deep learning
17	Zbigniew et al. [31]	Secure end-to-end slice isolation and management	Adaptable management and orchestration architecture (Focus more on 5G)
18	Amir et al. [32]	System-level resilience approach	Graph interdependencies
19	Kubra et al. [33]	Secure clustering mechanism	Software defined networking
20	Hussain et al. [34]	Dynamic authentication model	Multiparty computation
21	Md. Ashraf et al. [35]	Decentralized eHealth architecture	Blockchain technology
22	Lewis et al. [36]	Secure and privacy preserving collision avoidance system	Certificateless aggregate signcryption
23	Nilupulee et al. [37]	Optimized lightweight cryptography algorithm	Cryptographic techniques
24	Amir et al. [38]	Smart home resilient Model	Graph theory

Table 5 (continued)

S. no.	Authors [References]	Development (techniques/tools)	Underlying approach
25	Rasheed et al. [39]	High level integrated security architecture	Software defined networking, SSL, TLS
26	Bocu et al. [40]	Intrusion detection system	AI models
27	Abdellah et al. [42]	Time series prediction approach	ML models
28	Mishra et al. [43]	5G architecture for e-health system	5G advanced radio approach
29	Dzogovic et al. [44]	Progressive approach for network slices isolation	Enhanced VPN technology
30	Kisung et al. [45]	Lightweight and secure access authentication scheme	AVISPA tool
31	Zhixin et al. [46]	Virtual end-to-end testbed for 5G network	Local cluster machines
32	Suleyman et al. [47]	Trust-based defense framework	External and internal incident scenarios
33	Christian et al. [48]	Intrusion prevention scheme	Reinforcement learning
34	Deebak, et al. [49]	Security authentication framework	Asymmetric cryptographic techniques
35	Prabhakar et al. [50]	Secure multimedia communication framework	Lightweight hybrid cipher techniques
36	Awaneesh et al. [53]	Multi-factor authentication protocol	Asymmetric cryptographic techniques
37	Yuanjie et al. [54]	Stateless mobile core network functionality	Geospatial mobility management approach
38	Valerian et al. [55]	Malware detection framework	Federated learning
39	Shubham et al. [56]	Inter-gNB handover protocol	AVISPA tool
40	Mustafa et al. [57]	Security ephemeral generation protocol	Stochastic method
41	Vibha et al. [58]	Cybtwin driven approach with multi-agent authentication	Authentication model
42	Vincent [59]	Security token derivation scheme	Security protocols
43	Awaneesh et al. [60]	Authentication and key agreement protocol	Symmetric cryptographic techniques
44	Mattia et al. [61]	Botnet detection framework	Security and privacy framework, ML models, domain generation algorithm
45	Reshmi [63]	Network diagnostics and self-healing technique	Time series analysis
46	Sankar et al. [65]	Authentication method for validating blocks	Blockchain techniques
47	Rahman et al. [66]	Healthcare sustainability framework	Deep learning, blockchain
48	Dakshita [67]	Architecture to ensure the secure sensing and tracking of an object	Blockchain, AI models
49	Ismaila et al. [68]	Lightweight mutual authentication and key agreement protocol	Real-or-random model, formal security verification techniques, and AVISPA toolkit

Table 5 (continued)

S. no.	Authors [References]	Development (techniques/tools)	Underlying approach
50	Aruna et al. [70]	Self-sovereign identity technique for secure data migration	Cryptographic techniques
51	Jinwen et al. [71]	Lightweight model for crowdsensing	Smart contracts, blockchain techniques
52	Fábio et al. [72]	Multi-layered context broker federation platform	Data federation techniques
53	Rao et al. [73]	Hyperledger fabric data protection framework	Blockchain techniques
54	Pronaya et al. [74]	Lightweight proof-of-proximity scheme	Blockchain techniques
55	XIANJUN et al. [75]	Resilience models for deploying 5G-IoT nodes	Confident information coverage technique
56	Deepashika et al. [76]	Cybersecurity forensics Architecture	Digital signatures, blockchain techniques
57	Guilin et al. [77]	Secure network communication scheme	OT edge technology
58	Nilesh et al. [78]	AI-driven network softwarization scheme	AI models
59	Vincent et al. [79]	Network selection and authentication protocol	Neural networks, symmetric key cryptography
60	Lilhore et al. [80]	Intrusion detection model in 5G-IoT communication	Light-weight CNNs architecture and transfer learning
61	Borgohain et al. [81]	Lightweight D2D authentication protocol	Elliptic curve cryptography and symmetric key cryptography
62	Jesus Martins et al. [82]	Network management approach for assisting micro services	Natural language processing
63	Benlloch-Caballero et al. [83]	Cognitive closed loop system to offer distributed dual-layer self-protection capabilities	Network intrusion detection system
64	Ge et al. [84]	Game-theoretic zero-trust authentication framework	Game theory (Markov games), bayesian updates
65	Singh [85]	Group-based efficient authentication and key agreement protocol	Low-cost symmetric key cryptography
66	Alotaibi et al. [86]	Federated and softwarized intrusion detection framework	Hierarchical federated learning
67	Alamer et al. [87]	Lightweight privacy-preserving scheme	Homomorphic cryptographic technology under the elliptic curve methodology
68	Rajawat et al. [88]	Hybrid deep learning algorithm for monitoring IoT-based sensor security	Neural networks
69	Deebak et al. [89]	Robust lightweight secure multi-factor authentication	Elliptic-curve cryptography
70	Escaleira et al. [90]	Moving target defense-based protection technique	Moving target defense design principles

Table 5 (continued)

S. no.	Authors [References]	Development (techniques/tools)	Underlying approach
71	Nyangaresi et al. [91]	Packet replays prevention protocol	Message Authentication codes, symmetric cryptography, and elliptic curve cryptography
72	Kaushik et al. [92]	Lightweight learning with errors based algorithms	Symmetric and asymmetric key cryptography
73	Patruni et al. [93]	Privacy-preserving authentication mechanism	Elliptic curve arithmetic and collision-free hash function
74	Alcaraz et al. [94]	Layered protection framework for 6G-enabled IIoT environments	Protection layers (requirements, matching services)
75	Xu et al. [95]	Random coding approach for pilot encoding	Generalized superimposed code
76	Babu et al. [96]	Trusted blockchain system for edge-based 5G networks	Elliptic curve cryptography
77	Valadares et al. [97]	Threat model for 5G enabled IoT	STRIDE and CVSS system
78	Kumar et al. [98]	Ultralightweight authentication protocol	Blockchain techniques
79	Rajawat et al. [99]	5G enabled IoT architecture	Blockchain techniques

address data integrity and privacy in cloud-storage by implementing a robust, block-chain based, lightweight distributed architecture for auditing schemes. This is mainly to mitigate the issue of secret key exposure. In addition, Huaqun et al. [20] used blockchain to address the cybersecurity problem of remote data integrity checking for data stored remotely on cloud servers, particularly utilizing its tamper-resistant property.

Furthermore, Raghu et al. [15], Jorge et al. [16], Hiten [18], Amril et al. [26], Lewis et al. [36], Nilupulee et al. [37], Deebak et al. [49], Awaneesh et al. [53], Awaneesh et al. [60], Aruna et al. [70], Vincent et al. [79], Borgohain et al. [81], Singh [85], Alamer et al. [87], Deebak et al. [89], Nyangaresi et al. [91], Kaushik et al. [92], Patruni et al. [93], and Babu et al. [96] used applied cryptography, hash functions, digital signatures to develop security techniques for 5G and beyond-enabled IoT systems. For instance, Raghu et al. [15] used applied cryptography to address security and scalability issues in 5G networks. This is mainly by implementing a hierarchical authentication and access control scheme, employing dynamic key cryptography across multiple layers of the 5G network architecture. In addition, Kaushik et al. [92] used post-quantum public and private key cryptography to propose algorithms designed for effective encryption of data streams within a 5G-enabled IoT environment. Finally, Amir et al. [32] and Amir et al. [38] used graph theory to analyze the resilience and robustness of critical services and connections within smart home networks, focusing on both network connectivity and technology interdependence for 5G-enabled IoT security.

5.1 Performance evaluation metrics

Figure 4 (relates to RQ5) elaborates the most used performance analysis metric for 5G and beyond-enabled IoT in the included studies. This SLR finds that computation and communication overheads and costs, calculation time, and energy consumption are used by several included studies. Table 6 describes the performance evaluation metrics and/or accuracy of developed techniques or mechanisms or tools in the included studies. B.D. et al. [17], Hiten [18], Minahil et al. [19], Huaqun et al. [20], Amril et al. [26], Lewis et al. [36], Awaneesh et al. [53], Valerian et al. [55], Shubham et al. [56], Mustafa et al. [57],Vincent [59], Awaneesh et al. [60], Ismaila et al. [68], Vincent et al. [79], Borgohain et al. [81], Jesus Martins et al. [82], Alamer et al. [87], Deebak et al. [89], Kumar et al. [98], and Rajawat et al. [99] used the computation and communication cost and overheads as one of their performance evaluation metrics.

Whereas, B.D. et al. [17], Hiten [18], Mehdi et al. [27], Prabhakar et al. [28], Md. Ashraf et al. [35], Sankar et al. [65], Dakshita [67], Aruna et al. [70], Jinwen et al. [71], Fábio et al. [72], Pronaya et al. [74], Xianjun et al. [75], Deepashika

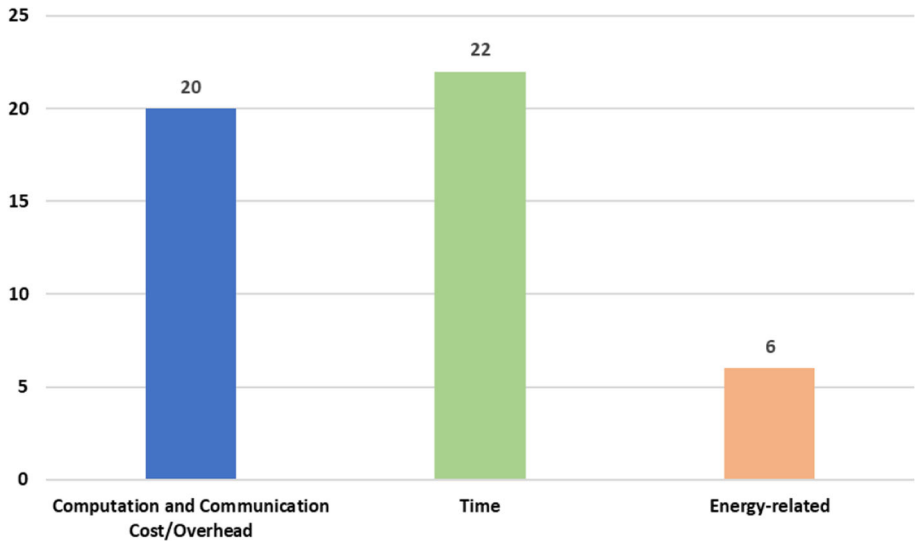

Fig. 4 Most used performance analysis metric for 5G and beyond-enabled IoT in the included studies

et al. [76], Borgohain et al. [81], Jesus Martins et al. [82], Benlloch-Caballero et al. [83], Alotaibi et al. [86], Rajawat et al. [88], Escaleira et al. [90], Kaushik et al. [92], Babu et al. [96], and Rajawat et al. [99] has used time metrics (mainly computation or execution or processing) for evaluating the performance of their studies. B.D. et al. [17], Md. Ashraf et al. [35], Awaneesh et al. [53], Awaneesh et al. [60], Ismaila et al. [68], and Deebak et al. [89] used energy consumption for performance evaluation. Other metrics used in these studies are data storage, audit message size, energy and time in B.D. et al. [17], execution time analysis in Hiten [18], signature size in Amril et al. [26], and average loss ratio, task duration in Lewis et al. [36]. B.D. et al. [17], Mehdi et al. [27], Prabhakar et al. [28], Ashraf et al. [35], have used time or time duration for analyzing performance. Ashraf et al. [35], and B.D. et al. [17] applied energy for performance analysis.

5.2 Validation mechanisms and approaches

We used comparison criteria "Validation Approach" to identify the type of validation approaches used in the included studies. Based on our analysis of the 79 studies, we observe that most of the studies have used simulation (70) for validation, where 8 studies have used both simulation and formal analysis. Other methods such as tool-based (1), and formal analysis (1) were also used to validate the proposed method or approach in the included studies, as shown in Table 7.

Moreover, in the simulation-based approach, there were three different ways in which they performed validation including: (1) prototype implementation and experiments (55), (2) numerical analysis (16), and (3) application scenarios (1). Finally, there were 9 studies in which validation was not performed.

We used the comparison criterion "Validation Mechanism" to analyze the validation methods used in the 79 included studies. We considered three different validation mechanisms: (1) hardware-based, (2) software-based, and (3) theoretical. From Fig. 5 (relates to RQ6), we observed that the majority of the studies (35 in total), considered software-based validation mechanisms. Additionally, a considerable number of studies (19 in total), utilized a combination of both hardware and software-based validation. Six studies relied on hardware-based validation, while six studies employed theoretical validation methods. Moreover, two studies incorporated all three validation mechanisms, hardware-based, software-based, and theoretical. One study utilized a combination of hardware-based and theoretical validation, while seven studies employed both software-based and theoretical validation methods. However, nine studies did not explicitly present any validation approach or methods.

6 Application domains and focused layer

We used the comparison criteria *"Application Domain"* to identify the type of application domains in which these included studies were demonstrated as shown in Table 8 (RQ4). From Fig. 6 (relates to RQ4), we infer that 53 out of 79 studies did not have any specific application domain. However, these studies focused on IoT in general and can be adapted to different application domains. For instance, Raghu et al. [15] proposed a cyclic key generation approach for producing a large number of dynamic keys for operating in resource constrained IoT systems. In addition, Hiten [18] presented a scheme called "HashXor", which helps to protect the identity privacy of IoT. Furthermore, there were 12 out of 79 studies focused on healthcare. For instance, Minahil et al. presented a novel authentication protocol for e-Health cloud [19]. This helps to prevent some attacks like impersonation, users' anonymity.

