A Review on the Security of the Internet of Things: Challenges and Solutions

Article *in* Wireless Personal Communications · August 2021

DOI: 10.1007/s11277-021-08348-9

Wireless Personal Communications
https://doi.org/10.1007/s11277-021-08348-9

A Review on the Security of the Internet of Things: Challenges and Solutions

Oludare Isaac Abiodun[1,2] · Esther Omolara Abiodun[1] · Moatsum Alawida[1] · Rami S. Alkhawaldeh[3] · Humaira Arshad[4]

Accepted: 19 February 2021

Abstract
The Internet of Things (IoT) has emerged as a modern wave of Internet technologies that promises great transformation of life in areas such as smart health, smart cities, smart homes, intelligent transport, amongst others. However, security often serves as a critical reason for the widespread adoption of any innovation. While the IoT has increased business productivity and enriched diverse areas of life over the years, the world is yet to see a methodical revolution of its humongous application and transformation given its ubiquity and highly interconnected global network structure. The main culprit for such lapses is principally attributed to security and privacy issues which have been widely discussed in research articles and reviews but remain largely unaddressed in the literature. Hence, this paper provides a state-of-the-art review of IoT security and its challenges. It overviews technical and legal solutions that are useful to private, organizational, and governmental enterprises. The study encompasses the review and security analysis of IoT's evolution and revolution, IoT security assessments, requirements, current research challenges in security and much more. Consequently, it offers potential solutions to address the security challenges discussed and further present open research issues, research gaps, opportunities, future development, and recommendations. This overview is intended to serve as a knowledgebase that will proffer novel foresight to guide users and administrators in positioning themselves and their organizations in a manner that is consistent with their overall objectives, mission, and vision for remarkable outcomes. Likewise, interested scholars and researchers can explore topics and directions from the study in providing better solutions to the numerous problems in IoT security.

Keywords Internet of things (IoT) · Security and privacy challenges in the internet of things · Solutions to IoT security and privacy challenges · IoT research gaps · Future development in the IoT

✉ Esther Omolara Abiodun
styleest2011@gmail.com

[1] School of Computer Science, University Sains Malaysia, George Town, Penang, Malaysia

[2] Department of Computer Science, Bingham University, New Karu, Nasarawa State, Nigeria

[3] Department of Computer Information Systems, The University of Jordan, Aqaba 77110, Jordan

[4] The Islamia University of Bahawalpur, Bahawalpur, Pakistan

Published online: 06 March 2021

1 Introduction

The human race is on an expedition to digitize the world and an ever-evolving dataSphere is the ensuing after-effect. The global world is witnessing a *sensorized* magnitude of intelligence which apparently the Internet of Things (IoT) is a major and integral contributor. An IoT object or device refers to a uniquely identifiable "thing" or endpoint that can autonomously connect bi-directionally utilizing connectivity to exchange data via the web. In their course of connection, they generate data that enables observation, management, investigation and analysis to be performed on the state of the objects or the surrounding environment.

According to a recent prediction from a world-known premier global provider of market intelligence called the International Data Corporation (IDC), the year 2025 will bring about 41.6 billion connected IoT devices/things (a composite of sensors, machines, cameras, etc.) which will be generating 79.4 zettabytes of data. Their prediction was borne from an accumulated analysis over the years 2018–2025 where they ventured that the IoT devices would see a compound annual growth rate (CAGR) of 28.7% over the forecasted period [1].

The number of connected IoT devices progressively ascends in tandem with the amount of data generated. Thus, data becomes the shared factor enabling the exchange of information from people, things, and processes to create value for enterprises, governments, and people across diverse spheres of life ranging from industrial, automotive, household, medical, amongst others. It is critical for organizations to understand the volume of data generated from the multitude of associated devices to enable the development of solutions that can scale in the data-driven market of IoT. Nevertheless, such obligation comes with diverse security vulnerabilities and privacy concerns which must be addressed before any massive adoption can be experienced. For instance, the development of drones which helps to access remote areas which are difficult to view/cover by traditional cameras, deployment of 4G and 5G networks which offers higher bandwidth with low latency and dense coverage all show the potential the IoT offers. The adoption of such high-tech devices remains low due to security, private and public safety concerns.

