STM JOURNALS

International Journal of
Mobile Computing Technology

ISSN: 3049-0871
Volume 3, Issue 1, 2025
January—June
DOI (Journal): 10.37591/IJMCT

https://journals.stmjournals.com/ijmct

Review IJMCT

A Secured Architecture of Internet of Things (IoT) in the 5G Age

Qutaiba I. Ali[1,*], Mustafa Haitham Mohammed[2], Ali Fathel Rasheed[2]

Abstract

Internet of things (IoT) is a technology capable of connecting vast number of devices of many types worldwide via the internet using unique IP addresses. The connected devices can communicate ubiquitously anywhere, anytime for any given user. Such globally distributed networks require a high level of connectivity among its components like smart sensors, workstations as well as networking devices. Thankfully, with the aid of the recently emerged 5G technology, which offers improved characteristics in terms of capacity, reliability and coverage, the demands that IoT imposes can finally be satisfied. However, preserving the cybersecurity of 5G enabled IoT while taking advantage of its capabilities is not a trivial task. In this study, we review some of the techniques applied for the realization of IoT in 5G networks. Also, we aim at presenting a critical view about some of the recent works regarding the cybersecurity aspect of 5G based IoT. The accessibility and availability features of IoT may also give rise to various threats which may jeopardize the security of the network. This imposes a vital need to provide secure connectivity in terms of confidentiality, integrity and privacy for 5G enabled IoT in order to take full advantage of its potential.

Keywords: IoT, 5G, layered architecture, security, connectivity

INTRODUCTION

Recent years have witnessed the birth and evolution of the concept commonly known as Internet of Things "IoT". Despite its modernity, the term IoT dates back to 1999 when it was firstly invented by Kevin Ashton of Procter & Gamble [1]. Ashton was working in supply chain optimization and he wanted to attract senior management's attention to the RFID technology, which was relatively new back then, so he called his presentation "Internet of Things". However, after more than 20 years and especially in the last decade, the term dominated the world of science and industry, revolutionizing people's daily life on many aspects, from studying to working and not limited to heath and transportation, providing a smart environment that facilitates many life activities [2, 3].

Based on the above, IoT can be considered as an intelligent technology and service where all 'things' including sensors, smartphones, and home applications are connected for conveying information between people and things based on the Internet [4]. Duo to its accelerated pace of evolution, the number of IoT enabled devices are expected to grow exponentially, reaching more than 27 billion devices worldwide and up to 100 billion in 2030 [3, 5]. Duo to their diversity, these devices serve in a variety of applications, ranging from simple smart house solutions to business models and industrial automation and finally mission-critical, lifesaving health care systems. Both of the aforementioned reasons in terms of growth rate and diversity level of IoT devices imposes a rhythm that cannot be met by the wireless equipment currently in use. As a

***Author for Correspondence**
Qutaiba I. Ali
E-mail: Qut1974@gmail.com

[1]Professor, Department of Computer Engineering, Mosul University, Mosul, Iraq
[2]Assistant Lecture, Department of Computer Engineering, Mosul University, Mosul, Iraq

Received Date: January 28, 2025
Accepted Date: January 28, 2025
Published Date: February 14, 2025

Citation: Qutaiba I. Ali. A Secured Architecture of Internet of Things (IoT) in the 5G Age. International Journal of Mobile Computing Technology. 2025; 3(1): 33–43p.

result, the 5G mobile architecture in designed and supported by various new technologies to cope with the ever-increasing demands by the IoT infrastructure [5]. Existing wireless technology such as 3G and 4G cannot meet the demand of 5G wireless requirements, as 5G offers improved features over the 4G-technology in terms of latency bandwidth per unit area, energy efficiency, availability and many more [6]. These improvements can be summarized in Table 1 [3]:

Table 1. Comparison between 5G and 4G networks.

S.N.	Features	5G 2020–25	4G 2010–20
1	Technology	LTE-M New Radio (NR)	LTE, LTE-A
2	Network Latency	Ultra-Low (below 1 ms)	Low (30–70)
3	Network Speed	Ultra-High Speed	High Speed
4	Network Capacity	Ultra-High	High
5	Data rate	10 Gbps	50–100 Mbps
6	Mobility	Ultra-High	High
7	Spectrum Efficiency	Ultra-High	High

Current implementations of 5G include, but are not limited to, network slicing (i.e., assigning logical networks for particular applications), mobile edge computing (MEC), network function virtualization (NFV), and software-defined networking (SDN), which will be explained later. Nevertheless, despite its attractive features, security and privacy remain a major challenge to address in 5G networks. This is duo to the diverse nature of 5G traffic and the dynamic environment that 5G networks enjoy, which demands the security requirement to be more strict than previous generations [7–9]. The security architecture extends the 3G and 4G networks to meet the specific requirements of 5G.