Table 6 Performance evaluation metrics in the included studies

S. no.	Authors [References]	Performance evaluation metrics	Description
1	Raghu et al. [15]	Entropy, randomness, and keys storage capacity	These are used for measuring randomness of generated keys
2	Jorge et al. [16]	Privacy protection level, unlinkability, availability	An enhanced symmetric-key protocol is proposed to evaluate the performance of developed system
3	B.D. et al. [17]	Computation cost, energy and time	For analyzing data storage and audit
4	Hiten [18]	Execution time analysis, and computational cost	Analysis of security; Analysis of computation cost and execution time
5	Minahil et al. [19]	Computation and communication overheads	Comparative analysis of security features; Performance analysis of computation cost, communication cost, storage cost, and computation time
6	Huaqun et al. [20]	Computation cost	For analyzing efficiency of systems
7	Will [21]	Tampering error	Analysis of learning and mining time, number of learning and mining iterations, learning and mining error, learning and mining threshold, tampering error
8	Alberto et al. [22]	Price volatility degree, power law fit, clustering coefficients	To perform intentional risk management for 5G systems
9	Mohammed et al. [23]	None	None
10	Sultan et al. [24]	Self-adaptiveness, feasibility	To find out that the system provides intelligent, resource-efficient
11	Raluca et al. [25]	None	None
12	Amril et al. [26]	Computational cost and signature size	Analysis of signature time, computation time
13	Mehdi et al. [27]	Coherence time, Secret key rate, ergodic secrecy rate, power allocation	Evaluate the accuracy of 5G enabled IoT system
14	Prabhakar et al. [28]	Attack detection scalability and speed, processing time	Evaluation on the following aspects: throughput effect on benign traffic, latency overhead analysis of key operations, avoidance of control channel saturation due to data plane authority layer, flow table update capacity of controller, resilience, speed, botnet tracking, performance of key functions

Table 6 (continued)

S. no.	Authors [References]	Performance evaluation metrics	Description
15	Vishal et al. [29]	Packet loss, and handover failure	Check whether the proposed protocol is vulnerable and susceptible to any assailment or not
16	Anurag et al. [30]	Spoofing attack scenario	Evaluate Secure5G deep learning model on how it can be used to proactively prevent DDoS attacks on a 5G network based on the incoming network connections before it even reaches to the core network
17	Zbigniew et al. [31]	None	None
18	Amir et al. [32]	Access link failure	Analysis of throughput, and delay
19	Kubra et al. [33]	Connectivity of the network, compromised Cluster Head Ratio, Compromised links	Analysis of performance in terms of compromised cluster head ratio, connectivity, compromised links, and additionally compromised links
20	Hussain et al. [34]	Average authentication delay	Analysis of authentication delay
21	Md. Ashraf et al. [35]	Execution time, energy consumption, reliability, traffic overhead, fault tolerance, scalability	Analysis of energy consumption, block generation time; Analysis of performance of the security protocol
22	Lewis et al. [36]	Computational cost, average loss ratio, task duration	Evaluate security in terms of privacy preservation, authentication, authorization
23	Nilupulee et al. [37]	Key size, security level, block size, packet error ratio	Analysis of security level, block size, target attacks (Software/Hardware), and key size
24	Amir et al. [38]	connectivity, centrality, betweenness, Closeness, Shortest path	Calculate various graph analysis metrics i.e., distance-based centrality metrics, connectivity-based centrality metrics, and spectra centrality metrics
25	Rasheed et al. [39]	None	None
26	Bocu et al. [40]	Computation overheads, precision, reliability, tradeoff, accuracy, and false positives rate	Improving the performance of real-time intrusion detection process
27	Abdellah et al. [42]	Mean square error, root mean square error, and mean absolute percentage error	Predicting delay in IoT and tactile internet networks
28	Mishra et al. [43]	Throughput, latency, average delay	Efficiency time sensitive healthcare applications
29	Dzogovic et al. [44]	Regression analysis, probability of attack sources	Evaluating the likelihood an attacker can acquire information

Table 6 (continued)

S. no.	Authors [References]	Performance evaluation metrics	Description
30	Kisung et al. [45]	Resistance against a single point of failure attack	Improving the security level for 5G-IoT applications
31	Zhixin et al. [46]	Attack rate, memory and CPU usage	Analyzing the HTTP requests for the victim servers
32	Suleyman et al. [47]	Trustability, level of resilience	Dynamically ensuring trust and resilience
33	Christian et al. [48]	Packet delivery ratio, duty cycle, and adequate delay	Enhancing capabilities to improve the rank attacks
34	Deebak, et al. [49]	Packet delivery ratio, throughput rate and transmission delay	Secure exchange of session keys between medical devices
35	Prabhakar et al. [50]	Authentication delay, packet loss ratio, and throughput	Robust against the communication channel attacks
36	Awaneesh et al. [53]	Energy consumption, computation and communication costs	Balancing the security services and energy consumption
37	Yuanjie et al. [54]	Scalability and resilience	Improving the threats and failure detection capabilities
38	Valerian et al. [55]	Accuracy, computation and communication costs	Improving the efficiency of cyber threats detection
39	Shubham et al. [56]	Computation and communication overheads	Improving efficiency for handover systems
40	Mustafa et al. [57]	Computation overheads and communication costs	Assessing the authentication protocol's performance
41	Vibha et al. [58]	None	None
42	Vincent [59]	Computation and communication costs, and security features	Ensuring minimal communication and computation complexities for 5G-IoT
43	Awaneesh et al. [60]	Energy consumption and computation, communication and storage costs	Reducing the overheads under unknown attacks
44	Mattia et al. [61]	Resources consumption	Enabling the deployment of DGA-based botnet detection modules in resource-constrained environments
45	Reshmi [63]	Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Error (MAS) and Mean Absolute Percent Error (MAPE)	Evaluating the accuracy of anomaly detection and prediction
46	Sankar et al. [65]	Immutability, throughput, time overhead, bandwidth, latency, response time, and an end to end delay	Evaluating the efficiency of developed approach
47	Rahman et al. [66]	Model loss, accuracy, receiver Operating Characteristic (ROC)	Evaluating the efficiency of developed approach

Table 6 (continued)

S. no.	Authors [References]	Performance evaluation metrics	Description
48	Dakshita [67]	Data transfer time, and mobility level of dynamic autonomous vehicles connectivity	To evaluate the performance of the proposed system based on round-trip latency and mobility level
49	Ismaila et al. [68]	Communication and storage overheads, and energy consumption	Analyzing the costs of sending and receiving the information by 5G-IoT devices
50	Aruna et al. [70]	Encryption and decryption time	Balancing the security and resource consumption
51	Jinwen et al. [71]	Running time for block generation, throughput, transaction latency, communication time	Improving the data processing and computing potentials for the IoT systems
52	Fábio et al. [72]	Latency, processing time	Testing the efficiency of batteries in different sets of messages
53	Rao et al. [73]	None	None
54	Pronaya et al. [74]	Bid price and thresholds, serving and parsing time	Addressing scalable and resource efficient approach for IoT system
55	Xianjun et al. [75]	deployment costs and accuracies, correlation distance, execution time and estimation error	Measuring the resilient deployment cost under different analogue error and transmission error
56	Deepashika et al. [76]	Computation time on the data plane and control plane, and total time consumption	Evaluating the total time consumption for the IoT device and switches for traffic processing
57	Guilin et al. [77]	None	None
58	Nilesh et al. [78]	Accuracy, precision, F1-score, packet drop ratio, and latency	Measuring the effectiveness of predictive analytics
59	Vincent et al. [79]	Computation and communication costs, packet loss ratio, and latency variations	Measuring the overheads and costs of the system for deploying 5G-IoT solution
60	Lilhore et al. [80]	MSE, RMSE, MAE, accuracy, precision, recall, F-Measure, confusion matrix	Measuring the performance of the proposed method in different factors
61	Borgohain et al. [81]	Time complexity, computation and communication costs	Evaluating and comparing the effectiveness of the proposed scheme within the area of security in D2D communication
62	Jesus Martins et al. [82]	Deployment time, computational and network overheads	Assessing the overhead of the developed system
63	Benlloch-Caballero et al. [83]	Average execution time of the self-protection loop, attack detection and mitigation capabilities	Measuring the performance of the architecture and system mainly in terms of two different metrics

Table 6 (continued)

S. no.	Authors [References]	Performance evaluation metrics	Description
64	Ge et al. [84]	Trust score, reliability of evidence, true-positive rate, average steps to converge	Evaluating the zero-trust security approach using different metrics to evaluate the trustworthiness of an agent in the network
65	Singh [85]	Signaling overhead, bandwidth usage, computational cost, and transmission latency	Analyzing the performance of the protocol
66	Alotaibi et al. [86]	Accuracy, training loss, total training time, convergence time, communication time complexity	Assessing the performance in terms of prediction, efficiency, and convergence
67	Alamer et al. [87]	Computation and communication overheads	Evaluating the performance base on resource consumption and overheads
68	Rajawat et al. [88]	Execution time, precision, recall, F-measure, RMSE	Evaluating the performance for monitoring IoT device security
69	Deebak et al. [89]	Signaling cost, communication cost, computation cost, bandwidth consumption, energy consumption, throughput rate, packet delivery ratio, and end-to-end delay	Assessing the performance by balancing resources and security
70	Escaleira et al. [90]	Failures ratio, number of requests per second, average response time, OSM CPU usage, OSM RAM usage, Kube API received packets, Kube API transmitted packets, Kube API received MB, and Kube API transmitted MB	Analyzing the impact of moving target at the management and user plane levels
71	Nyangaresi et al. [91]	Execution time, and bandwidth requirements	Evaluating the performance of the protocol using the key metrics
72	Kaushik et al. [92]	Time and memory requirements, security, and time for key generation, encryption and decryption	Examining the performance of the system in different metrics needed for execution
73	Patruni et al. [93]	Data transmission ratio, authentication delay, and throughput rate	Evaluating the performance of privacy-preserving authentication with device verification
74	Alcaraz et al. [94]	None	None
75	Xu et al. [95]	Code performance, resource overheads, and system reliability performance	Evaluating the performance of resilient and secure ultra reliable low latency communications

Table 6 (continued)

S. no.	Authors [References]	Performance evaluation metrics	Description
76	Babu et al. [96]	Number of participants in the network, running time of edge-device registration, running time of edge-device operations, throughput, and running time of peers	Assessing the performance via Hyperledger fabric platform
77	Valadares et al. [97]	None	None
78	Kumar et al. [98]	Security and functionality features, computation and communication costs	Analyzing the performance for the authentication and key agreement phases
79	Rajawat et al. [99]	Computation time, throughput, evaluation time	Evaluating the resources required for the proposed approach to offer decentralized and secure communication

On the other hand, there were 5 out of 79 studies demonstrated in the transportation domain. Vishal et al. [29] proposed an authentication protocol for vehicular networks over a highway. In contrast, there were 3 out of 79 studies demonstrated in the home automation domain. For instance, Amir et al. [38] presented a smart home architecture. In addition, there were 2 out of 79 studies demonstrated in the edge-cloud computing domain. For instance, Vibha et al. [58] introduced a novel approach that combines deep reinforcement learning with Cybertwin technology to create a unified framework for resource allocation and computation offloading in 6G wireless networks. Finally, there was a study demonstrated in each of the following domains, which we classified as *"Others"* in Fig. 6 (relates to RQ4): (1) tactile internet networks [42], (2) multimedia [50], (3) smart city [21], (4) space [54], (5) mobile and edge computing [61], (6) environment [75], (7) energy [77], and (8) military [89].

We used the comparison criteria "Security Goal(s) Addressed" to understand which of the following security goal(s) these included studies addressed: (1) confidentiality, (2) integrity, and (3) availability [162]. The security goal "confidentiality" means that the systems and resources are protected against unauthorized viewing [162]. Furthermore, the security goal "integrity" refers to the assurance that the data has not been tampered with, whereas the security goal "availability" means that the only authorized users may get access to the infrastructure if required [139].

From Table 8 (relates to RQ4), we infer that 18 out of 79 studies addressed the security goals including confidentiality, integrity, and availability. For instance, Raghu et al. presented a unique key generation approach which ensures these security goals [15]. Furthermore, Ashraf et al. proposed a decentralized architecture for healthcare [35]. This study addressed confidentiality using ring signatures, whereas integrity and availability are addressed through the employment of multiple patient agents at different levels. In contrast, we infer that 30 out of 79 studies addressed both confidentiality and integrity. For instance, B.D. et al. [17] proposed a lightweight architecture using blockchain technology which ensures both confidentiality and integrity. Furthermore, Lewis et al. [36] presented a secure and privacy-preserving method for transportation systems to ensure confidentiality and integrity, Lewis et al. [36] employed certificateless aggregate signcryption in conjunction with a pseudonymous technique. On the other hand, we infer that 3 out of 79 studies addressed both confidentiality and availability in addition 2 out of 79 studies addressed both integrity and availability. For instance, Jorge et al. [16] proposed an enhanced version of Braeken protocol that ensures confidentiality and availability, whereas Anurag et al. [30] presented AI models-based secure network slicing in 5G which ensure integrity and availability.

We also infer that 10 out of 79 studies addressed only confidentiality, whereas 5 out of 79 studies addressed only integrity and 8 out of 79 studies addressed only availability. For instance, Amril et al. [26] performed the comparative analysis of Identity-based aggregation signature (IBAS) schemes that ensure confidentiality. Furthermore, Huaqun et al. [20] proposed a decentralized data integrity checking method using blockchain technology that ensures integrity. Moreover, Mehdi et al. [27] presented a lightweight jamming resistant scheme for IoT in 5G networks that ensures availability. Notably, 3 out of 79 studies focus on resilience instead of security [32, 38, 47].