Securing the Internet of Things (IoT) is a matter of public opinion that involves all stakeholders, including, the service providers, manufacturers of devices, organizations, vendors, and clients. As discussed above, even with the current phase four industrial revolution, referred to as Industry 4.0, the IoT is yet to function well due to security challenges. Without the intervention of the government at various levels, the IoT will stand to be dangerously insecure.

Recently, the United States of American's (USA) Senators introduced a bill designed to improve IoT security. The IoT cybersecurity improvement act of 2017 is a modest piece of legislation [2]. The bill was meant to leverage the government's buying power to nudge the market; that is, any IoT product the government purchases must satisfy minimum security standards. It requires vendors to ensure that devices can not only be patched but rather patched in an authenticated and timely manner, and not having unchangeable default passwords, and must be free from vulnerabilities. This singular move by USA senators would considerably improve security and at the same time, it speaks volumes about the current state of IoT security challenges.

Several incidences in the past have made the IoT devices challenging to trust [3, 4]. Smart televisions, phones, computers, and cash machines have been hacked [5], which have negatively affected consumers' trust and questions the capability of the effective delivery

of confidential service of business enterprises. Other challenges impeding IoT's wide adoption, such as device identification, addressing, interoperability, mobility, massive scaling, management, energy efficiency, etc., remains widely discussed but not fully addressed [6].

In the research community, there have also been articles and reviews which serve as efforts to tackle some of the various challenges of IoT from various angles, including security and privacy. Some of the works closely related and have touched the security perspectives of IoT include a survey work by Alaba et al. [7], where they taxonomically characterized security threats and vulnerabilities with regards to application, architectural design and communication. They delineated the contrasts between conventional devices and the sensor-based IoT devices and how the same kind of security measures cannot work for both genres of devices. Hence, they proposed their taxonomy which is different from the traditional layered architecture.

Khan and Salah [8] overviewed IoT security with respect to its application in blockchains. Their widely cited research categorized security issues into a high, intermediate and low-level IoT layers by utilizing parametric analysis of security vulnerabilities and mapping them as a potential response to IoT security challenges. They further examined the essential attributes of the blockchain-based security solutions and analysis of their viability for securing IoT. Likewise, Granjal et al. [9] investigates security protocols and mechanisms for the secure operationality of IoT. Other studies explore the security of IoT in the context of intrusion detection system [10, 11], cryptographic primitives [12, 13], fog computing [14–16], security issues emanating from the nature of the service delivery models of an IoT system [17–19] amongst many others [20–24]. Unlike other works, this review work is not tailored to a specific protocol. It overviews all the boundaries in IoT in the context of security. Additionally, it is different from other review works in literature as it gives the following contributions:

1.1 Contributions

1.1.1 An Up-to-Date Overview

This review will assemble, analyze and synthesize abundant resources of current works as regards to the security of IoT with the sole purpose of bringing together what exactly is the state-of-the-art in IoT security. Generally, it is developed on top of existing works to highlight the research efforts of other works while converging the state-of-the-art in terms of what is attainable today in IoT and its security. Ultimately, it is an extended effort to inform government, business enterprises, and private personnel on the state of IoT security especially the urgent need to navigate and manage new security concerns and vulnerabilities resulting from the effective adoption of the IoT infrastructure.

1.1.2 Look-Up Manual

Experts, practitioners, researchers and analysts in the domain seek clarity in understanding the effect of security and privacy on adopting the Internet of Things. Moreover, it will serve as a useful guideline or referential manual for prospective researchers joining the field to quickly understand some critical concept and grasp the keywords in IoT. The knowledge will save time and increase efficiency by guiding the potential researchers or enterprise to align their business with fail-proof architectures to improve the performance of their business.

1.1.3 Future Perspectives and Directions

Elaborate discussions on current trends, constraints in the security of IoT, potential solutions and prospective future research explorations and directions are given. Exploring such factors highlights the contributions and limitations of the reviewed papers with the intention of delineating novel concepts in IoT security and the underpinnings of future research. In summary, this paper presents the state of the art of different levels of IoT's security by analyzing various existing research proposals and pointing out some problems and open research issues.

2 Review Methodology

This review work overviews and report the current state of the security of IoT research. It investigates and examines contemporary literature on current trends, security design, revolution, security analysis, security requirements, assessments and much more.