However, this inheritance may cause security issues to rise in terms of user authentication, confidentiality, availability, and privacy, which may trigger various security attacks duo to these flaws in the 5G infrastructure, like eavesdropping, impersonation, tracing and tampering and last but not least, denial-of-service attacks. Also, user fidelity is another concern as users tend to selfishly acquire more benefits from the network than what they actually need. Other reasons may relate to the trustworthiness of some IoT service providers towards user privacy, (interests, habits and activities) from their subscribed IoT services [10]. These reasons might put the 5G based IoT at a disadvantageous situation and hinder any attempts to fully utilize its capabilities in terms of data rate, latency and capacity. To overcome these limitations, the security of 5G networks should provide advanced features with more complicated design: the currently in use three-party trust model comprising a mobile network operator, a service provider, and an end user, is no longer sufficient for 5G as different roles are needed such as Virtualized Infrastructure provider, and VNF provider, etc. while establishing trust relations among these roles explicitly [7].

The purpose of this research work is to present a critical review on a group of recent methodologies suggested by a number of published articles. At first, the infrastructure of the IoT based framework is given, revising security threats that may occur at each layer, then the presented IoT ideas are discussed and analyzed, with strongpoints and shortcomings of each approach. Finally, these ideas are summarized to give a general comprehensive overview for better comparison.

The rest of this work is arranged as follows: the next sections will present previously published researches related to this field; the IoT infrastructure is demonstrated and discussed; a comparative analysis regarding the security of various IoT technologies and finally the conclusion of the study.

RELATED WORK

A variety of research contributions regarding design ideas of 5G based IoT architectures were presented in recent years by many researchers and research groups. Some of these ideas focused on the

structured layers of 5G enabled IoT, like Rahimi *et al.* who suggested an IoT architecture based on multiple modern technologies involving Heterogeneous Networks (HetNet), Wireless Network Function virtualization (WNFV), Wireless Software Defined Networks (WSDN) and Mobile Cloud Computing (MCC) [9]. The authors suggested an 8-interconnnected layers architecture with security layer spans all other layers. The authors claimed that their proposed layer is able to provide the required level of Simplicity, Reliability, Reconfigurability and security.

Another architecture is presented by Obaidat *et al.*, who proposed six-layers security architecture framework for IoT [11]. The model provides a finer level of security for each layer, with improved accommodation and adaptation upon need. It also specifies the security needs and functions demanded for each layer to meet the required security level.

A third paper made by Mrabet *et al*. presented a five-layers contracted and optimized architecture for IoT, using various technologies at each one [12]. Then the authors explain common attacks against IoT devices along with the required countermeasures as shown in Figure 1.

Finally, Burhan *et al.*, presented a survey about various layered architectures of IoT along with the possible threats that may target the security of each layer [13]. The authors exhibit the lack of a single agreed-on standard when it comes to the architecture of IoT. According to this paper, IoT layered architecture can have three, four or five layers, stating that, to some extent, a layer at one model can be thought of as a combination of two layers in another.

A similar work presented by Shin *et al.*, who proposed a 5G based IoT architecture that combines the efforts of Wireless Sensor Network (WSN) with elliptic curve cryptography (ECC) for authentication, authorization, and key agreement purposes [4]. The authors proposed that their suggested model can successfully act as a remedy for the drawbacks of another presented scheme, alleviating many threats while maintaining the required level of security.