We used comparison criteria *"Development Lifecycle Phase Addressed"* to understand which development lifecycle phases were addressed in our included studies. The

Table 7 Validation mechanisms and approaches used in the included studies

S. no.	Authors [References]	Validation mechanism	Validation approach
1	Raghu et al. [15]	Hardware-based	Simulation (Prototype implementation and experiments (Testbed)
2	Jorge et al. [16]	Not Validated	Not Validated
3	B.D. et al. [17]	Hardware-based and Theoretical	Simulation (Prototype implementation and experiments; Numerical analysis)
4	Hiten [18]	Hardware-based and Software-based	Tool-based and developed prototyped based validation based on different experiments
5	Minahil et al. [19]	Hardware-based and Software-based	Simulation (Prototype implementation and experiments)
6	Huaqun et al. [20]	Hardware-based	Simulation (Prototype implementation and experiments)
7	Will [21]	Software-based	Simulation (Prototype implementation and experiments)
8	Alberto et al. [22]	Not Validated	Not Validated
9	Mohammed et al. [23]	Not Validated	Not Validated
10	Sultan et al. [24]	Not Validated	Not Validated
11	Raluca et al. [25]	Not Validated	Not Validated
12	Amril et al. [26]	Theoretical	Simulation (Numerical analysis)
13	Mehdi et al. [27]	Theoretical	Simulation (Numerical analysis)
14	Prabhakar et al. [28]	Hardware-based and Software-based	Simulation (Prototype implementation and experiments (Testbed))
15	Vishal et al. [29]	Software-based and Theoretical	Formal Analysis, and Simulation (Numerical analysis)
16	Anurag et al. [30]	Hardware-based and Software-based	Simulation (Prototype implementation and application scenarios (Volume-based Attack (Flooding), Masking Botnet Attack (Spoofing))
17	Zbigniew et al. [31]	Not Validated	Not Validated
18	Amir et al. [32]	Software-based	Simulation (Prototype implementation and experiments)
19	Kubra et al. [33]	Software-based	Simulation (Prototype implementation and experiments)
20	Hussain et al. [34]	Software-based	Simulation (Prototype implementation and experiments)

Table 7 (continued)

S. no.	Authors [References]	Validation mechanism	Validation approach
21	Md. Ashraf et al. [35]	Software-based	Simulation (Prototype implementation and experiments)
22	Lewis et al. [36]	Software-based and Theoretical	Simulation (Prototype implementation and experiments, Numerical analysis)
23	Nilupulee et al. [37]	Theoretical	Simulation (Prototype implementation and experiments)
24	Amir et al. [38]	Theoretical	Formal graph representation
25	Rasheed et al. [39]	Not Validated	Not Validated
26	Bocu et al. [40]	Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
27	Abdellah et al. [42]	Software-based	Simulation (Prototype implementation and experiments)
28	Mishra et al. [43]	Software-based	Simulation (Prototype implementation and experiments)
29	Dzogovic et al. [44]	Hardware-based	Simulation (Prototype implementation and experiments)
30	Kisung et al. [45]	Software-based	Simulation (Numerical analysis)
31	Zhixin et al. [46]	Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
32	Suleyman et al. [47]	Software-based	Simulation (Prototype implementation and experiments)
33	Christian et al. [48]	Software-based	Simulation (Prototype implementation and experiments)
34	Deebak, et al. [49]	Software-based	Simulation (Prototype implementation and experiments)
35	Prabhakar et al. [50]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
36	Awaneesh et al. [53]	Software-based	Simulation (Numerical analysis)
37	Yuanjie et al. [54]	Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
38	Valerian et al. [55]	Software-based	Simulation (Prototype implementation and experiments)
39	Shubham et al. [56]	Software-based	Simulation (Prototype implementation and experiments)

Table 7 (continued)

S. no.	Authors [References]	Validation mechanism	Validation approach
40	Mustafa et al. [57]	Software-based and Hardware-based	Simulation (system modeling and computational analysis)
41	Vibha et al. [58]	Software-based	Simulation (Prototype implementation and experiments)
42	Vincent [59]	Software-based	Simulation (Prototype implementation and experiments)
43	Awaneesh et al. [60]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed)), Formal Analysis
44	Mattia et al. [61]	Software-based	Simulation (Prototype implementation and experiments)
45	Reshmi [63]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
46	Sankar et al. [65]	Software-based	Simulation (Prototype implementation and experiments)
47	Rahman et al. [66]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments)
48	Dakshita [67]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments)
49	Ismaila et al. [68]	Software-based	Simulation (Prototype implementation and experiments), Formal Analysis
50	Aruna et al. [70]	Software-based	Simulation (Prototype implementation and experiments)
51	Jinwen et al. [71]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
52	Fábio et al. [72]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
53	Rao et al. [73]	Software-based	Simulation (Prototype implementation and experiments)
54	Pronaya et al. [74]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments (Testbed))
55	Xianjun et al. [75]	Software based	Simulation (Prototype implementation and experiments)
56	Deepashika et al. [76]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments)

Table 7 (continued)

S. no.	Authors [References]	Validation mechanism	Validation approach
57	Guilin et al. [77]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments)
58	Nilesh et al. [78]	Software-based and Hardware-based	Simulation (Prototype implementation and experiments)
59	Vincent et al. [79]	Software-based	Simulation (Prototype implementation and experiments), Formal Analysis
60	Lilhore et al. [80]	Software-based	Simulation (Prototype implementation and experiments)
61	Borgohain et al. [81]	Software-based and Theoretical	Formal Analysis, Simulation (Numerical analysis)
62	Jesus Martins et al. [82]	Hardware-based and Software-based	Simulation (Prototype implementation and experiments)
63	Benlloch-Caballero et al. [83]	Hardware-based and Software-based	Simulation (Prototype implementation and experiments (Testbed))
64	Ge et al. [84]	Software-based	Simulation (Prototype implementation and experiments)
65	Singh [85]	Software-based and Theoretical	Formal Analysis, Simulation (Numerical analysis)
66	Alotaibi et al. [86]	Software-based	Simulation (Prototype implementation and experiments)
67	Alamer et al. [87]	Hardware-based, Software-based, and Theoretical	Simulation (Prototype implementation and experiments), and Simulation (Numerical analysis)
68	Rajawat et al. [88]	Software-based	Simulation (Prototype implementation and experiments)
69	Deebak et al. [89]	Software-based and Theoretical	Formal Analysis, Simulation (Numerical analysis)
70	Escaleira et al. [90]	Software-based	Simulation (Prototype implementation and experiments)
71	Nyangaresi et al. [91]	Theoretical	Security proofs, Simulation (Numerical analysis)
72	Kaushik et al. [92]	Software-based and Theoretical	Simulation (Numerical analysis)
73	Patruni et al. [93]	Hardware-based, Software-based, and Theoretical	Simulation (Prototype implementation and experiments), and Simulation (Numerical analysis)

Table 7 (continued)

S. no.	Authors [References]	Validation mechanism	Validation approach
74	Alcaraz et al. [94]	Not validated	Not validated
75	Xu et al. [95]	Theoretical	Simulation (Numerical analysis)
76	Babu et al. [96]	Software-based	Simulation (Prototype implementation and experiments)
77	Valadares et al. [97]	Not validated	Not validated
78	Kumar et al. [98]	Software-based and Theoretical	Formal Analysis, Simulation (Numerical analysis)
79	Rajawat et al. [99]	Software-based	Simulation (Prototype implementation and experiments)

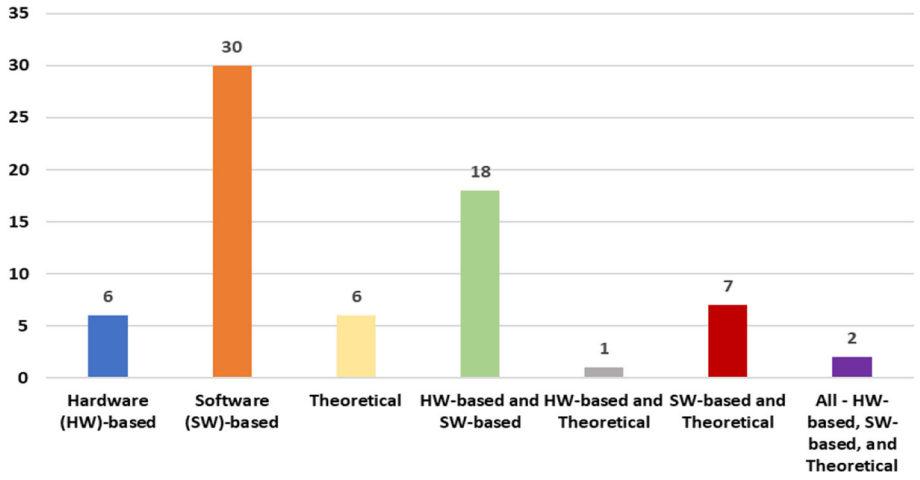

Fig. 5 Comparisons of validation mechanisms used in the included studies

development lifecycle phases include planning, system analysis and requirements, system design, development, integration and testing, implementation, and operations and maintenance. From Table 9 (relates to RQ4), we infer that predominantly (i.e., 32 out of 79 studies) addressed system design, system development, and implementation. For instance, Raghu et al. [15] designed and developed a dynamic key generation model which corresponds to system design and system development, whereas they analyzed the performance and security of the developed scheme which corresponds to implementation. Furthermore, 19 out of 79 studies addressed system design and implementation. Mehdi et al. [27] designed a lightweight jamming resistant scheme for IoT in 5G networks which corresponds to system design, whereas they did not develop the designed scheme. In addition, they analyzed the efficiency of the proposed scheme to state-of-the-art through numerical examples which correspond to implementation.

In addition, 3 out of 79 studies addressed system design and system development. For instance, Jorge et al. [16] designed and developed an enhanced version of Braeken protocol which corresponds to system development and system design. However, this study mainly lacks implementation compared to Raghu et al. [15] as they have not evaluated the performance of the developed protocol. Finally, 1 out of 79 studies addressed system requirements and system design [94].

From Table 9 (relates to RQ4), we also infer that 9 out of 79 studies addressed system design, whereas 14 out of 79 studies addressed implementation. Amril et al. [26] performed the comparative analysis of IBAS schemes which corresponds to implementation. Compared to the above-mentioned studies, this study did not design and/or develop schemes.

We used comparison criteria *"Operational layer"* to identify which operational layer(s) the included studies address. The operational layers include: (1) perception layer, (2) network layer, and (3) application layer. Perception layer observes the physical environment through sensors, whereas a network layer connects to other smart things, network devices and servers, in addition transmits and processes

Table 8 Application domain and security goal addressed in the included studies

S. no.	Authors [References]	Application domain	Security goal(s) addressed
1	Raghu et al. [15]	Generic (IoT)	Confidentiality, Integrity, and Availability
2	Jorge et al. [16]	Generic (IoT)	Confidentiality, and Availability
3	B.D. et al. [17]	Generic (Industrial IoT)	Confidentiality, and Integrity
4	Hiten [18]	Generic (IoT)	Confidentiality, and Integrity
5	Minahil et al. [19]	Health Care (e-health cloud)	Confidentiality
6	Huaqun et al. [20]	Transportation (Internet of Vehicles)	Integrity
7	Will [21]	Smart Cities (IoT and 5G Infrastructure)	Confidentiality
8	Alberto et al. [22]	Generic (IoT Platforms: IOTA and IoTeX)	Integrity
9	Mohammed et al. [23]	Generic (IoT)	Integrity
10	Sultan et al. [24]	Generic (IoT)	Integrity
11	Raluca et al. [25]	Health Care (Remote Patient Monitoring)	Confidentiality
12	Amril et al. [26]	Generic (Massive IoT)	Confidentiality
13	Mehdi et al. [27]	Generic (IoT)	Availability
14	Prabhakar et al. [28]	Generic (IoT)	Availability
15	Vishal et al. [29]	Transportation (Vehicular Networks)	Confidentiality, and Integrity
16	Anurag et al. [30]	Generic (IoT)	Integrity, and Availability
17	Zbigniew et al. [31]	Generic (IoT)	Confidentiality, and Integrity
18	Amir et al. [32]	Home Automation (Smart Home)	N/A—Resilience
19	Kubra et al. [33]	Generic (IoT)	Confidentiality
20	Hussain et al. [34]	Generic (Industrial IoT)	Confidentiality
21	Md. Ashraf et al. [35]	Health Care (Remote Patient Management)	Confidentiality, Integrity, and Availability
22	Lewis et al. [36]	Transportation (Internet of Vehicles)	Confidentiality, and Integrity
23	Nilupulee et al. [37]	Generic (Smart IoT Devices)	Confidentiality
24	Amir et al. [38]	Home Automation (Smart Home)	N/A—Resilience
25	Rasheed et al. [39]	Transportation (Vehicular Networks)	Confidentiality, and Integrity
26	Bocu et al. [40]	Generic (IoT)	Confidentiality, and Availability
27	Abdellah et al. [42]	Tactile Internet Networks	Availability
28	Mishra et al. [43]	Healthcare (Seamless Health Monitoring)	Availability
29	Dzogovic et al. [44]	Healthcare (Healthcare Verticals)	Confidentiality, and Availability
30	Kisung et al. [45]	Generic (IoT)	Confidentiality
31	Zhixin et al. [46]	Generic (IoT)	Availability
32	Suleyman et al. [47]	Generic (IoT)	N/A—Resilience

Table 8 (continued)