A comprehensive study of related works in literature were reviewed to achieve the objectives stated above. The reviewed literatures were extracted from the abundant resources in well-established and reputable databases containing journal articles, reviews, conference papers and proceedings, books, edited volumes, thesis, symposiums, preprints, gray literature and magazines amongst others.

The relevant works in the literature were identified by querying related search terms such as, "Internet of Things", "IoT", "Security and privacy challenges in the Internet of Things", "Solutions to IoT security and privacy challenge". The returned results were downloaded, read and relevant papers were collated for the final analysis. The scholarly databases queried for the literature are as follows:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- Scopus
- ResearchGate
- Springer
- EBSCO Host
- Taylor and Francis
- Google Scholar

Overall, 104 papers were used for the review.

3 Overview of IoTs and Its Security

IoT refers to billions of physical devices that are connected to the Internet to collect and share data. The IoT digital revolution materialized in this current era of the world's phase four industrial development. A computer and innovative digital expert, named Kevin Ashton, was popularly said to be the first person that used the term IoT. The digital

revolution of the IoTs can be traced back to the first, second, and third phases of industrial development and now that the world is in her fourth phase called Industry 4.0. The Industry 4.0 framework on digital technologies can be represented in Fig. 1.

Figure 1 represents the Industry 4.0 framework features on digital technologies. One can easily understand that it involves the connection of heterogeneous systems for information gathering and sharing, especially in the business entity.

3.1 Security Design in IoT Device

Although the IoT is reshaping lives, it concurrently raises issues due to their low security level, which is vulnerable to attackers for malicious intent [25]. In addressing the burning issue of IOT security, one of IoT start-up companies of industry 4.0, Winix Technologies has developed and implemented an IoT platform that can be used for diverse purposes. An example of the platform's use case is Wireless Tracking System (WTS) called Wi-MAP. The Wi MAP is an Indoor Location Intelligence Platform (ILIP) that combines the best of Bluetooth, Wi-Fi, and low energy sensors to function.

Besides, it can be used to gather movement of people in a geographical location, then provide them with turn-by-turn indoor guidance on either a map or floor plan, and trigger actions when a device is close to or leaves a targeted point. Moreover, Wi-MAP has features that users can use to track people's movements, assets, and more in real-time

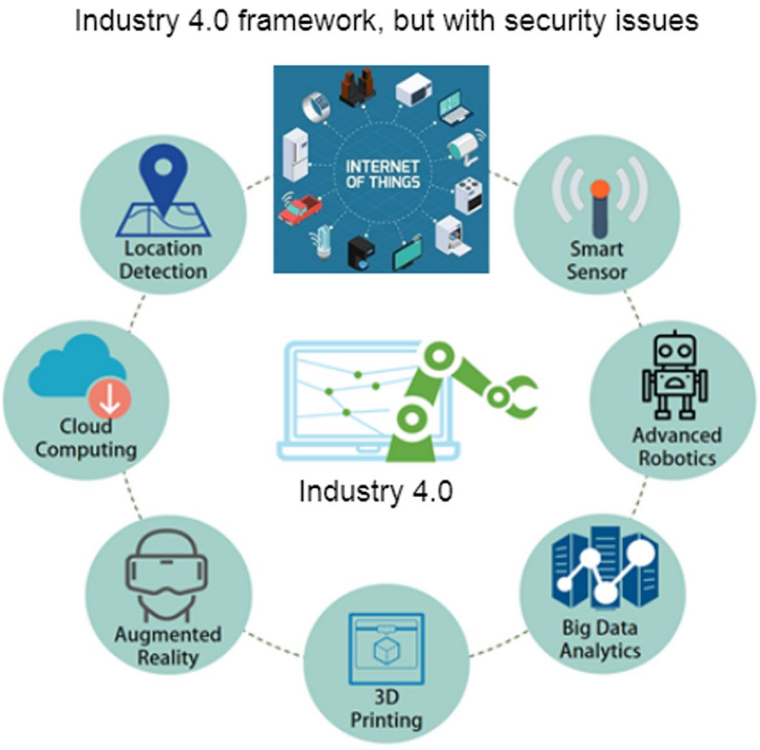

Fig. 1 Industry 4.0 framework- digital technologies

scenarios. The remarkable part of it is that all these features were developed while taking cognisant of people's privacy.