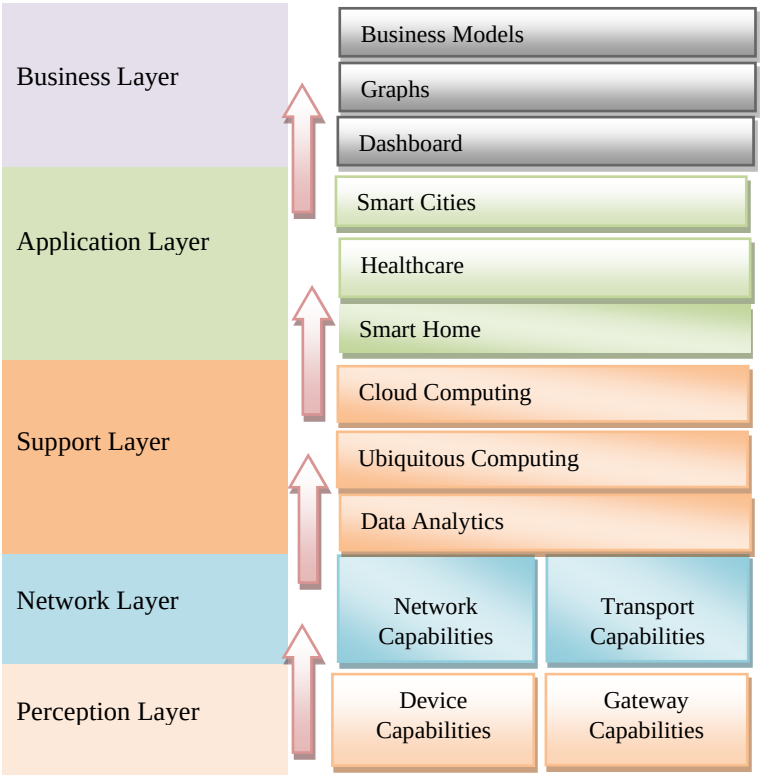

Figure 1. IoT architecture for five-layer.

Apart from layered architecture, some authors have concentrated on the design of security protocols for plugging some of the gaps that may be present in the layered architecture. For e.g., the work presented by Sharma *et al.*, who presented an application layer security protocol to alleviate public access network-based attacks. The security protocol was tested by a software tool called Skyther. The authors claimed that their suggested protocol exhibits liveness, non-injective agreement and non-inactive synchronization, which makes it impervious against confidentiality, integrity and availability based attacks.

Another paper presented by Kumar *et al.* designed a protocol for node-to-node data transfer authentication service [3]. The authors claimed that the designed protocol is immune to the cyber-attacks targeting confidentiality, integrity and availability.

As stated before, IoT services cover wide aspects of our daily life, one instance is related to the field of transportation. Here, Vehicular IoT is considered as one promising application where vehicular ad-hoc networks (VANETs) can take advantage of the 5G technology features such as high data rate, high reliability and low latency. In this regard, Xie *et al.* proposed a paper examining the security and privacy concerns related to the transportation system and the vehicular IoT environment in SDN-enabled 5G-VANET model [14].

Designing a blockchain-based security framework for enhancing the vehicular IoT services; here, vehicular messages were managed and verified based on real-time cloud-based video reporting system. The authors, Wijethilaka and Liyanage, claimed achieving secure and trustworthy vehicular IoT environment while preserving user privacy [15].

Another IoT trend that is thoroughly inspected is network slicing, which refers to the demonstration of the physical network as independent logical subsystems called slices, in which each slice has its own distinctive, application-oriented features and capabilities. In this context, Ni *et al.* exploited the concept of network slicing for building an authentication structure that is both secure and efficient for 5G-enabled IoT services [10]. Request for service can be conducted with the 5G core network anonymously and gain access to the IoT service using the proper network slice, depending on the type of service required. This, according to the authors, make the paradigm both efficient and practical, and preserve security and privacy of end users.

Another network slicing related work is presented by Wijethilaka & Liyanage [15], who presented an inclusive study about the utilization of network slicing in IoT implementations. The authors presented a number of application cases where network slicing can be exploited along with the technical difficulties it can solve. The paper also points out other promising technologies such as Artificial Intelligence and blockchain and their integration with network slicing and IoT for smarter and more secure 5G enabled applications.

CYBERSECURITY-ORIENTED IOT ARCHITECTURE

A range of designs are projected for IoT by researchers. IoT architecture follows a similar thought of OSI seven-layer architecture, i.e., a layer below services the layer above. Perception layer is employed to service the network layer and therefore the network layer is used to service the appliance layer, as shown in Figure 2. Because of the nonuniformity of the devices utilized in IoT and the number of IoT applications, it is not doable to use one single architecture for IoT. Also, IoT is growing exponentially and it is not possible to use one design. IoT started with a basic three-layer architecture, as shown in Figure 2 [13, 16–20].

The three-layer design is not ready to meet the demand of burgeoning IoT and thus the four-layer architecture was supported by International Telecommunication Union (ITU) and projected by Darwish [18]. within the four-layer architecture, a further layer referred to as service support and therefore the application support layer is introduced between network and application layers as shown in Figure 3.