S. no.	Authors [References]	Application domain	Security goal(s) addressed
33	Christian et al. [48]	Generic (IoT)	Availability
34	Deebak, et al. [49]	Healthcare (Remote point-of-care)	Confidentiality, and Integrity
35	Prabhakar et al. [50]	Multimedia	Confidentiality, and Integrity
36	Awaneesh et al. [53]	Generic (IoT)	Confidentiality
37	Yuanjie et al. [54]	Space (Satellite communication)	Confidentiality, Integrity, and Availability
38	Valerian et al. [55]	Generic (IoT)	Confidentiality, and Integrity
39	Shubham et al. [56]	Generic (IoT)	Confidentiality, and Integrity
40	Mustafa et al. [57]	Generic (IoT)	Confidentiality, and Integrity
41	Vibha et al. [58]	Edge-cloud Computing (Cybertwin-driven Edge Computing)	Confidentiality, and Integrity
42	Vincent [59]	Generic (IoT)	Confidentiality, and Integrity
43	Awaneesh et al. [60]	Generic (IoT)	Confidentiality, and Integrity
44	Mattia et al. [61]	Mobile and Edge Computing	Confidentiality, Integrity, and Availability
45	Reshmi [63]	Generic (IoT)	Confidentiality, Integrity, and Availability
46	Sankar et al. [65]	Generic (IoT)	Confidentiality, and Integrity
47	Rahman et al. [66]	Healthcare (Internet of Health Things)	Confidentiality, and Integrity
48	Dakshita [67]	Transportation (Autonomous Vehicles)	Confidentiality, Integrity, and Availability
49	Ismaila et al. [68]	Healthcare (Tactile Internet-assisted remote surgery application)	Confidentiality, Integrity, and Availability
50	Aruna et al. [70]	Edge-cloud Computing	Confidentiality, and Integrity
51	Jinwen et al. [71]	Generic (IoT)	Integrity
52	Fábio et al. [72]	Generic (IoT)	Confidentiality, Integrity, and Availability
53	Rao et al. [73]	Home Automation (Smart Home)	Confidentiality, and Integrity
54	Pronaya et al. [74]	Generic (IoT)	Confidentiality, and Integrity
55	Xianjun et al. [75]	Environment	Availability
56	Deepashika et al. [76]	Generic (IoT)	Confidentiality, Integrity, and Availability
57	Guilin et al. [77]	Energy (Smart Grids)	Confidentiality
58	Nilesh et al. [78]	Generic (IoT)	Confidentiality, Integrity, and Availability
59	Vincent et al. [79]	Generic (IoT)	Confidentiality and Integrity
60	Lilhore et al. [80]	Generic (IoT)	Confidentiality, and Integrity
61	Borgohain et al. [81]	Generic (IoT)	Confidentiality, and Integrity
62	Jesus Martins et al. [82]	Healthcare (Remote Patient Monitoring)	Confidentiality, Integrity, and Availability
63	Benlloch-Caballero et al. [83]	Generic (IoT)	Integrity, Availability
64	Ge et al. [84]	Generic (IoT)	Confidentiality, and Integrity

Table 8 (continued)

S. no.	Authors [References]	Application domain	Security goal(s) addressed
65	Singh [85]	Healthcare (Internet of Medical Things)	Confidentiality, and Integrity
66	Alotaibi et al. [86]	Generic (IoT)	Confidentiality, Integrity, and Availability
67	Alamer et al. [87]	Generic (IoT)	Confidentiality, and Integrity
68	Rajawat et al. [88]	Generic (IoT)	Confidentiality, Integrity, and Availability
69	Deebak et al. [89]	Military (Intelligent Drone-assisted Zone Surveillance)	Confidentiality, and Integrity
70	Escaleira et al. [90]	Generic (IoT)	Confidentiality, Integrity, and Availability
71	Nyangaresi et al. [91]	Generic (IoT)	Confidentiality, and Integrity
72	Kaushik et al. [92]	Generic (IoT)	Confidentiality, and Integrity
73	Patruni et al. [93]	Healthcare (Internet of Medical Things)	Confidentiality, and Integrity
74	Alcaraz et al. [94]	Generic (IoT)	Confidentiality, Integrity, and Availability
75	Xu et al. [95]	Generic (IoT)	Availability
76	Babu et al. [96]	Generic (IoT)	Confidentiality, Integrity, and Availability
77	Valadares et al. [97]	Generic (IoT)	Confidentiality, Integrity, and Availability
78	Kumar et al. [98]	Generic (IoT)	Confidentiality, Integrity, and Availability
79	Rajawat et al. [99]	Healthcare (Internet of Medical Things)	Confidentiality, and Integrity

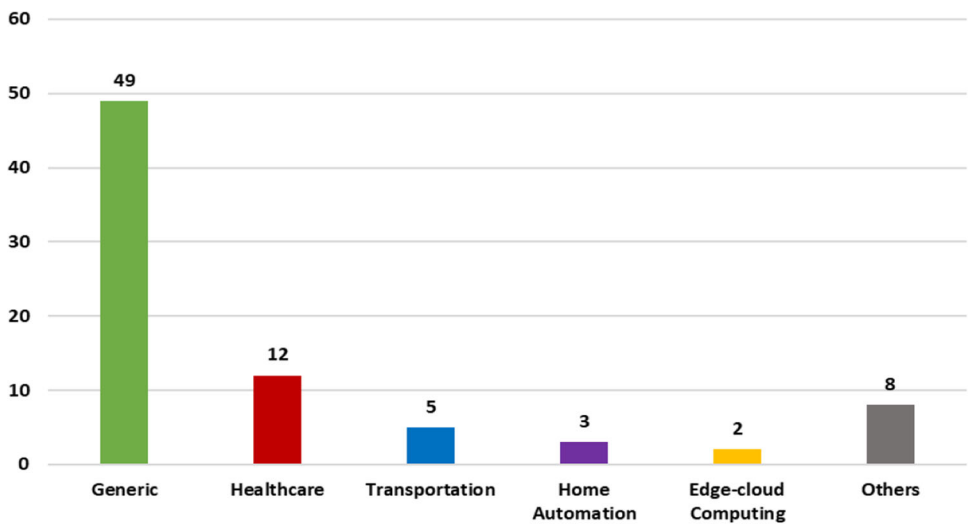

Fig. 6 Comparisons of application domains of the included studies

observed environment data. Finally, an application layer provides a user with application-specific services.

From Fig. 7 (RQ4), we infer that 14 out of 79 studies address all the operational layers. For instance, Lewis et al. [36] presented a secure and privacy-preserving collision avoidance system which addresses perception (through vehicle speed sensors), network (via 5G network), and application layer (use of roadside cloud). Furthermore, we infer that the included studies predominantly (i.e., 47 out of 79 studies) addressed network and application layers. For instance,

Table 9 Development lifecycle phase and operational layer in included studies

S. no.	Authors [References]	Development lifecycle phase	Operational layer
1	Raghu et al. [15]	System Design, System Development, and Implementation	Network Layer, and Application Layer
2	Jorge et al. [16]	System Design, and System Development	Network Layer, and Application Layer
3	B.D. et al. [17]	System Design, System Development, and Implementation	Network Layer, and Application Layer
4	Hiten [18]	System Design, System Development, and Implementation	Network Layer, and Application Layer
5	Minahil et al. [19]	System Design, System Development, and Implementation	Network Layer, and Application Layer
6	Huaqun et al. [20]	System Design, System Development, and Implementation	Network Layer, and Application Layer
7	Will [21]	System Design, System Development, and Implementation	Network Layer, and Application Layer
8	Alberto et al. [22]	System Design	Network Layer
9	Mohammed et al. [23]	N/A	N/A
10	Sultan et al. [24]	System Design	Perception Layer, Network Layer, and Application Layer
11	Raluca et al. [25]	System Design	Perception Layer, Network Layer, and Application Layer
12	Amril et al. [26]	Implementation	Network Layer, and Application Layer
13	Mehdi et al. [27]	System Design, and Implementation	Network Layer, and Application Layer
14	Prabhakar et al. [28]	System Design, System Development, and Implementation	Network Layer, and Application Layer
15	Vishal et al. [29]	System Design, System Development, and Implementation	Network Layer, and Application Layer
16	Anurag et al. [30]	System Design, System Development, and Implementation	Network Layer, and Application Layer
17	Zbigniew et al. [31]	System Design	Network Layer, and Application Layer
18	Amir et al. [32]	System Design, System Development, and Implementation	Network Layer
19	Kubra et al. [33]	System Design, System Development, and Implementation	Network Layer
20	Hussain et al. [34]	System Design, System Development, and Implementation	Network Layer, and Application Layer

Table 9 (continued)

S. no.	Authors [References]	Development lifecycle phase	Operational layer
21	Md. Ashraf et al. [35]	System Design, System Development, and Implementation	Perception Layer, Network Layer, and Application Layer
22	Lewis et al. [36]	System Design, System Development, and Implementation	Perception Layer, Network Layer, and Application Layer
23	Nilupulee et al. [37]	System Design, System Development, and Implementation	Network Layer, and Application Layer
24	Amir et al. [38]	System Design, System Development, and Implementation	Network Layer
25	Rasheed et al. [39]	System Design, System Development	Network Layer, and Application Layer
26	Bocu et al. [40]	System Design, and Implementation	Network Layer, and Application Layer
27	Abdellah et al. [42]	Implementation	Network Layer, and Application Layer
28	Mishra et al. [43]	System Design	Perception Layer, Network Layer, and Application Layer
29	Dzogovic et al. [44]	Implementation	Perception Layer, and Network Layer
30	Kisung et al. [45]	System Design, and Implementation	Network Layer, and Application Layer
31	Zhixin et al. [46]	System Design, and Implementation	Network Layer, and Application Layer
32	Suleyman et al. [47]	Implementation	Network Layer, and Application Layer
33	Christian et al. [48]	System Design, and Implementation	Network Layer, and Application Layer
34	Deebak, et al. [49]	Implementation	Network Layer
35	Prabhakar et al. [50]	System Design, System Development, and Implementation	Network Layer, and Application Layer
36	Awaneesh et al. [53]	System Design, and Implementation	Network Layer, and Application Layer
37	Yuanjie et al. [54]	System Design, System Development, and Implementation	Perception Layer, Network Layer, Application Layer
38	Valerian et al. [55]	Implementation	Network Layer, and Application Layer
39	Shubham et al. [56]	Implementation	Network Layer, and Application Layer
40	Mustafa et al. [57]	Implementation	Perception Layer, and Network layer
41	Vibha et al. [58]	System Design, and Implementation	Perception Layer, Network Layer, and Application Layer
42	Vincent [59]	System Design, and Implementation	Network Layer, and Application Layer

Table 9 (continued)

S. no.	Authors [References]	Development lifecycle phase	Operational layer
43	Awaneesh et al. [60]	System Design, and Implementation	Network Layer, and Application Layer
44	Mattia et al. [61]	System Design, and Implementation	Perception Layer, Network Layer, and Application Layer
45	Reshmi [63]	Implementation	Network Layer, and Application Layer
46	Sankar et al. [65]	Implementation	Network Layer, and Application Layer
47	Rahman et al. [66]	Implementation	Perception Layer, Network Layer, and Application Layer
48	Dakshita [67]	Implementation	Perception Layer, Network Layer, and Application Layer
49	Ismaila et al. [68]	System Design, and Implementation	Network Layer, and Application Layer
50	Aruna et al. [70]	Implementation	Network Layer, and Application Layer
51	Jinwen et al. [71]	System Design, and Implementation	Network Layer, and Application Layer
52	Fábio et al. [72]	Implementation	Perception Layer, Network Layer, and Application Layer
53	Rao et al. [73]	System Design, and Implementation	Network Layer
54	Pronaya et al. [74]	System Design, and Implementation	Network Layer
55	Xianjun et al. [75]	System Design, and Implementation	Network Layer, and Application Layer
56	Deepashika et al. [76]	System Design, and Implementation	Perception Layer, Network Layer, and Application Layer
57	Guilin et al. [77]	System Design, and implementation	Perception Layer, Network Layer, and Application Layer
58	Nilesh et al. [78]	System Design	Network Layer, and Application Layer
59	Vincent et al. [79]	System Design	Perception Layer, and Network Layer
60	Lilhore et al. [80]	System Design, System Development, and Implementation	Network Layer
61	Borgohain et al. [81]	System Design, System Development, and Implementation	Network Layer, and Application Layer
62	Jesus Martins et al. [82]	System Design, System Development, and Implementation	Network Layer
63	Benlloch-Caballero et al. [83]	System Design, System Development, and Implementation	Network Layer

Table 9 (continued)

S. no.	Authors [References]	Development lifecycle phase	Operational layer
64	Ge et al. [84]	System Design, and Implementation	Network Layer, and Application Layer
65	Singh [85]	System Design, System Development, and Implementation	Network Layer, and Application Layer
66	Alotaibi et al. [86]	System Design, System Development, and Implementation	Network Layer
67	Alamer et al. [87]	System Design, System Development, and Implementation	Network Layer, and Application Layer
68	Rajawat et al. [88]	System Design, System Development, and Implementation	Network Layer
69	Deebak et al. [89]	System Design, and Implementation	Network Layer, and Application Layer
70	Escaleira et al. [90]	System Design, System Development, and Implementation	Network Layer, and Application Layer
71	Nyangaresi et al. [91]	System Design, and System Development	Network Layer, and Application Layer
72	Kaushik et al. [92]	System Design, System Development, and Implementation	Network Layer
73	Patruni et al. [93]	System Design, System Development, and Implementation	Network Layer, and Application Layer
74	Alcaraz et al. [94]	System Requirements, and System Design	Perception Layer, Network Layer, and Application Layer
75	Xu et al. [95]	System Design	Network Layer, and Application Layer
76	Babu et al. [96]	System Design, System Development, and Implementation	Network Layer, and Application Layer
77	Valadares et al. [97]	System Design	Network Layer
78	Kumar et al. [98]	System Design, System Development, and Implementation	Network Layer, and Application Layer
79	Rajawat et al. [99]	System Design, System Development, and Implementation	Network Layer, and Application Layer

Vishal et al. proposed a novel key exchange and authentication protocol which addressed network and application layers [29]. In addition, we also infer that 3 out of 79 studies addressed perception and network layers. For instance, Dzogovic et al. implemented a VPN + transport network connecting the centralized unit of a 5G C-RAN to the core network within the transport network, which addressed perception and network layers [44]. Finally, we infer that 14 out of 79 studies addressed network layers. Importantly, all the included studies addressed network layer due to the focus of this study involving 5G and beyond. Table 10 elaborates the pros and cons of included studies in this SLR.