Furthermore, Wi-MAP is built as a part of the retail infrastructure to accurately define the point of service (POS) by knowing a customer's movement in real-time. In the schools, Wi-MAP is used to establish better security, such as assisting teachers in knowing their pupil location. It also helps parents know their children's location and ward or in real-time, from inside the school bus to their classrooms. Wi-MAP could target public spaces such as shopping malls, shops, exhibition halls, museums, hospitals, etc.

3.2 IoTs Revolution

The revolution of IoT can be viewed as a gradual growth in technology that is related to time. Standalone machines were the beginning of the computing world; the next was the era of networking to enable resources and information sharing. Consequently, the interconnection of computing objects leads to the emergence of the most innovative and useful network called the Internet. The Internet consists of various intranets, personal computing devices, and organizations' computing devices. Progressively, the Internet now has wireless connectivity. The advent of wireless connectivity and miniaturization of computing devices bring the world to mobile computing. With all these advancements in technologies and the availability of many devices together with electronic equipment such as sensors and actuators, the new phase of technology is a situation where every device is assumed to intelligently sense with some computing abilities, that become the era of IoT.

The IoT has three major components:

1. The "things" (i.e. technologies, devices, objects, animals, or humans).
2. The networks of communication that connect the device.
3. The computer networks through data streaming from the Internet to device.

The IoT is the network of physical objects and other items that are embedded with electronics, sensors, software, and network connection, which permit these objects to collect and change data. The main strength of the IoT evolution is the high effect it has on distinct areas of daily-life and users' behaviour. For example, home security systems could let one remotely monitor the thermostats or locks on doors in the house. IoT as a network of many networks is represented in Fig. 2.

It is clear from Fig. 2 that the IoT is not a single technology, and rather it is an idea in which many objects are either connected or interconnected and activated. For example, objects with embedded sensors, streetlights that are networked together, image or object recognition abilities, near field communication with protocol, augmented reality, services, and new resources management, etc. The main idea of the IoT is to help obtain better information about the close or remote environment so that one can understand, control, and respond to the collected information to support human existence.

These integrations of objects have brought many business opportunities. Nevertheless, its complexity of management in the field of telecommunication and information technology, especially security and privacy issues require to be addressed for effective advancement and success in technology.

Though IoT is an evolving paradigm with significant momentum, however, the evolving technology continues to be plagued with security and privacy problems. Security and privacy concerns require urgent and timely solutions as the world continues to increase in

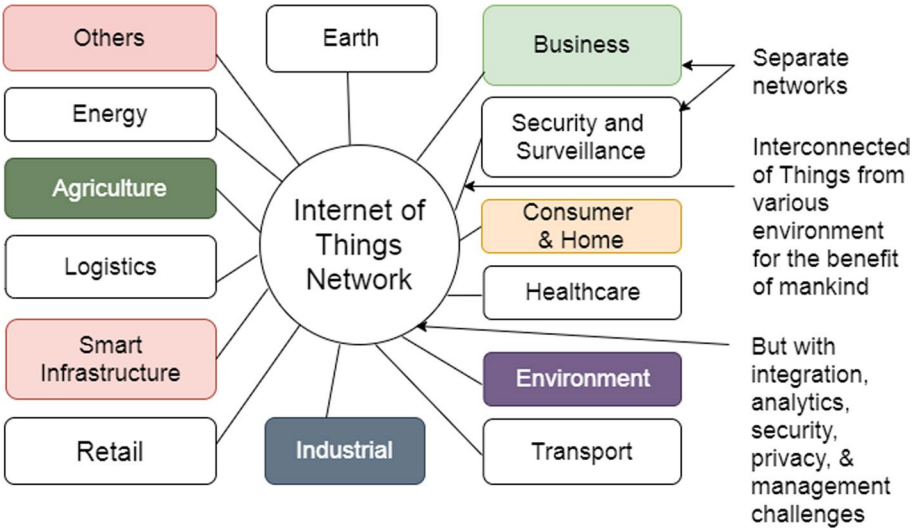

Fig. 2 IoT as a network of many networks to benefit humanity

tandem with IoT connected device. Based on the enumerated figures and facts, the ratio between the number of connected devices and the population figure could be estimated. This estimation and generated ratios are presented in Table 1.