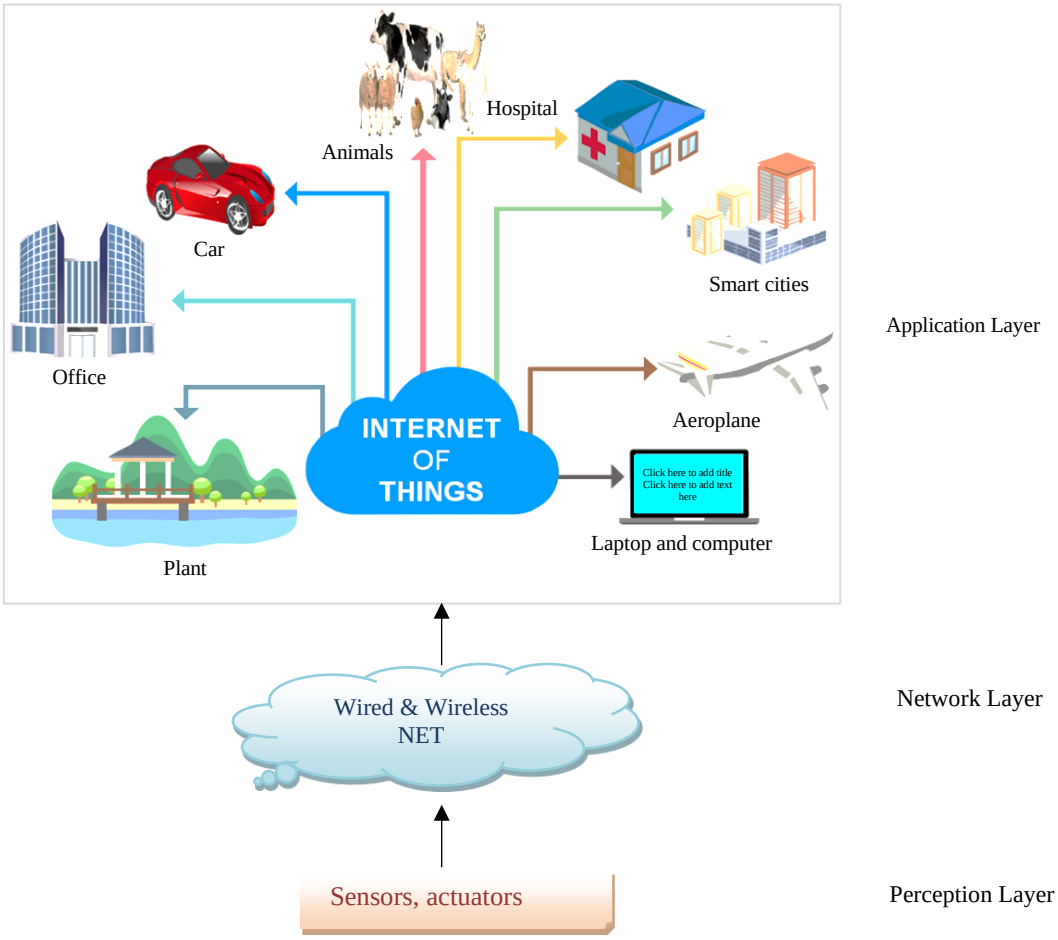

Figure 2. IoT Architecture for three layer.

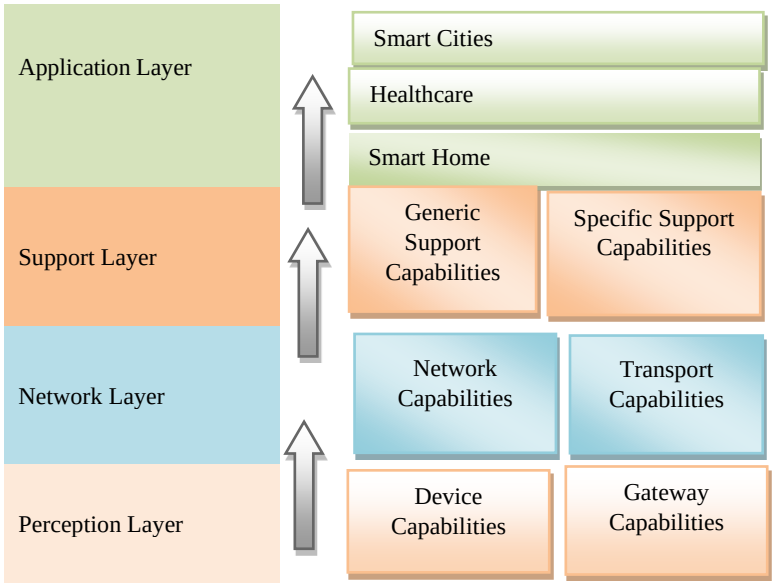

Figure 3. IoT Architecture for four-layers.