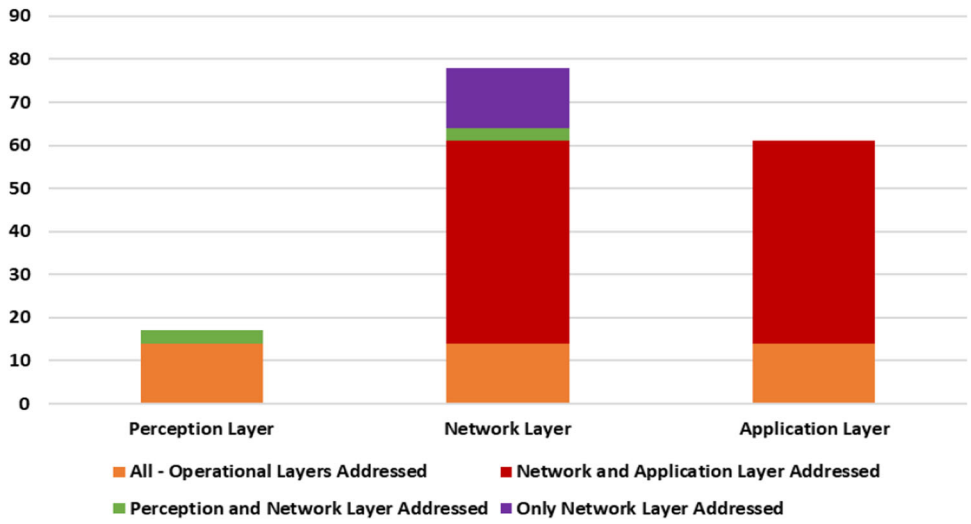

Fig. 7 Operational layers addressed in the included studies

7 Open challenges and proposed tentative solutions

Based on our classification and characterization of existing research, and identification and analysis of trends, strategies, key patterns, mechanisms, performance evaluation, validation parameters and challenges for cybersecurity and resilience for 5G and beyond-enabled IoT in the included studies as a part of this SLR, we identified the following research challenges and proposed their respective tentative solutions.

1. *New Security Vulnerabilities* 5G has a different security architecture than 4G, so it comes up with different security vulnerabilities (For example, one identified new vulnerability in 5G networks is device fingerprinting [163]). The studies considered in this SLR did not focus on addressing the new 5G vulnerabilities (e.g., device fingerprinting). Therefore, we need to consider how to deal with new security vulnerabilities for developing 5G and beyond-enabled IoT systems.

Proposed Tentative Solution: A possible solution to address this new vulnerability is that the network service providers must include the authentication mechanism so device radio capabilities can be accessed once adequate security is established. Modifying certain core network capabilities can cause power drain attacks on Narrowband (NB)-IoT devices.

2. *Lack of Standard Architecture* From our analysis on security standards, there is no standard architecture for 5G, which is widely accepted, thus lacking in offering optimal risk prevention methodologies. Different researchers and service providers have come up with different measures in handling cyber risks for 5G and beyond-enabled IoT.

Proposed Tentative Solution: A generic benchmark based on any reputable standard bodies, such as NIST, ISO, IEC will be crucial for 5G and beyond-enabled IoT systems. This will not only provide a common understanding of new communication systems, but also act as a backbone for compliance for analyzing cyber risk in 5G and beyond-enabled IoT.

3. *Self-Healing Communication* There is a need for reliable and high-speed self-healing in 5G and beyond communication networks of the IoT, especially during times of faults, and cyber-attacks. This also needs to ensure a sufficient security and privacy level. From Table 5, there is only one study which focused on self-healing [63]. However, it lacks performance evaluation utilizing real-time scenarios and also DL techniques have not been used.

Proposed Tentative Solution: In order to validate the legitimacy of a large number of nodes, users, servers, and devices in 5G and beyond communication networks of IoT, autonomous and dynamic adaptive key management schemes and mutual authentication protocols should be developed/evaluated/adapted.

4. *Lack of Application-Oriented Empirical Research* There is a lack of application-oriented and feasible empirical research in the development of security approaches for 5G and beyond-enabled IoT. This is also evident from studies that we analyzed in this SLR [33, 37].

Proposed Tentative Solution: The development of 5G and beyond-enabled IoT testbeds, which would aid in the research on development and evaluation of techniques/tools/methods for cybersecurity of 5G and beyond-enabled IoT.

5. *Lack of Proper Authentication Process* In the 5G and beyond-enabled IoT systems, the core network and radio access capabilities may be obtained from the end users without following proper authentication process [164]. This can be one of the key vulnerabilities in 5G and beyond networks which allows an active or passive attacker to steal the identity of devices. From Table 5, there are different studies from our SLR which focused on authentication in the context of 5G and beyond-enabled IoT [16, 19, 21, 26, 29, 45, 49, 53, 58,

Table 10 Pros and Cons of included studies

S. no.	Authors [References]	Pros	Cons
1	Raghu et al. [15]	Dynamic key generation scheme is proposed for secure 5G mobile communication which reduces computational overheads	The analysis is focused on IoT network scenarios without trusted third parties
2	Jorge et al. [16]	Improves Braeken's protocol for 5G (2-pass AKA) for addressing privacy issues and vulnerabilities, and also offers an enhanced version with forward secrecy for low-cost IoT devices	Prone to DoS attacks due to trade-offs between privacy and availability when achieving unlinkability through symmetric-key protection
3	B.D. et al. [17]	Presented a robust blockchain-based lightweight distributed architecture which addresses limitations associated with centralized architectures	The use of smart contracts to improve transparency and speed up transaction speeds is lacking
4	Hiten [18]	Developed a lightweight scheme for identity privacy in 5G mobile networks, addressing IoT device constraints. It is computationally efficient	The security analysis and formal analysis are conducted using specific tools. There is a lack of validation in practical applications
5	Minahil et al. [19]	Developed an e-Health cloud protocol to enhance the security by preventing major attacks and reducing the computation and communication costs	Adaptive authentication was not considered
6	Huaqun et al. [20]	Developed a blockchain-based remote data integrity checking (RDIC) scheme for IoT-generated big data in 5G networks and reduce computational cost and communication cost	The study is limited to the IoT generated data. Different RDIC schemes are needed for different types of data for example data based on privacy requirements, security requirements, data ownership
7	Will [21]	The developed approach increases cybersecurity resilience and enables decentralized access and connectivity of users	An alternative neural network based approach can be introduced to validate the blockchain and to increase the performance
8	Alberto et al. [22]	This study contributes to understanding the IoT market dynamics through visibility graphs for price volatility into complex networks	This study does not focus on using the time series clustering with multiplex networks
9	Mohammed et al. [23]	Contribute to highlighting adversarial AI roles for providing automation solutions including security for 5G-enabled IoT	The details of the case study are not presented including the performance evaluation metrics and other important parameters

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
10	Sultan et al. [24]	Explored the potential of fog and edge computing to enhance the key features such as self-adaptiveness and resilience in cyber-physical systems in the 5G era and IoT deployment	In order to upgrade services to the growing smart IoT applications, a more effective framework and services are needed
11	Raluca et al. [25]	This paper highlights the importance of remote healthcare services	The risks of healthcare IoT including loss of data due to connectivity issues, and the necessity of robust integration with AI technologies are not addressed
12	Amril et al. [26]	Investigated the aggregate authentication scheme for massive IoT in 5G networks which shows better computation time and short aggregation signature size	When an authenticator cannot verify messages, repeated authentication processes are required and communication issues must be addressed
13	Mehdi et al. [27]	Proposed jamming-resistant scheme to ensure high-quality communication. It focuses on maximizing the ESR to provide robustness against jamming	The proposed scheme may not be efficient for the complex attacks and it may also have scalability issues
14	Prabhakar et al. [28]	Presented a distributed threat analytics and response system by integrating SDN and Fog/Edge computing for robust security	The proposed approach does not include the extended attack scenarios
15	Vishal et al. [29]	For mobile Xhaul networks security, developed a key exchange and authentication protocol capable of ensuring privacy and perfect forward secrecy without compromising performance	The method needs further advancement as the mobile Xhaul networks face growing security challenges
16	Anurag et al. [30]	This paper focuses on the detection and elimination of security threats through a network slicing model based on neural networks	The model can be trained in real time based device and traffic behavior data utilizing reinforcement learning and recurrent learning
17	Zbigniew et al. [31]	Examined the capability of end-to-end slice isolation in a realistic ecosystem of heterogeneous multi-vendor multi-tenant 5G network	*Network slicing:* needs mechanism for E2E slicing, security management and accounting users. *Slice isolation:* Observation of isolation in actual network states using new isolation methods and security network functions

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
18	Amir et al. [32]	Modeling and simulating the interactions between diverse smart home technologies and the core internet to increase resilience	Development of simulation techniques for comprehensive understanding of multilevel architecture in diverse networks is missing
19	Kubra et al. [33]	The proposed SDN uses secure clustering to ensure QoE and QoS for scalable IoT communication, addressing issues such as mobility, priority, power and trust	The experiments involving the real testbed and definition of the trust parameters are missing
20	Hussain et al. [34]	Made an effort towards development of flexible and secure authentication of IIoT components in 5G environments that shows the significance of less delays	Lack in the experiments involving real testbeds
21	Md. Ashraf et al. [35]	A blockchain-based decentralized eHealth architecture is more feasible in the processing and storage of RPM data	Development of a dynamic storage selection algorithm based on patient privacy and security preferences is missing
22	Lewis et al. [36]	Presented a secure and privacy-preserving collision avoidance system that shows better efficiency in terms of computation and communication overhead	Need to focus on the security consideration such as availability for 5G fog based internet of vehicles
23	Nilupulee et al. [37]	Lightweight cryptography algorithms for smart IoT, focusing on the effective performance of Long-Range Wide Area Network (LoRaWAN)	Development of new algorithms and implementation is missing
24	Amir et al. [38]	Examined the resilience of smart homes	Complex and diverse networks may pose some challenges to the proposed approach
25	Rasheed et al. [39]	Presented the challenges associated with integrating 5G with the Vehicular Ad Hoc Network (VANET) and proposed an efficient and adaptive secure architecture for vehicular networks	This study presents the high-level architecture
26	Bocu et al. [40]	Developed a real-time intrusion detection system based on machine learning for software defined 5G networks	This study does not consider generalizability and scalability issues
27	Abdellah et al. [42]	Improved network security, reliability, and QoS through the development of a machine learning algorithm for predicting delay in IoT and tactile internet	To enhance the accuracy in traffic predictions, the deep learning algorithm are not developed incorporating robust loss functions and dynamic IoT parameters

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
28	Mishra et al. [43]	Proposed architecture for real-time and seamless health monitoring	The proposed architecture lacks clarity and requires validation in a real and diverse environment
29	Dzogovic et al. [44]	Developed an approach that enhances the isolation of the network slices by leveraging the enhanced VPN + technology	The approach lacks performance evaluation
30	Kisung et al. [45]	Focused on bringing efficient solution to overcome cyber security weaknesses using informal and formal approaches	The results are acquired from the simulation, and are based on merely preliminary analysis
31	Zhixin et al. [46]	This study involves the automatic validation process for security events to check compliance with 3GPP specifications	It is not specifically mentioned what is the scalability for different critical sectors
32	Suleyman et al. [47]	The proposed approach allows optimization of the utilities using external and internal incident scenarios	Multi-level hierarchies and complex scenarios were not considered
33	Christian et al. [48]	The developed scheme offers effective solution to prevent rank attacks	There is a need to implement this scheme on real-time systems
34	Deebak, et al. [49]	The proposed framework offers security protection against cyber-attacks	The presented results are still preliminary
35	Prabhakar et al. [50]	This study offers viable framework to resist the communication channel attacks	Lacks in providing concrete evidence and specifications for threat actors
36	Awaneesh et al. [53]	The proposed protocol provides trade-off between overheads and security features	Does not clearly elaborate how the developments can be used in diverse real-time scenarios
37	Yuanjie et al. [54]	The proposed stateless solution has a good performance under extreme mobility conditions	Not a robust solution, it becomes costly when used in harsh outer space
38	Valerian et al. [55]	Robust federated model for malware detection	Impact of cyber-attacks was only based on supervised learning scenarios, whereas unsupervised learning was not considered
39	Shubham et al. [56]	This study offers resource efficient security protocol	Does not focus on real-time implementation
40	Mustafa et al. [57]	The proposed protocol ensures the secure assessment of data	Real-world IoT scenarios are not considered
41	Vibha et al. [58]	The proposed system offers energy efficient solution for dynamic environment	Does not provide balance between resource consumption and security in a peer-to-peer distributed scenario

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
42	Vincent [59]	Proposed token derivation scheme requires less complex computation	This study does not focus how to provide adaptive security for dynamic scenarios
43	Awaneesh et al. [60]	This research offers solution which require less overheads for protecting against unknown attacks	Does not focus on providing group authentication while dealing with cyber threats
44	Mattia et al. [61]	The proposed architecture is dynamic and scalable in detecting phishing attacks	The presented results are still preliminary
45	Reshmi [63]	This study offers automated self-Healing approach for anomaly detection	Accuracy needs to be improved, and should be focused on real-time scenarios
46	Sankar et al. [65]	This study reduces end-end delay and improves security for peer-peer networks	Results need to be validated based on different real-time scenarios
47	Rahman et al. [66]	The proposed framework provides sustainability and security for connected healthcare	In the developed system, accuracy can be improved, and security requirements by bringing hospitals and end-users in the loop needs to be incorporated
48	Dakshita [67]	The developed autonomous scheme is suitable for diverse applications	Alternative neural networks can be applied for validating the blockchain and for enhancing the performance
49	Ismaila et al. [68]	The developed protocol can be useful for practical deployment	The experiments should involve real testbed for analyzing performance in real-time
50	Aruna et al. [70]	The proposed solution has better speed for cloud to cloud data migration	Sufficient details are not provided about deployment and how the performance in terms of accuracy needs additional attention
51	Jinwen et al. [71]	The proposed model enhances the scalability and security of crowdsensing systems	Real-world scenarios were not considered
52	Fábio et al. [72]	Multi-layered platform suitable for applications having low latency and high-density requirements	Security of communications between different devices moving from an area to another was not focused
53	Rao et al. [73]	Hyperledger fabric framework is developed for offering high performance and scalability	Does not focus on real-time implementation
54	Pronaya et al. [74]	Proposed scheme is suitable for data offloading in energy-constrained applications	Autonomous security can be included for detecting threats in real-time
55	Xianjun et al. [75]	This study improves confident information coverage for effectively deploying smart nodes in IoT applications	Results need to be validated based on different real-time scenarios