Concerning Table 1, in 2003, the world population was computed to be 6.3 billion, while connected IoT devices were about half a billion (0.5 billion). Also, in the year 2010, the connected devices were 12.5 billion and the world population was 6.8 billion. More also, in 2015, the population became 7.2 billion. Meanwhile, the number of connected devices grew to a whopping 25 billion. With the current trend of the IoT, by the end of the year 2020, the population figure will attain 7.6 billion, and the connected devices will grow to about 50 billion [1, 26–29].

3.3 Possibilities, Opportunities and Security Analysis of IoTs

IoT, as a system of interrelated intelligent devices, digital and mechanical machines, objects, people, or animals is assigned unique identifiers (UIDs). The interconnection possesses the capability to send data over a network without requiring human-to-human or human-to-computer interaction. The high-level connectivity of intelligent computational devices and their severe constraints in the IoT brings about different security challenges that do not streamline with the classical design of wireless networks. For

Table 1 Ratio of the World population with IoT connected devices from year 2003 to 2020

Years	World Population (in billion)	IoT Connected devices (in billion)	Ratio
2003	6.3	0.5	0.08
2010	6.8	12.5	1.84
2015	7.2	25	3.47
2020	7.6	50	6.58

instance, in terms of technology and deployment, how IoT security and privacy issues work differs from how it works with conventional and wireless networks. The layout of IoT networks is based on low-power and lossy networks which are constrained by energy, processing power and memory. Consequently, lightweight encryption schemes are leveraged for ensuring the security of the IoT environment. Even though they have been discussed extensively in the literature, such aspects of IoT have remained largely unsolved [7, 30, 31].

Recently, an organized body, the defence advanced research projects agency (DARPA) has identified a "security shield" for IoT as a project with a potential effect wider than the Internet itself. According to Banafa [32] and Sicari et al. [12], security is one of IoT's challenges. Most of the security challenges associated with IoT are complexity in establishing safe, private, and secure communications. The IoT complexity is caused by different components that converge at the network node, which hampers smooth safety and secure communication.

Additionally, there are some data confidentiality and secrecy issues related to IoT. For example, the system operation involves the interconnection of networks, a problematic situation whereby most users cannot control individual networks—enabling data leaks and other confidentiality and secrecy vulnerabilities. Moreover, IoT comprises of many devices and heterogeneous network systems [33–35]. This heterogeneity of interconnected objects makes it challenging to access, identify, and monitor sensitive components to ensure compliance even with security laws and policies [6, 36]. Furthermore, it is challenging to provide a complete level of secure communication of information, privacy, and trust among various vertical and horizontal computer infrastructures of IoT [37–39].

Indeed, IoT affects people, data, processes, and things. It affects people because more objects are connected in terms of the machine to man, which can be controlled, monitored, and subsequently aid the individual's capabilities. Also, the IoT affects processes, as users and more machines would be able to communicate with each other in real-time. The communication enables complex tasks to be accomplished quickly as the time of engagement and finishing in doing a job are significant. The IoT has also impacted data, the capability to collate data at a higher frequency and its reliability can enable rational decision-making on the issue at hand.

Furthermore, the IoT affects "things": the ability to control things like devices (sensors, processors, and actuators) that could communicate with each other to deliver a meaningful purpose and more precisely. Hence, the value of objects like mobile devices will be more helpful. IoT is one of the new markets that can offer numerous opportunities for businesses in diverse fields.

Importantly, changes occur by a small difference, and the IoT could be the source of billions of changes in many areas in just a few years. Consider the IoT as one source for generating data that affects information technology (IT) infrastructure. The utilization of improved approaches in data analysis is part of exceptional and critical opportunities in data generation [40]. Gathering, preparation, and analysis of massive amount of data is not an easy task. Firstly, the volume of data could be doubled or tripled in a few months. Secondly, the nature of this type of data has its peculiar complexities. This type of data template variability is vast and always involves numerous pseudo structured or unstructured formations. Most significantly, to achieve a comprehensive view of the sensor's data, it should not be impossible to evaluate and manage structured and unstructured data. An analysis based on a particular data template can significantly limit the innovative potential idea. Considering its composition, data analysis provides an inclusive analytical perspective to managers who make strategic decisions on the business.