Perception Layer

The perception layer called the sensor layer that sensors, actuators, and area gadgets interact with and acquire facts from the environment. Sensors are speaking with the community and with software, this

is going to control that item as a networking item. It is just like the physical layer in the OSI seven-layer architecture. The main functions of perception layer are:

- Perception and identity of objects.
- Catching information.

Common threats in this layer are:

- *Eavesdropping:* This is a real-time attack in which private communications are illegally intercepted, such as important phone calls, text messages, fax transmissions, or video meetings that are intercepted by an attacker. It tries to steal the information or data available when it enters through that network. Wherever it is obtained sends it over the network.
- *Node Capture:* It is one of the risky assaults confronted inside this layer of IoT. When a key node is fully controlled by the attacker, it additionally leaks communication of all information among sender and receiver, the key used to make secure-communication, and data saved in the memory.
- *False and malicious node:* An attack where the attacker provides a node to the device and inserts dummy data into the layer. Its objectives are to prevent the transmission of active information. A node delivered by an attacker after control consumes the full power of the physical nodes and may destroy that network [13].

Network Layer

It is commonly known as transmission layer. It acts as a bridge or routing between the two layers, including the perception layer and the applications layer. It is also responsible for transmitting real information from physical objects like sensors, where they are fetched from a lower level of the layer through wireless transmission and reception. Therefore, they are more vulnerable to attack by attackers, so they are more sensitive. It may have a prominent role in several issues in terms of the credibility and safety of information transfer between layers in that network. Some of the problems and threats facing these layers are:

- *Denial of Service (DoS) attack:* A DoS attack is an attack which is the responsibility falling on the original users to prevent them from accessing devices or networks. This is usually accomplished by masking the devices under their control that have excessive demands in order to make them unavailable on network resources, or impossibly linking to some users, or trusting users to use that network or devices.
- *Main-in-The-Middle (MiTM) attack:* A MiTM attack is where the attack is carried out secretly. The attacker uses a tactical method that changes the communication or session between the sender and the receiver so that he receives the information from one of them and then changes the content of the message according to his needs and then resends the message without the connected with each other. So, this type of threat poses a risk to their possession of information over the Internet because it gives the attacker the ability to capture information and alter content in real time.
- *Storage attack:* where the attack is on the cloud or available storage devices that store users' information in it; when the attacker takes control of that cloud or storage devices, by changing the data or putting wrong information or a database is available, which creates an opportunity to repeat information related to people in that cloud, potentially leading to an increased number of attackers.
- *Exploitation attack:* This sort of attack is unlawful and immoral. This type of attack uses a program, a part of the available data, or a pattern series of commands in that attack, wherever it finds loopholes or security flaws in those devices or systems available for the purpose of controlling a system, and then content theft of information available in devices via that network.

Support Layer

This layer is additionally known as either middleware layer or process layer. This layer is accountable to handle the knowledge received from the transport layer. Here, the tangential information is removed, and therefore the relevant information and holds on to victimization technologies like cloud computing,

omnipresent computing, and data analytics. This layer stores, analyses, and processes the info received from the network layer. The main purpose of this layer is to change the decision-making process by triggering commands back to the physical devices within the perception layer so as to perform actions to influence the general condition of the environment where the devices are deployed. These are some common threats in this layer:

- *DoS attack:* A DoS attack at the support layer is associated with the network layer. The attacker sends a huge amount of data that the network cannot absorb, causing network traffic to stop. Thus, the consumption of those resources greatly depletes the system followed by the Internet of Things, making it difficult to access the system by the use.
- *Exhaustion:* An attacker uses fatigue in an unobtrusive manner to disrupt the processing of the IoT infrastructure. This happens as an after-effect of receiving attacks, such as a DoS attack where the victim receives many requests by the attacker sending over the network and renders them unavailable to the users. Which causes the exhaustion of these resources due to the attacks, such as battery resources and memory loss. The Internet of Things has a special system in distributed so it is free of risks. It is the simplicity of the protection procedure to prevent this attack.
- *Malware:* where an attack is made on users and the confidentiality of information saved in that network is taken. It is then used for some programs such as application viruses, spyware, adware, Trojans, and worms available to that system. It takes the form of icons, an executable smart tool, simple scripts, and content. It works against the requirements available in the system to steal confidential information from users [13].