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
56	Deepashika et al. [76]	This study proposed the resource efficient forensics architecture for IoT environments	Lack of offering standard solutions for different critical applications
57	Guilin et al. [77]	This study developed the effective model for identifying PD in power cables	The details of the case study are not presented
58	Nilesh et al. [78]	The empirical findings demonstrated that the suggested approach excels in terms of both accuracy and controller efficiency	This study has not explored network-related challenges in SDN-based IoT applications, nor has it enhanced their performance with respect to energy efficiency and data rates
59	Vincent et al. [79]	The proposed protocol provides numerous security features while incurring relatively low communication and computation costs	The performance in machine learning aspect of this protocol is not compared with related schemes
60	Lilhore et al. [80]	The proposed method blends lightweight structures, transfer learning and fine tuning for specific tasks to efficiently detect network intrusions under resource constraints and changing conditions	A limitation of this study is the model's time complexity and its lack of implementation in a real environment
61	Borgohain et al. [81]	The proposed scheme is lightweight and efficient in terms of both computational and communication costs, especially when compared to other prominent works in this field	Lack of efficient solutions for other use case scenarios of D2D authentication
62	Jesus Martins et al. [82]	The proposed solution is demonstrated to offer monitoring and security solutions for an entire network slice transparently, ensuring adherence to privacy standards with minimal interventions by the network slice tenant	The proposed solution is limited to small subset of applications
63	Benlloch-Caballero et al. [83]	The proposed system supports both edge and core networks, aiming to detect, analyze, and orchestrate responses to mitigate large-scale DDoS attacks	Resource constraints are a significant obstacle in replicating the scenarios and attacks conducted in this research
64	Ge et al. [84]	By employing the moving-horizon computation, the proposed zero-trust framework has developed a robust security model that can adjust to unforeseen environmental shifts and evolving attacks	The proposed zero-trust framework is not evaluated using a realistic testbed environment or implemented in a real environment

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
65	Singh [85]	The proposed protocol employs low-cost cryptographic operations and message aggregation techniques to achieve its objectives, which lowers computational costs, bandwidth usage, and signaling load within the IoMT network, making it well-suited for low-power IoMT devices	Only mathematical analysis of the protocol is performed, which lacks experimentation
66	Alotaibi et al. [86]	The proposed framework for intrusion detection systems enhances scalability and communication efficiency	Adaptive and zero day attack detection is lacking
67	Alamer et al. [87]	The proposed scheme incorporates a feature to decrease latency issues arising from the cost of cryptographic computations	Suit of secure mechanisms that ensure privacy while minimizing data storage and cryptographic overhead is lacking
68	Rajawat et al. [88]	The proposed algorithm is accessible and distributed for monitoring the security of IoT-based sensors, which also addresses the challenges of big data presented in the context of IoT security	Generalizability and scalability of the proposed algorithm is not addressed
69	Deebak et al. [89]	The proposed authentication scheme, while less cost-efficient in terms of computation, communication, bandwidth, and energy, is designed to improve the performance efficiency of surveillance systems	Validation of the proposed authentication scheme's complexity to determine the execution cost in surveillance networks is missing
70	Escaleira et al. [90]	The proposed system is effective in protecting a CNF against zero-day-based attacks	The protection capability can be significantly improved when used with other MTD techniques by incorporating various movement techniques, which is currently lacking
71	Nyangaresi et al. [91]	The proposed protocol has demonstrated the ability to provide anonymity, mutual authentication, and key secrecy in both forward and backward directions	Formal verification of the security features in the proposed protocol is missing
72	Kaushik et al. [92]	The proposed symmetric key algorithm is superior mainly in terms of its computation, decryption, and encryption time	Cipher text and public key size generated can be decreased in the proposed symmetric key algorithm

Table 10 (continued)

S. no.	Authors [References]	Pros	Cons
73	Patruni et al. [93]	The proposed system not only reduces operational costs like computation and communication, but also offers security efficiencies making it well-suited for resource-limited IoT networks	A current limitation is that the proposed system's efficiencies, such as convergence rate and clinical accuracy, could be improved
74	Alcaraz et al. [94]	The proposed framework ensures QoS anticipated in 6G networks and to meet the goals of industry 5.0	The results are not validated from a practical standpoint. The development of adaptive FL techniques for advanced detection systems supported by DTNs remain unexplored
75	Xu et al. [95]	The proposed random structure code that leverages channel characteristics and code redundancy to improve the security of URLLC access	This study has not investigated the optimization of code structure or the design of quantum algorithms
76	Babu et al. [96]	The proposed work ensures secure communication between edge devices, offering protection against DDoS and side-channel attacks	Aggregate signature scheme for short signatures is missing and a lack of an efficient verification process for all edge devices in the blockchain system
77	Valadares et al. [97]	Threat model that can support regulatory institutions for the cyber risk management process of 5G-IoT deployment	Tool that can search for vulnerabilities using specific databases and calculate a risk score based on the CVSS of each identified vulnerability in an IoT application is lacking
78	Kumar et al. [98]	The proposed authentication protocol is demonstrated to be efficient and secure offering better computational and communication costs compared to other relevant protocols through simulation	Evaluation of the proposed authentication protocol is limited as it is not applied in a testbed/real environment
79	Rajawat et al. [99]	As a part of the proposed architecture, communication mechanism operating on a fluid computing architecture, characterized by its low overhead and secure storage capabilities	In the proposed architecture, protocols for secure data sharing is overlooked when it comes to linking multiple healthcare providers and stakeholders

60, 65, 68, 79, 81, 84, 85, 89, 91, 93, 98]. However, they are mainly static in nature and possess adaptability and scalability issues.

Proposed Tentative Solution: The development of fuzzy logic- or advanced data analytics-based dynamic authentication mechanisms to analyze the new vulnerabilities in 5G networks while considering the dynamic and scalable properties of edge and IoT.

6. *Man-in-the-middle Attacks* 5G and beyond networks will narrowly handle data transmission between end-to-end devices, which reduces the possibility of eavesdropping via the communication channel. However, there is a possibility for man-in-the-middle attacks directed at 5G and beyond frequencies which may be a crucial security concern. From Table 5, there are various studies which addressed intrusion detection [28, 40, 80, 83, 86]. However, these are not evaluated against man-in-the-middle attacks.

Proposed Tentative Solution: There is a need to design/develop new man-in-the-middle attack intrusion detection mechanism (or modify existing techniques) to provide protection reducing the probability of eavesdropping via the communication channel in 5G and beyond-enabled IoT systems

7. *Secure Communication in Extreme Wave-Denied Surroundings* 5G and beyond will play an important role in different applications and use cases which may include extreme wave-denied surroundings. Molecular Communication (MC) systems have enormous potential to be a new physical layer for 6G to deal with such surroundings. This kind of communications will handle highly sensitive information with several security and privacy challenges on the communication, authentication, and encryption process. Various researchers have already validated that MC is prone to attacks such as collision, jamming, and tampering [139]. However, based on our analysis in this study, there are a lack of studies that address the security and privacy of MC technology.

Proposed Tentative Solution: Molecular signals inside our bodies can play a role as harmonization commands between devices, drug delivery, and secure communication between entities. Therefore, an efficient authentication mechanism using MC technology for 5G and beyond-enabled IoT applications is essential so that only authorized entities can access the data.

8. *AI Security* From Table 5, there are different studies which use different AI methods as the underlying approach for developing techniques/mechanisms/tools for ensuring 5G and beyond-enabled IoT security and resilience [21, 30, 40, 42, 48, 63, 78, 80, 88]. However, there is a lack of focus on AI security in such studies and has not been addressed. AI is essential for security in various stages of cybersecurity protection in 5G and beyond-enabled IoT applications. One of the key challenges in these systems is AI security itself, since AI may face challenges in data resilience, trustworthiness, and ethics issues.

Proposed Tentative Solution: One of the potential solutions is to develop dynamic AI models which can auto-update the code in case of any new vulnerability or security threats in the system related to AI security.

9. *Privacy in IoT-Edge Computing* IoT-Edge computing-based servers have the potential to extract meaningful analytics from a large number of IoT devices. This is essential for different systems like 5G and beyond-enabled IoVs/smart traffic, which is evident from [20]. However, there are privacy concerns when data providers offer edge applications for direct access to their embedded services.

Proposed Tentative Solution: Privacy-preserving techniques and models can be used in 5G and beyond-enabled IoT to address this issue. Blockchain and federated learning are techniques that have been predominantly used in domains such as energy, health for privacy-preserving data aggregation and perhaps address the above-mentioned challenge.

10. *Lack of Dynamic and Automated Trust Management* 5G and beyond-enabled IoT systems involve communication between IoT devices and also with remote servers. However, from Table 5 on current techniques/mechanisms/tools developed, there is a lack of framework/method that enables dynamic and automated trustworthy communication.

Proposed Tentative Solution: The application of AI techniques in dynamic and automated trust evaluation, prediction, and management can be investigated. Furthermore, the lightweight trust management mechanism needs to be developed for IoT systems.

8 Concluding remarks and future research directions

This study focused on providing a survey of the recent developments in the field of cybersecurity for 5G and beyond-enabled IoT. The developed taxonomy assisted us to classify and characterize the state-of-the-art. We have presented a detailed comparative analysis of the included studies in terms of different security aspects, standards, methods and tools, security metrics, validation mechanisms, application domains, open challenges, and respective tentative solutions. The major security aspects for the 5G and beyond-enabled IoT as per analysis from the existing studies are authentication and access control (35%), data security (8%), data integrity (5%), privacy (13%), resilience (9%), network security (9%), identity management (1%), security threat detection and prevention (10%), security and risk management (4%), forensics (1%), and other (5%). This SLR found out that there are some standards, specifications, and guidelines available for 5G and IoT by 3GPP, NIST, ENISA, GSMA, and ETSI, however they either focus on 5G security

or IoT security and do not consider 5G and beyond-enabled IoT as a whole. They also lack in providing security standards or guidelines for 6G enabled IoT because 6G technology is still in its development phase.

The main findings of this SLR suggest that most of the included studies have generic applications (62%), whereas 15% of the total studies focused on healthcare as their main targeted critical sector. Additionally, 34% of the included studies performed real-time implementations using hardware systems, while the remaining studies have either performed simulation or theoretical analysis for validation. The operational layers of 5G and beyond-enabled IoT are focused on the perception, network and application layers. The combination of network layer and application layer is the most focused layer (59%) in the included studies.

Along with identifying and analyzing the patterns, trends, methods in the existing literature, this SLR has also underlined key open research challenges and their tentative respective solutions which have potential to shape the future research efforts. In addition to what are mentioned in Sect. 7, we pinpoint the following future research directions: (1) to develop innovative methodologies by using modern technologies such as AI, Quantum Computing, and Digital Twins further to strengthen cybersecurity for 5G and beyond-enabled IoT applications, and (2) to present automated cyber risk assessment and quantification methodologies for securing 5G and beyond-enabled IoT infrastructures so that they can be protected against known/unknown cyber risks. We believe our results from this SLR will help to advance the research in 5G and beyond-enabled IoT domain.

Acknowledgements This research is funded from the Research Council of Norway through, the *SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS)*, with the Project Number #310105 in addition to INTPART projects, *Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway-US Partnership (RECYCIN)*, with the Project Number #309911 and *International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance)*, with the Project Number #337316.

Author contributions SP, SC, and AS did initial conceptualisation and data records analysis; SP, and HA prepared the study design and literature review; SP, SC, and AS were involved in writing-original draft preparation; and HA did writing-review and editing. All authors have revised the manuscript together, read and agreed to the published version of the manuscript.

Data availability Authors confirm that all relevant data are included in the article.

Declarations

Conflict of interest The authors declare that they do not have conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Heidari, A., Jabraeil Jamali, M.A.: Internet of Things intrusion detection systems: a comprehensive review and future directions. Clust. Comput. **26**(6), 3753–3780 (2023)
2. Nord, J.H., Koohang, A., Paliszkiewicz, J.: The Internet of Things: review and theoretical framework. Expert Syst. Appl. **133**, 97–108 (2019)
3. Sethi, P., Sarangi, S.R.: Internet of things: architectures, protocols, and applications. J. Electr. Comput. Eng. **2017** (2017)
4. Gartner, IoT Security Primer: Challenges and Emerging Practices (2020). https://www.gartner.com/en/doc/iot-security-primer-challenges-and-emerging-practices. Access date: 29.01.2024
5. US Homeland Security, 5G impacts on cybersecurity (2023). https://www.dhs.gov/sites/default/files/2023-09/23_0906_oia_01_5G_Security_508_Compliant.pdf. Access date: 29.01.2024
6. Al-Aqrabi, H., Johnson, A.P., Hill, R., Lane, P., Liu, L.: A multi-layer security model for 5G-enabled industrial Internet of Things. In: International Conference on Smart City and Informatization. Springer, pp. 279–292 (2019)
7. Chandra Shekhar Rao, V., Kumarswamy, P., Phridviraj, M., Venkatramulu, S., Subba Rao, V.: 5G enabled industrial internet of things (IIoT) architecture for smart manufacturing. In: Data Engineering and Communication Technology. Springer, pp. 193–201 (2021)
8. Guo, F., Yu, F.R., Zhang, H., Li, X., Ji, H., Leung, V.C.: Enabling massive IoT toward 6G: a comprehensive survey. IEEE Internet Things J.8(15), 11891-11915 (2021)
9. Woźniak, M., Zielonka, A., Sikora, A., Piran, M.J., Alamri, A.: 6G-enabled IoT home environment control using fuzzy rules. IEEE Internet Things J. **8**(7), 5442–5452 (2020)
10. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., ... & Poor, H. V. . 6G Internet of Things: A comprehensive survey. IEEE Internet Things Journal, 9(1), 359-383 (2021)
11. Shah, Y., Sengupta, S.: A survey on classification of cyber-attacks on IoT and IIoT devices. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). IEEE, pp. 0406–0413 (2020)
12. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. **20**(4), 3453–3495 (2018)
13. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. **6**(5), 8182–8201 (2019)
14. Eichhammer, P., et al.: Towards a robust, self-organizing IoT platform for secure and dependable service execution. Tagungsband des FB-SYS Herbsttreffens 2019 (2019)
15. Pothumarti, R., Jain, K., & Krishnan, P. . A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. Ambient Intell. Hum. Comput.12, 1–19 (2021)
16. Munilla, J., Burmester, M., Barco, R.: An enhanced symmetric-key based 5G-AKA protocol. Comput. Netw. **198**, 108373 (2021)
17. Deebak, B., Fadi, A.-T.: A robust and distributed architecture for 5G-enabled networks in the smart blockchain era. Comput. Commun. **181**, 293–308 (2022)
18. Choudhury, H.: HashXor: a lightweight scheme for identity privacy of IoT devices in 5G mobile network. Comput. Netw. **186**, 107753 (2021)
19. Ayub, M.F., Mahmood, K., Kumari, S., Sangaiah, A.K.: Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. Digit. Commun. Netw. **7**(2), 235–244 (2021)