IoT devices, such as sensor data, smartphones, intelligent software, and social media, are useful to decision-makers. It avails them the opportunity of getting valuable data about users, fraud detection, and anticipate future trends. Likewise, consumer connected devices like smart speakers, smart TVs, toys, smart appliances, and wearable devices provide valuable data about users, fraud detection. With the generation of transparent and usable data, big data can create values for organizations to make the changes understandable and widening their performance. The use of generated data from the IoT and the analytical tools brings many opportunities for organizations. These tools utilize predictive modelling techniques, clustering, classification to provide solutions to data mining. IoT improves the decision-making knowledge of decision-makers.

The emergence of IoT and related technologies, like cloud computing, provides the capability to eliminate data sources in various domains. Usually, any data is useful in the domain itself, and data on shared domains can provide various strategies. Artificial intelligence (AI) such as, machine learning algorithms or deep learning algorithms, are key technologies that are applied to offer value-added applications along with IoT and big data besides their utilization in a stand-alone mode [41]. However, the use of these intelligent computational systems was impossible before the advent of cloud computing and IoT, simply due to the extensive data and the need for computational power.

Emerging platforms such as business intelligence platforms, data analysis platforms, and analytical applications help industries and organizations transform processes. Thus, improving productivity which can detect a fault. It is expected that the speed of technological advancement in the next ten years will be equivalent to the last thirty years. Hence, the need to update the IoT technology regarding software, hardware and particularly their security.

Currently, physically unclonable functions (PUFs) are used as one of the promising advanced technologies to secure IoT, simply because of its capability to identify and authenticate IoT objects. It is made possible based on the security protocol of PUFs which utilizes unique keys and timestamps to substantiate nodes and information switch in a given network. However, the approach has a shortfall as it requires a plethora of computing energy to authenticate all the objects and messages over the IoT network [6]. Likewise, the approach of using an authentication server could cause a bottleneck that can reduce performance.

Data sensors, data processing, data connection, software information, smart applications, and several intelligent services connecting to the Internet in collecting and sharing data have tremendously widened the IoT domain. However, these connected devices have resulted in several IoT challenges, which include connectivity, scalability, big data, heterogeneity, security, privacy, and so on. These several challenges are based on different IoT security assessments from multiple sources.

3.4 IoT Security Assessments from Multiple Sources

3.4.1 Data at Rest

Data stored in databases, software applications, or in the cloud can be referred to as being "at rest." Most private and public organizations depend on traditional perimeter-based defences, using anti-virus or firewall programs, in protecting data at rest. But cybercriminals discover these stores of data attractive and vulnerable. Thus, the cloud security alliance (CSA) and broadband internet technical advisory group (BITAG) help recommend

the deployment of both software and hardware encryption techniques to maintain the integrity and security of data at rest.

3.4.2 Data in Use

The data "in use" should be accessible to devices and users through an application or gateway; this situation makes the data difficult to secure. Therefore, with data in-use, security relies on the power of verification or authentication and authorization procedures and the number of devices and users accessing the data.

3.4.3 Data in Flight

This involves data transition from one place to another, such as from a device to the Cloud. Well-established Internet communication protocols armed with modern cryptography algorithms make it virtually impossible for cybercriminals like hackers to decipher data in transit. Although numerous IoT devices support multiple security protocols, few provide security as part of the initial configuration. IoT devices that are connecting to either remote gateways or mobile software applications utilize the hypertext transfer protocol secure (HTTPS), and secure file transfer protocol (SFTP). It also utilizes transport layer security (TLS), domain name system (DNS), security extensions, and other secure encryption protocols. The main problem is that IoT and connected objects are entirely new; therefore, security was not often the priority in many products design.

Different factors influence the security assessment of IoT and how it is addressed. Most of these factors accurately identify previous, current, and future security risks, calculating financial cost and non-financial cost. That is, estimating the cost of eliminating security risks. Likewise, there is a need to focus security assessment on IoT's multifaceted security requirements such as confidentiality, integrity, authentication, authorization, access, and integrity. Such security requirements in the domain of the IoTs is discussed in the next section.