Application Layer

This layer is known as the management layer. It is used by some applications related to the Internet of Things over the network to extend the scope of service and publish applications, and thus has an effective role in carrying out the following functions: QoS manager; Device manager; Business process modeling; Business process execution; Delegation; Key exchange and management; Trust and reputation; and Identity management. In this layer, you will have to consider that all actions are made to control the application in terms of security and management layer [19]. Common threats and problems infecting the application layer are:

- *Cross-site scripting:* It is an injection attack. Through the injection, the tasks are done by inserting a script from the client interface without paying attention to it, and one of the simplest ways is to use some programs for JavaScript in a web page that users view as available content. By doing so, the attacker can extrude and manipulate the contents of the program in accordance with his wishes and illegally use the original information or content.
- *Flexibility in dealing with big data:* With a large set of data stored in devices and a huge amount of knowledge transfer between users, processing cannot be handled according to requirements. As a result, it ends up in network disruption and data loss [13].

Business Layer

This layer is also called the ‘Services layer’ that is used in controlling and managing applications, business models for IoT systems, for instance, flow charts, graph models, dashboards and things that serve the business etc. Work is done in this layer after receiving data from the application layer which is further processed according to strategic management and future actions of the IoT platform. Therefore, this layer is responsible for protecting user privacy

All these three-layer, four-layer, and five-layer designs are largely employed by researchers and academicians; however in real applications, it is inconceivable to use one common architecture because of diversity of IoT applications and therefore the completely different communication technologies involved in it. In fact, these layers are called IoT architecture under different names and where some additional layers have been added in some other applications [20].

SECURITY OF IOT BASED TECHNOLOGIES AND IMPLEMENTATIONS

Over the past few years, the concept of IoT has been evolving to withstand some of the newly invented technologies being applied for the realization of its applications. These technologies are not initially intended to function in the IoT environment, but they can advocate for the its evolution to produce the next generation of IoT applications. Current IoT implementations are not free from any of these methods, which can be included in its underlying architecture. Some of these technologies are briefly explained below [21–24]:

Heterogeneous Networks (Het-Net)

Heterogenicity is one of the fundamental aspects of IoT based environment duo to the diversity of the nature of the connected devices, which require flexibility in the network connecting them. Unlike traditional homogeneous networks, this would allow the network to provide on-demand response to a variety of requests and process different types of information. Regarding its security, Het Nets may suffer from multiple attacks such as misrouting, snooping or packet dropping, which may deteriorate the performance of the network in terms of packet delivery.

Millimeter Wave (mmWave)

The current speed and capacity of IoT has outdated the traditional frequency spectrum below 6 GHz duo to its inability the cope with the flexibility and data rate requirement of the network. This requires employing higher frequencies to meet these demands. Millimeter Wave (mmWave) communication brings a favorable higher frequency up to 80 GHz to support faster 5G-IoT operations. Nevertheless, it may suffer from eavesdropping and other reconnaissance related attacks.

Wireless Software-Defined Networks (WSDN)

WSDN is a relatively new technology that facilitates the process of network management and configuration, resulting in improved flexibility and troubleshooting. WSDN provides a centralized network control which gives more adaptability to real-time modifications while maintaining the required performance. However, its centralized structure makes it vulnerable to Distributed DoS (DDoS) and man-in-middle attacks.

Mobile Edge Computing (MEC)

Edge (fog) computing is suggested to demonstrate the realization of services located at the system boundaries. It is an intermediate layer serving as an interface between IoT devices and sensors and the distributed database. MEC is mainly about distributing data, tasks, storage and applications efficiently among distributed sources on the network. Still, the flexibility offered by fog computing can be a source of authentication and trust issues. Moreover, privacy can also present a problem as the number of connected networks increases.

Wireless Network Function Virtualization (WNFV)

WNFV is a technique used to create a virtualization of network services and isolate them from the underlying physical infrastructure for facilitating the evolution of 5G based IoT framework. The previously mentioned concept of network slicing can be used in conjunction with WNFV to create specialized, cloud-based networks for 5G enabled IoT applications. Despite its benefits, WNFV can be subjected to multiple attacks, including insider and outsider attack, DNS amplification attack, and Denial of Service Protection Failure.