20. Wang, H., He, D., Yu, J., Xiong, N.N., Wu, B.: RDIC: a blockchain-based remote data integrity checking scheme for IoT in 5G networks. J. Parallel Distrib. Comput. **152**, 1–10 (2021)
21. Serrano, W.: The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities. J. Netw. Comput. Appl. **175**, 102909 (2021)
22. Partida, A., Criado, R., Romance, M.: Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT. Electronics **10**(18), 2282 (2021)
23. Bohara, M.H., Patel, K., Saiyed, A., Ganatra, A.: Adversarial artificial intelligence assistance for secure 5G-enabled IoT. In: Blockchain for 5G-Enabled IoT. Springer, pp. 323–350 (2021)
24. Ahmad, S., Afzal, M.M.: Deployment of fog and edge computing in IoT for cyber-physical infrastructures in the 5G era. In: International Conference on Sustainable Communication Networks and Application. Springer, pp. 351–359 (2019)
25. Aileni, R.M., Suciu, G., Valderrama Sukuyama, C.A., Pasca, S.: Internet of Things and communication technology synergy for remote services in healthcare. In: IoT and ICT for Healthcare Applications. Springer, pp. 59–82 (2020)
26. Syalim, A., Anggorojati, B., Baek, J., Gerbi, D., You, I.: Aggregate authentication for massive Internet of Things in 5G networks. In: International Symposium on Mobile Internet Security. Springer, pp. 3–12 (2019)
27. Letafati, M., Kuhestani, A., Behroozi, H., Ng, D.W.K.: Jamming-resilient frequency hopping-aided secure communication for Internet-of-Things in the presence of an untrusted relay. IEEE Trans. Wirel. Commun. **19**(10), 6771–6785 (2020)
28. Krishnan, P., Duttagupta, S., Achuthan, K.: SDN/NFV security framework for fog-to-things computing infrastructure. Softw. Pract. Exp. **50**(5), 757–800 (2020)
29. Sharma, V., You, I., Leu, F.-Y., Atiquzzaman, M.: Secure and efficient protocol for fast handover in 5G mobile Xhaul networks. J. Netw. Comput. Appl. **102**, 38–57 (2018)
30. Thantharate, A., Paropkari, R., Walunj, V., Beard, C., Kankariya, P.: Secure5G: a deep learning framework towards a secure network slicing in 5G and beyond. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, pp. 0852–0857 (2020)
31. Kotulski, et al.: Towards constructive approach to end-to-end slice isolation in 5G networks. EURASIP J. Inf. Secur. **2018**(1), 1–23 (2018)
32. Modarresi, A., Symons, J.: Technological heterogeneity and path diversity in smart home resilience: a simulation approach. Procedia Comput. Sci. **170**, 177–186 (2020)
33. Kalkan, K.: SUTSEC: SDN utilized trust based secure clustering in IoT. Comput. Netw. **178**, 107328 (2020)
34. Al-Aqrabi, H., Lane, P., Hill, R.: Performance evaluation of multiparty authentication in 5G IIoT environments. In: Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health. Springer, pp. 169–184 (2019)
35. Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V.: Blockchain leveraged decentralized IoT eHealth framework. Internet of Things **9**, 100159 (2020)
36. Nkenyereye, L., Liu, C.H., Song, J.: Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles. Future Gener. Comput. Syst. **95**, 488–499 (2019)
37. Gunathilake, N.A., Buchanan, W.J., Asif, R.: Next generation lightweight cryptography for smart IoT devices: implementation, challenges and applications. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, pp. 707–710 (2019)
38. Modarresi, A., Symons, J.: Modeling and graph analysis for enhancing resilience in smart homes. Procedia Comput. Sci. **160**, 197–205 (2019)
39. Hussain, R., Hussain, F., Zeadally, S.: Integration of VANET and 5G security: a review of design and implementation issues. Future Gener. Comput. Syst. **101**, 843–864 (2019)
40. Bocu, R., Iavich, M., Tabirca, S.: A real-time intrusion detection system for software defined 5G networks. In: International Conference on Advanced Information Networking and Applications. Springer, Cham, pp. 436–446 (2021)
41. Adil, M., Song, H., Khan, M. K., Farouk, A., Jin, Z.: 5G/6G-enabled metaverse technologies: taxonomy, applications, and open security challenges with future research directions. J. Netw. Comput. Appl. 223, 103828 (2024)
42. Abdellah, A.R., Mahmood, O.A., Kirichek, R., Paramonov, A., Koucheryavy, A.: Machine learning algorithm for delay prediction in IoT and tactile internet. Future Internet **13**(12), 304 (2021)
43. Mishra, L., Vikash, Varma, S.: Seamless health monitoring using 5G NR for internet of medical things. Wirel. Person. Commun. **120**(3), 2259–2289 (2021)
44. Dzogovic, B., Mahmood, T., Santos, B., Feng, B., Do, V. T., Jacot, N., Van Do, T.: Advanced 5g network slicing isolation using enhanced vpn+ for healthcare verticals. In: Smart Objects and Technologies for Social Good: 7th EAI International Conference, GOODTECHS 2021, Virtual Event, September 15–17, 2021, Proceedings 7. Springer, pp. 121–135 (2021)
45. Park, K., Park, Y.: On the security of a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks. Appl. Sci. **12**(9), 4265 (2022)
46. Wen, Z., Pacherkar, H.S., Yan, G.: VET5G: a virtual end-to-end testbed for 5G network security experimentation. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, pp. 19–29 (2022)
47. Uslu, S., et al.: Trustability for resilient internet of things services on 5G multiple access edge cloud computing. Sensors **22**(24), 9905 (2022)
48. Miranda, C., Kaddoum, G., Boukhtouta, A., Madi, T., Alameddine, H.A.: Intrusion prevention scheme against rank attacks for software-defined low power IoT networks. IEEE Access **10**, 129970–129984 (2022)
49. Deebak, B.D., Al-Turjman, F., Nayyar, A.: Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. Multimed. Tools Appl. **80**, 17103–17128 (2021)
50. Krishnan, P., Jain, K., Jose, P.G., Achuthan, K., Buyya, R.: SDN enabled QoE and security framework for multimedia applications in 5G networks. ACM Trans. Multimed. Comput. Commun. Appl. **17**(2), 1–29 (2021)
51. Fang, D., Qian, Y., Hu, R.Q.: Open issues and future research directions for security and privacy in 5G networks (2024)
52. SinghKaunert, B.C.: Integration of cutting-edge technologies such as Internet of Things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. GLS Law J. **6**(1), 13–20 (2024)
53. Yadav, A.K., Misra, M., Pandey, P.K., Kaur, K., Garg, S., Chen, X.: A provably secure ECC-based multi-factor 5G-AKA authentication protocol. In: GLOBECOM 2022–2022 IEEE Global Communications Conference. IEEE, pp. 516–521 (2022)
54. Li, Y., Li, H., Liu, W., Liu, L., Chen, Y., Wu, J., et al.: A case for stateless mobile core network functions in space. In: Proceedings of the ACM SIGCOMM 2022 Conference, pp. 298–313 (2022)
55. Rey, V., Sánchez, P.M.S., Celdrán, A.H., Bovet, G.: Federated learning for malware detection in IoT devices. Comput. Netw. **204**, 108693 (2022)
56. Gupta, S., Parne, B.L., Chaudhari, N.S., Saxena, S.: SEAI: secrecy and efficiency aware inter-gNB handover authentication and key agreement protocol in 5G communication network. Wirel. Person. Commun. **122**(4), 2925–2962 (2022)

57. Al Sibahee, M.A., et al.: Stochastic security ephemeral generation protocol for 5G enabled Internet of Things. In: International Conference on Internet of Things as a Service. Springer, Cham (2021)
58. Jain, V., Kumar, B., Gupta, A.: Cybertwin-driven resource allocation using deep reinforcement learning in 6G-enabled edge environment. J. King Saud Univ. Comput. Inf. Sci. **34**(8), 5708–5720 (2022)
59. Nyangaresi, V.O.: Terminal independent security token derivation scheme for ultra-dense IoT networks. Array **15**, 100210 (2022)
60. Yadav, A.K., Misra, M., Pandey, P.K., Braeken, A., Liyange, M.: An improved and provably secure symmetric-key based 5G-AKA protocol. Comput. Netw. **218**, 109400 (2022)
61. Zago, M., Pérez, M.G., Pérez, G.M.: Early DGA-based botnet identification: pushing detection to the edges. Clust. Comput. 1–16 (2021)
62. Kasera, R.K., Gour, S., Acharjee, T.: A comprehensive survey on IoT and AI based applications in different pre-harvest, during-harvest and post-harvest activities of smart agriculture. Comput. Electron. Agric. **216**, 108522 (2024)
63. Reshmi, T.R., Azath, M.: Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Netw. Appl. **14**(1), 375–391 (2021)
64. Wang, J., Li, J., Liu, J.: Digital twin-assisted flexible slice admission control for 5G core network: a deep reinforcement learning approach. Future Gener. Comput. Syst. **153**, 467–476 (2024)
65. Sankar, S.P., Subash, T.D., Vishwanath, N., Geroge, D.E.: Security improvement in block chain technique enabled peer to peer network for beyond 5G and internet of things. Peer-to-Peer Netw. Appl. **14**(1), 392–402 (2021)
66. Rahman, M.A., Hossain, M.S., Showail, A.J., Alrajeh, N.A., Alhamid, M.F.: A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. Sustain. Cities Soc. **72**, 103083 (2021)
67. Reebadiya, D., Rathod, T., Gupta, R., Tanwar, S., Kumar, N.: Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5g networks. Peer-to-Peer Netw. Appl. **14**, 2757–2774 (2021)
68. Kamil, I.A., Ogundoyin, S.O.: A lightweight mutual authentication and key agreement protocol for remote surgery application in Tactile Internet environment. Comput. Commun. **170**, 1–18 (2021)
69. Sharma, R., Jindal, P., Singh, B.: Physical key generation using modified discrete wavelet transforms for the Internet of Things. Int. J. Comput. Digit. Syst. **15**(1), 207–220 (2024)
70. Aruna, M.G., Hasan, M.K., Islam, S., Mohan, K.G., Sharan, P., Hassan, R.: Cloud to cloud data migration using self sovereign identity for 5G and beyond. Clust. Comput. **25**(4), 2317–2331 (2022)
71. Xi, J., Zou, S., Xu, G., Lu, Y.: CrowdLBM: a lightweight blockchain-based model for mobile crowdsensing in the Internet of Things. Pervasive Mob. Comput. **84**, 101623 (2022)
72. Cabrini, F.H., de Castro Barros Filho, A., Maciel, D.B., Valiante Filho, F., Neto, A.J.V., Kofuji, S.T.: Helix Multi-layered: a context broker federation for an efficient cloud-to-things continuum. Ann. Telecommun. **77**(11–12), 867–879 (2022)
73. Ali, R.F., Muneer, A., Dominic, P.D.D., Taib, S.M.: Hyperledger fabric framework with 5G network for blockchain-based security of IoT smart home applications. In: 2021 International Conference on Decision Aid Sciences and Application (DASA). IEEE, pp. 1109–1114 (2021)
74. Bhattacharya, P., Patel, F., Tanwar, S., Kumar, N., Sharma, R.: MB-MaaS: mobile blockchain-based mining-as-a-service for IIoT environments. J. Parallel Distrib. Comput. **168**, 1–16 (2022)
75. Deng, X., et al.: Resilient deployment of smart nodes for improving confident information coverage in 5G IoT. ACM Trans. Sens. Netw. **18**(3), 1–21 (2022)
76. Rathnayake, D.J., Halgamuge, M.: Computation time estimation of switches and controllers process on 6G-based SDN-cyber security forensics architecture in the blockchain-based IoT environment. In: AI and Blockchain Technology in 6G Wireless Network. Springer, Singapore, pp. 135–164 (2022)
77. Wang, G., Xu, W., Wang, Y., Liu, H., Xiang, J., Tang, Z.: Application research of edge IoT proxy technology based on 5G in power demand side management system. In International Conference on Computer Engineering and Networks. Springer, Singapore, pp. 486–495 (2022)
78. Jadav, N.K., Nair, A.R., Gupta, R., Tanwar, S., Lakys, Y., Sharma, R.: AI-driven network softwarization scheme for efficient message exchange in IoT environment beyond 5G. Int. J. Commun. Syst. e5336, 1–20 (2022)
79. Nyangaresi, V.O., Ahmad, M., Alkhayyat, A., Feng, W.: Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert. Syst. **39**(10), e13126 (2022)
80. Lilhore, U.K., Dalal, S., Simaiya, S.: A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. Comput. Secur. **136**, 103560 (2024)
81. Borgohain, P., Choudhury, H.: A lightweight D2D authentication protocol for relay coverage scenario in 5G mobile network. Comput. Netw. **225**, 109679 (2023)
82. de Jesus Martins, R., Wickboldt, J.A., Granville, L.Z.: Assisted monitoring and security provisioning for 5G microservices-based network slices with SWEETEN. J. Netw. Syst. Manag. **31**(2), 36 (2023)
83. Benlloch-Caballero, P., Wang, Q., Calero, J.M.A.: Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Comput. Netw. **222**, 109526 (2023)
84. Ge, Y., Zhu, Q.: GAZETA: GAme-theoretic ZEro-trust authentication for defense against lateral movement in 5G IoT networks. IEEE Trans. Inf. Forensics Secur. 19, 540–554 (2023)
85. Singh, G.: GBEAKA: group-based efficient authentication and key agreement protocol for LPIoMT using 5G. Internet Things **22**, 100688 (2023)
86. Alotaibi, A., Barnawi, A.: IDSoft: a federated and softwarized intrusion detection framework for massive internet of things in 6G network. J. King Saud Univ. Comput. Inf. Sci. **35**(6), 101575 (2023)
87. Alamer, A.M.A., Basudan, S.A.M., Hung, P.C.: A privacy-preserving scheme to support the detection of multiple similar request-real-time services in IoT application systems. Expert Syst. Appl. **214**, 119005 (2023)
88. Rajawat, A.S., Goyal, S.B., Bedi, P., Kautish, S., Shrivastava, D.P.: Analysis assaulting pattern for the security problem monitoring in 5G-enabled sensor network systems with big data environment using artificial intelligence/machine learning. IET Wirel. Sens. Syst. 12049, 1–14 (2023)
89. Deebak, B.D., Hwang, S.O.: Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era. Comput. Netw. **225**, 109664 (2023)
90. Escaleira, P., Cunha, V.A., Gomes, D., Barraca, J.P., Aguiar, R.L.: Moving target defense for the cloud/edge telco environments. Internet Things **24**, 100916 (2023)
91. Nyangaresi, V.O., Ma, J., Al Sibahee, M.A., Abduljabbar, Z.A.: Packet replays prevention protocol for secure B5G networks. In: Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 2 (pp. 507–522). Springer, Singapore (2022)