4 IoT Security Requirements

Security issues often accompany new technologies, just as in the IoT domain. It does not hinder their immediate adoption, but it affects their full adoption in every field and their effective usage. People are interested in new technologies because they want to understand the novel idea behind such technology. Hence the craving for utilization without knowing that there is little or no security defence in such technology. Nevertheless, insufficient security defences and legal protections in new technology can have low adoption in the nearest future.

Currently, the security condition of IoT is poor, ranging from architectural design to application level. Therefore, it is urgently required to ensure sufficient security and legal protection for the IoT. Like traditional information technologies, IoT security requirements involve availability, integrity, confidentiality, authentication, authorization, and access control. These requirements should not be limited to data, but need to include the "Things", sensing objects, network communications, and applications of IoT. Some of the requirements are briefly discussed as follows:

Accessibility accessibility or access is about allowing only the legal users to retrieve or get data or information from a digital device. The legal users are not deprived of using such data or information.

Confidentiality confidentiality is about ensuring that data is stored privately with only the legal users of the data. Confidentiality involves providing the security mechanism in the form of encryption protocol that would seal the IoT system and make it impossible for a hacker to launch attacks. In so doing, confidence is given to the users to utilize the IoT without fear of insecurity or thought about an intruder's threat. Cryptographic techniques have gained the popularity of ensuring confidentiality in the usage and functionality of IoT for security purposes.

Authentication has to do with the verification of data to ensure that the request is not coming from an unauthorized source and that it is delivered to the real user or sender.

Authorization after verification of data, then access or service can be granted to the user that is presumed to be legal. The security requirements of IoT are presented in Table 2.

5 Security Challenges of IoT

IoT security refers to the safeguarding measures taken to ascertain the smooth functionality of IoT devices, minimizing their operational or handling damages and also limiting susceptibility to remote attacks by criminals. Security and privacy are now an issue with the type of ubiquitous computing that is coming in the future. Data security would continue to be an issue in IoT devices and on the cloud platform. Similarly, there are concerns in the aspect of privacy. Over the years, the number of devices connected to the Internet has rapidly increased.

The increasing threat to IoT underlines the significance of researching for practical solutions. The practical solution that can address the trending insecurity issue and eliminate or drastically mitigate the rate at which IoT systems may be attacked by hackers operating from the cyberspace. In the year 2016, one can recall that the distributed denial of service (DDoS) attacks affected IoT services and devices across the World. It was an eye-opener and a proof that the security threat against IoT is not abstract but is real. Notwithstanding, a solution can be feasible when personal security measures could use safeguard devices against known and unknown cyber-attackers.

Today, intelligent transportation, smart cities, smart home, smart grids, smart healthcare, and others have significantly expanded the IoT network. IoT networks are not just a kind of sensor network, but they are multi-complex and implement or use the WSNs scheme as a sub-part of their entire ecosystem. Since many devices are connected to the Internet, therefore, there are different challenges in IoT, especially in the aspect of its vulnerability. These challenges include the rise of botnets, lack of encryption, weak password, connectivity, financial breaches, unreliable detection model, scalability, big data, heterogeneity, security, privacy, etc.

5.1 New Security Vulnerabilities

In as much as more businesses embrace the IoTs, then new security vulnerabilities will continue to emerge. The increased risk of security breaches may be attributed to device/object limitations. Some of the challenges in the security of IoTs are discussed as follows;

Table 2 IoT Security requirements

Security requirements	Description	IoT security properties
Availability	The IoT resource is readily available	Security features and mechanisms must be capable of preventing or detecting denial of service (DoS) attacks on IoT resources
Integrity	Guarantee of IoT trustworthiness, accuracy, and consistency of data and services of its life cycle	Security apparatus must be capable of detecting data manipulation and modification like deletion, insertion or occurring attacks on the "Things" or IoT data
Confidentially	IoT protection from illegal user and access	Security mechanisms and defences must be capable of protecting: Connection between or amongst "things", sensing objects, network communications Data at storage in the data warehouse, data centre, i.e. protection of data-at-rest Data transmission to/from "things", sensing systems, network communications and applications of IoT (protecting data-in-motion) Information delivered to end-users like the result of the analysis
Authentication	The guarantee that the user is the right person	Security defences must be capable of ensuring "things" Verification or Authentication Sources of data- authentication
Authorization	Prevention of illegal utilization of IoT resources	Security mechanisms must be capable of ensuring that Only the legal "Things" can access the network of IoT
Access Control	The management and prevention of illegal use of resources of IoT	Security mechanisms must be capable of ensuring that Devices of IoT are qualified to verify if specific devices are authorized to access their available data