Big Data Analysis

The interest in the analysis of big data had increased recently as companies aim at extracting useful and valuable information from datasets acquired from the internet. Data analysis plays a key role to a prospering IoT application, such as smart factories which may contain large number of sensors continuously producing data items. The resulting accumulated data cannot be treated by conventional software tools and algorithms. The analysis of big data collected socially can give an accurate look

about the general trend of the population in order to build a good understanding to their needs. Attacks on big data can take various forms, like Malwares, Injection Attacks, DoS, Web Botnets, Phishing and Social Engineering. This is due to difficulty in dodging attacking attempts in the presence of huge amounts of data. Table 2 is derived depending on the information given for each of the technologies mentioned above:

Three IoT layered architecture frameworks were presented in this study by Mrabet *et al.* [12], Obaidat *et al.* [11], and Rahimi *et al.* [9], comprising of five, six, and eight layers, respectively. First of all, it is noticed that the suggested number of layers varies from the ones previously stated. This implies that choosing an optimum number of layers for a given security architecture is still a controversial topic. Secondly, it is observed that some of the layers are present in all the three presented models, like the physical, network, and applications layer. This refers to the essential operations that are required by any IoT application. Finally, and most importantly, the security aspect of architecture is treated differently by the researchers, while the model presented by Rahimi *et al.* [9] places the security as an independent layer, overlooking the rest of the model, security in manifested implicitly in each layer of the model suggested by Obaidat *et al.* [11] and Mrabet *et al.* [12]. The later one specifically focuses on both security threats and their solutions per layer for maximum illustration. The three presented architectural models in these references can be collectively summarized as in the Figure 4:

Table 2. Cyberattacks types that are more likely to be encountered based on different IoT technologies.

Attack\Name	DDoS	Man in the Middle	Malwares	Eaves-dropping	Snooping, misrouting	DNS attack	other
Het Net					✓		
mmWave				✓			✓
WSDN	✓	✓					
MEC		✓					✓
WNFV	✓					✓	
Big data			✓				✓

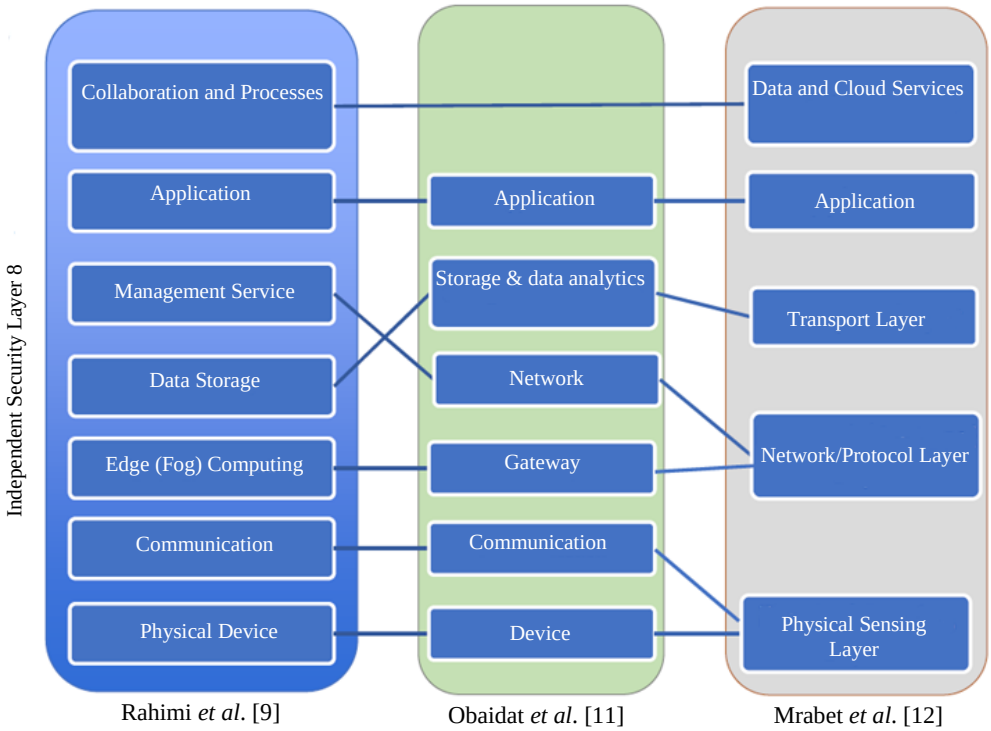

Figure 4. Comparison summary among the three reviewed secure architectures.

CONCLUSION

In this study, an overview about the concept of Internet of Things (IoT) is presented, along with its secure layered architecture, and the possible security threats for each layer, applications and the latest trends regarding its integration with the ever-growing 5G technology. Also, some of the most notable technologies that can be exploited to enhance IoT application are briefly described, including the Het Net, mmWave, WSDN, MEC, WNFV, and big data, along with the security threats these technologies may be vulnerable to. Finally, the presented data were tabularly summarized to give an overall glimpse about the knowledge given throughout the study.