92. Kaushik, A., Vadlamani, L.S.S., Hussain, M.M., Sahay, M., Singh, R., Singh, A.K., et al.: Post quantum public and private key cryptography optimized for IoT security. Wirel. Person. Commun. **129**(2), 893–909 (2023)
93. Patruni, M.R., Humayun, A.G.: PPAM-mIoMT: a privacy-preserving authentication with device verification for securing healthcare systems in 5G networks. Int. J. Inf. Secur. 23(1), 679-698 (2023)
94. Alcaraz, C., Lopez, J.: Protecting digital twin networks for 6G-enabled industry 5.0 ecosystems. IEEE Netw. **37**(2), 302–308 (2023)
95. Xu, D., Yu, K., Zhen, L., Choo, K.K.R., Guizani, M.: Quantum learning on structured code with computing traps for secure URLLC in industrial IoT scenarios. IEEE Internet Things J. 10(18), 16516-16530 (2023)
96. Babu, E.S., Barthwal, A., Kaluri, R.: Sec-edge: trusted blockchain system for enabling the identification and authentication of edge based 5G networks. Comput. Commun. **199**, 10–29 (2023)
97. Valadares, D.C., Will, N.C., Sobrinho, Á.Á.C., Lima, A.C., Morais, I.S., Santos, D.F.: Security challenges and recommendations in 5G-IoT scenarios. In: International Conference on Advanced Information Networking and Applications, pp. 558–573. Springer, Cham (2023)
98. Kumar, S., Banka, H., Kaushik, B.: Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. Wirel. Netw. 1–22 (2023)
99. Rajawat, A.S., Goyal, S.B., Chee, M.W., Kautish, S.: Securing the sustainable 5G enabled IoMT-Fog computing environment: a blockchain-based approach. In: International Conference on Sustainable Development through Machine Learning, AI and IoT, pp. 216–235. Springer, Cham (2023)
100. Gentry, C., Ramzan, Z.: Identity-based aggregate signatures. In: International Workshop on Public Key Cryptography. Springer, pp. 257–273 (2006)
101. Yuan, Y., Zhan, Q., Huang, H.: Efficient unrestricted identity-based aggregate signature scheme. PLoS ONE **9**(10), e110100 (2014)
102. Madakam, S., Lake, V., Lake, V., Lake, V.: Internet of Things (IoT): A literature review. Journal of Computer and Communications **3**(05), 164 (2015)
103. Li, S., Xu, L.D., Zhao, S.: The internet of things: a survey. Inf. Syst. Front. **17**(2), 243–259 (2015)
104. Farooq, M.S., Riaz, S., Abid, A., Umer, T., Zikria, Y.B.: Role of IoT technology in agriculture: a systematic literature review. Electronics **9**(2), 319 (2020)
105. Gómez-Chabla, R., Real-Avilés, K., Morán, C., Grijalva, P., Recalde, T.: IoT applications in agriculture: a systematic literature review. In: 2nd International Conference on ICTs in Agronomy and Environment. Springer, pp. 68–76 (2019)
106. Ben-Daya, M., Hassini, E., Bahroun, Z.: Internet of things and supply chain management: a literature review. Int. J. Prod. Res. **57**(15–16), 4719–4742 (2019)
107. Aryal, A., Liao, Y., Nattuthurai, P., Li, B.: The emerging big data analytics and IoT in supply chain management: a systematic review. Supply Chain Manag. Int. J. (2018)
108. Selvaraj, S., Sundaravaradhan, S.: Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl. Sci. **2**(1), 1–8 (2020)
109. Kashani, M.H., Madanipour, M., Nikravan, M., Asghari, P., Mahdipour, E.: A systematic review of IoT in healthcare: applications, techniques, and trends. J. Netw. Comput. Appl. **192**, 103164 (2021)
110. Mahmood, M.R., Matin, M.A., Sarigiannidis, P., Goudos, S.K.: A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. IEEE Access **10**, 87535–87562 (2022)
111. Qadir, Z., Le, K.N., Saeed, N., Munawar, H.S.: Towards 6G Internet of Things: recent advances, use cases, and open challenges. ICT express **9**(3), 296–312 (2023)
112. Kim, J.H.: 6G and Internet of Things: a survey. J. Manag. Anal. **8**(2), 316–332 (2021)
113. Hakak, S., Gadekallu, T.R., Maddikunta, P.K.R., Ramu, S.P., Parimala, M., De Alwis, C., Liyanage, M.: Autonomous vehicles in 5G and beyond: a survey. Veh. Commun. **39**, 100551 (2023)
114. Alotaibi, A., Barnawi, A.: Securing massive IoT in 6G: recent solutions, architectures, future directions. Internet Things **22**, 100715 (2023)
115. Bodkhe, U., Tanwar, S.: Network management schemes for IoT environment towards 6G: a comprehensive review. Microprocess. Microsyst. 103, 104928 (2023)
116. Akinbi, A.O.: Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. Wiley Interdiscip. Rev. Forensic Sci. **5**(6), e1496 (2023)
117. Cook, J., Rehman, S.U., Khan, M.A.: Security and privacy for low power iot devices on 5g and beyond networks: challenges and future directions. IEEE Access (2023)
118. Ahmad, R., Alsmadi, I.: Machine learning approaches to IoT security: a systematic literature review. Internet Things **14**, 100365 (2021)
119. Macedo, E.L., et al.: On the security aspects of Internet of Things: a systematic literature review. J. Commun. Netw. **21**(5), 444–457 (2019)
120. Mao, B., Liu, J., Wu, Y., Kato, N.: Security and privacy on 6g network edge: A survey. IEEE Commun. Surv. Tutor. 25(2), 1095–1127 (2023)
121. Jahid, A., Alsharif, M.H., Hall, T.J.: The convergence of blockchain, IoT and 6G: potential, opportunities, challenges and research roadmap. J. Netw. Comput. Appl. 217, 103677 (2023)
122. Mahmood, A., Beltramelli, L., Abedin, S.F., Zeb, S., Mowla, N.I., Hassan, S.A., Sisinni, E., Gidlund, M.: Industrial IoT in 5G-and-beyond networks: vision, architecture, and design trends. IEEE Trans. Ind. Inf. **18**(6), 4122–4137 (2021)
123. Irram, F., Ali, M., Naeem, M., Mumtaz, S.: Physical layer security for beyond 5G/6G networks: emerging technologies and future directions. J. Netw. Comput. Appl. **206**, 103431 (2022)
124. Zhang, M., Fang, Y.: Security analysis and enhancements of 3g pp authentication and key agreement protocol. IEEE Trans. Wirel. Commun. **4**(2), 734–742 (2005). https://doi.org/10.1109/TWC.2004.84294
125. Asmare, F.M., Ayalew, L.G.: Security challenges in the transition to 4G mobile systems in developing countries. Cogent Eng. **10**(1), 2166214 (2023)
126. Salahdine, F., Han, T., Zhang, N.: Security in 5G and beyond recent advances and future challenges. Secur. Privacy **6**(1), e271 (2023)
127. Gupta, A., Jha, R.K.: A survey of 5G network: architecture and emerging technologies. IEEE Access **3**, 1206–1232 (2015)
128. Li, Q.C., Niu, H., Papathanassiou, A.T., Wu, G.: 5G network capacity: key elements and technologies. IEEE Veh. Technol. Mag. **9**(1), 71–78 (2014)
129. Kumar, G.E.P., Lydia, M., Levron, Y. Security Challenges in 5G and IoT Networks: A Review. In: Velliangiri, S., Gunasekaran, M., Karthikeyan, P. (eds) Secure Communication for 5G and IoT Networks. EAI/Springer Innovations in Communication and Computing. Springer, Cham. 1-13 (2022) https://doi.org/10.1007/978-3-030-79766-9_1
130. Fayed, M.S.: Network generations and the security challenge in IoT applications. arXiv preprint arXiv:2201.01927 (2022)
131. ENISA Report NFV Security in 5G, February 2022
132. Jiang, W., Han, B., Habibi, M.A., Schotten, H.D.: The road towards 6G: a comprehensive survey. IEEE Open J. Commun. Soc. **2**, 334–366 (2021)

133. FG-NET, ITUT: Network 2030: A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond, p. 2019. ITU, Geneva (2019)
134. Chowdhury, M.Z., Shahjalal, M., Ahmed, S., Jang, Y.M.: 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. IEEE Open J. Commun. Soc. **1**, 957–975 (2020)
135. Latva-aho M., Leppänen K., Clazzer F., Munari A. Key drivers and research Challenges for 6G Ubiquitous Wireless Intelligence (White Paper). Technical Report. University of Oulu., (2019)
136. Huang, T., Yang, W., Wu, J., Ma, J., Zhang, X., Zhang, D.: A survey on green 6G network: architecture and technologies. IEEE Access **7**, 175758–175768 (2019)
137. Nakamura, T.: 5G Evolution and 6G. In: 2020 IEEE Symposium on VLSI Technology, pp. 1–5. IEEE (2020)
138. Zong, B., Fan, C., Wang, X., Duan, X., Wang, B., Wang, J.: 6G technologies: key drivers, core requirements, system architectures, and enabling technologies. IEEE Veh. Technol. Mag. **14**(3), 18–27 (2019)
139. Abdel Hakeem, S.A., Hussein, H.H., Kim, H.: Security requirements and challenges of 6G technologies and applications. Sensors **22**(5), 1969 (2022)
140. Aman, M.N., Javaid, U., Sikdar, B.: Security function virtualization for IoT applications in 6G networks. IEEE Commun. Stand. Mag. **5**(3), 90–95 (2021)
141. Hakeem, S.A.A., Hussein, H.H., Kim, H.: Vision and research directions of 6G technologies and applications. J. King Saud Univ. Comput. Inf. Sci. **34**(6), 2419-2442 (2022)
142. Nguyen, D.C., Ding, M., Pathirana, P.N., Seneviratne, A., Li, J., Niyato, D., et al.: 6G Internet of Things: a comprehensive survey. IEEE Internet Things J. (2021)
143. Saleem, K., Alabduljabbar, G.M., Alrowais, N., Al-Muhtadi, J., Imran, M., Rodrigues, J.J.: Bio-inspired network security for 5G-enabled IoT applications. IEEE Access **8**, 229152–229160 (2020)
144. Wazid, M., Das, A.K., Shetty, S., Gope, P., Rodrigues, J.J.: Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. IEEE Access **9**, 4466–4489 (2020)
145. Kumari, A., Gupta, R., Tanwar, S.: Amalgamation of blockchain and IoT for smart cities underlying 6G communication: a comprehensive review. Comput. Commun. **172**, 102–118 (2021)
146. Higgins J, Green S. Cochrane handbook for systematic reviews of interventions. version 5.1. 0. [updated March 2011]. The Cochrane Collaboration, 2011.
147. Weidt, F., Silva, R.: Systematic literature review in computer science-a practical guide. Relatórios Técnicos do DCC/UFJF **1**, 1–7 (2016). https://doi.org/10.1027/1016-9040.11.3.244
148. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., et al.: 6G white paper: research challenges for trust, security and privacy. arXiv preprint arXiv:2004.11665 (2020)
149. Nguyen, V.L., Lin, P.C., Cheng, B.C., Hwang, R.H., Lin, Y.D.: Security and privacy for 6G: a survey on prospective technologies and challenges. IEEE Commun. Surv. Tutor. **23**(4), 2384–2428 (2021)
150. Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., Zhou, W.: Security and privacy in 6G networks: new areas and new challenges. Digit. Commun. Netw. **6**(3), 281–291 (2020)
151. Je, D., Jung, J., Choi, S.: Toward 6G security: technology trends, threats, and solutions. IEEE Commun. Stand. Mag. **5**(3), 64–71 (2021)
152. https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/
153. .ENISA (2017). Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
154. NIST, NISTIR 8259 Series, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series
155. NIST SP 800-213 series, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/sp-800-213-series
156. Executive Order 14028, Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
157. NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/final
158. NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, https://csrc.nist.gov/publications/detail/nistir/8259a/final
159. NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline, https://csrc.nist.gov/publications/detail/nistir/8259b/final
160. OWASP IoT Security Verification Standard, https://owasp.org/www-project-iot-security-verification-standard/
161. ISO/IEC 27400:2022 Cybersecurity—IoT security and privacy—Guidelines https://www.iso.org/standard/44373.html
162. Samonas, S., Coss, D.: The CIA strikes back: redefining confidentiality, integrity and availability in security. J. Inf. Syst. Secur. **10**(3) (2014)
163. Shaik, A., Borgaonkar, R.: New vulnerabilities in 5G networks. In: Black Hat USA Conference (2019)
164. Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V.: A formal analysis of 5G authentication. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383–1396 (2018)