Maintaining the security of the aforementioned technologies proves to be a challenge, especially with the incorporation of the 5G technology into the IoT environment. The openness and versatility of the 5G architecture make it a fertile ground for attacking attempts. In this context, security is a process, and not a one-time job; having the right architecture or security equipment will never be enough. This involves developing workflows, establishing procedures, and fostering collaboration among teams tasked with ensuring the company's security and protection.

REFERENCES

1. Santos B, Feng B, van Do T. Towards a standardized identity federation for internet of things in 5g networks. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). 2018 Oct 8; 2082–2088.
2. Lu Y, Da Xu L. Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet Things J. 2018 Sep 12; 6(2): 2103–15.
3. Kumar KP, Padma TN, Goud BP. Efficient Secure Authentication Protocol for 5G Enabled Internet of Things Network. Technology. 2020; 2020(25): 4G.
4. Shin S, Kwon T. A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. IEEE Access. 2020 Apr 6; 8: 67555–71.
5. Wijethilaka S, Liyanage M. Survey on network slicing for Internet of Things realization in 5G networks. IEEE Commun Surv Tutor. 2021 Mar 22; 23(2): 957–94.
6. Sharma S, Satapathy S, Singh S, Sahu AK, Obaidat MS, Saxena S, Puthal D. Secure authentication protocol for 5G enabled IoT network. In 2018 IEEE 5th International Conference on Parallel, Distributed and Grid Computing (PDGC). 2018 Dec 20; 621–626.
7. Arfaoui G, Bisson P, Blom R, Borgaonkar R, Englund H, Félix E, Klaedtke F, Nakarmi PK, Näslund M, O'Hanlon P, Papay J. A security architecture for 5G networks. IEEE Access. 2018 Apr 17; 6: 22466–79.
8. Chettri L, Bera R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet Things Journal. 2019 Oct 22; 7(1): 16–32.
9. Rahimi H, Zibaeenejad A, Safavi AA. A novel IoT architecture based on 5G-IoT and next generation technologies. In 2018 IEEE 9th annual information technology, electronics and mobile communication conference (IEMCON). 2018 Nov 1; 81–88.
10. Ni J, Lin X, Shen XS. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE J Sel Areas Commun. 2018 Mar 12; 36(3): 644–57.
11. Obaidat M, Khodiaeva M, Obeidat S, Salane D, Holst J. Security architecture framework for Internet of Things (IoT). In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2019 Oct 10; 0154–0157.
12. Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors. 2020 Jun 28; 20(13): 3625.
13. Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors. 2018 Aug 24; 18(9): 2796.

14. Xie L, Ding Y, Yang H, Wang X. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access. 2019 Apr 29; 7: 56656–66.
15. Wijethilaka S, Liyanage M. Survey on network slicing for Internet of Things realization in 5G networks. IEEE Commun Surv Tutor. 2021 Mar 22; 23(2): 957–94.
16. Yun M, Yuxin B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In 2010 IEEE international conference on advances in energy engineering. 2010 Jun 19; 69–72.
17. Ngu AH, Gutierrez M, Metsis V, Nepal S, Sheng QZ. IoT middleware: A survey on issues and enabling technologies. IEEE Internet Things J. 2016 Oct 4; 4(1): 1–20.
18. Darwish D. Improved layered architecture for Internet of Things. Int J Comput Acad Res. 2015 Aug; 4(4): 214–23.
19. Sethi P, Sarangi SR. Internet of things: architectures, protocols, and applications. J Electr Comput Eng. 2017; 2017(1): 9324035.
20. Kumar PR, Wan AT, Suhaili WS. Exploring data security and privacy issues in internet of things based on five-layer architecture. Int J Commun Netw Inf Secur. 2020 Apr 1; 12(1): 108–21.
21. Wang C, Wang HM. Physical layer security in millimeter wave cellular networks. IEEE Trans Wirel Commun. 2016 May 3; 15(8): 5569–85.
22. Lal S, Taleb T, Dutta A. NFV: Security threats and best practices. IEEE Commun Mag. 2017 May 15; 55(8): 211–7.
23. Aljuhani A, Alharbi T. Virtualized network functions security attacks and vulnerabilities. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). 2017 Jan 9; 1–4.
24. Suraj MV, Singh NK, Tomar DS. Big data Analytics of cyber attacks: a review. In 2018 IEEE international conference on system, computation, automation and networking (ICSCA). 2018 Jul 6; 1–7.