1. The Rise of Botnets

Recently, there has been an increase in botnets attacks. Botnets are a network of computers infected with malicious software and controlled as a group without owners' knowledge among IoT devices. A botnet exists when malicious hackers remotely control internet-connected devices then use the information acquired for illegal purposes. An enterprise like a hospital can have their computer network devices co-opted as part of a botnet without the management knowing it. The problem is that most organizations, like the hospital, lack real-time security solutions to track botnet.

2. The large volume of IoT Devices

In the past few years, cybersecurity experts were focused mainly on protecting computers and mobile devices. Nevertheless, today, IoT devices have proliferated private and public organizations. There are currently about 7 billion devices around, and that number could increase to 20 billion by the year 2020. More IoT devices mean growing security vulnerabilities causing an increasing challenge for security experts.

3. Lack of Encryption

Though encryption technique is a great measure to halt hackers from gaining access to data, however, it is one of the key IoT security challenges. These IoT devices could lack storage and processing abilities that may be inclusive on a traditional computer. The result is an increasing attack where hackers could easily manipulate the designed algorithms for safety and protection.

4. Outdated Legacy Security

Another concern is the interconnected legacy systems. In an enterprise with an increasing number of IoT devices, legacy technologies seem to be out of place. A breach in a specific IoT device may result in a violation of an interconnected legacy system that has no modern security standards.

5. Weak Default Passwords

Most IoT devices have weak default passwords. Though the practice is that passwords should be changed, yet some information technology (IT) managers fail to take this simple instruction. A weak or easy-to-guess password can make a particular IoT device to be vulnerable to a brute force attack. This is a critical issue common in some country which requires urgent attention. For instance, in the USA, California authorities banned default passwords in the year 2018.

6. Unreliable Threat Detection Models

Many enterprises have numerous techniques for detecting data breaches involving spotting indicators, monitoring user's activity, and security protocols. An increasing number of IoT devices and device complexities, conventional threat handling approaches may not be reliable, but be of a challenge.

7. Small Scale Attacks in IoT

Although cyber-security practitioners are focusing on preventing large scale attacks, however, the small-scale kind of attack is amongst the security challenges of IoT. Small scale attacks are more complex to detect and can easily happen without the awareness of an organization. Hackers could breach major technologies of an organization such as cameras, scanners, and printers.

8. Phishing Attacks

Phishing is already a cyber-security concern across all organization technologies, and IoT devices could represent the latest attack vector. Most hackers may send a signal to a particular IoT device that could trigger various complications. Although it is one of the common forms of cyber-security attacks, it can be prevented. Nevertheless, most organizations fail to enlighten their staff on the latest phishing threats and how to ward off or handle different episodes in a case scenario.

9. Inability to Predict Threats

Although security professionals must be more proactive in preventing IoT security breaches early before it occurs. However, some organizations lack the flexible management system which can monitor activity and enable insights into any potential threats. Without this type of proactive solution, an organization will not have the ability to identify potential breaches early enough.

10. Lack of Frequent Software Updates

Software regular updates are one method that IT professionals manage security on mobile devices and computers to ensure their safety. Some IoT devices lack software updates that other technologies may receive; some organizations also struggle to provide important security updates to IoT devices.

11. IoT Financial Breaches

With some organization like a bank using IoT devices for electronic or e-payments, there is usually a risk for hackers breaching sensitive information and has access to steal money. Recently, many organizations are integrating machine learning or blockchain to curb financial fraud before it occurs. Yet, not every organization or enterprise has deployed this solution. The summary of IoT security attack classification is presented in Fig. 3.

Figure 3 depicts various attacks in the IoT, particularly on the hardware and software domain. Several attacks are classified in different forms such as physical attacks, software attacks, network attacks, and encryption attacks. The solution to the challenges must offer a flexible and interoperable communication system with the devices.

12. User's Privacy

Importantly, enterprises must protect user data, that is, the user's data for both the organization's internal and external users. It is a concern because many staff are utilizing

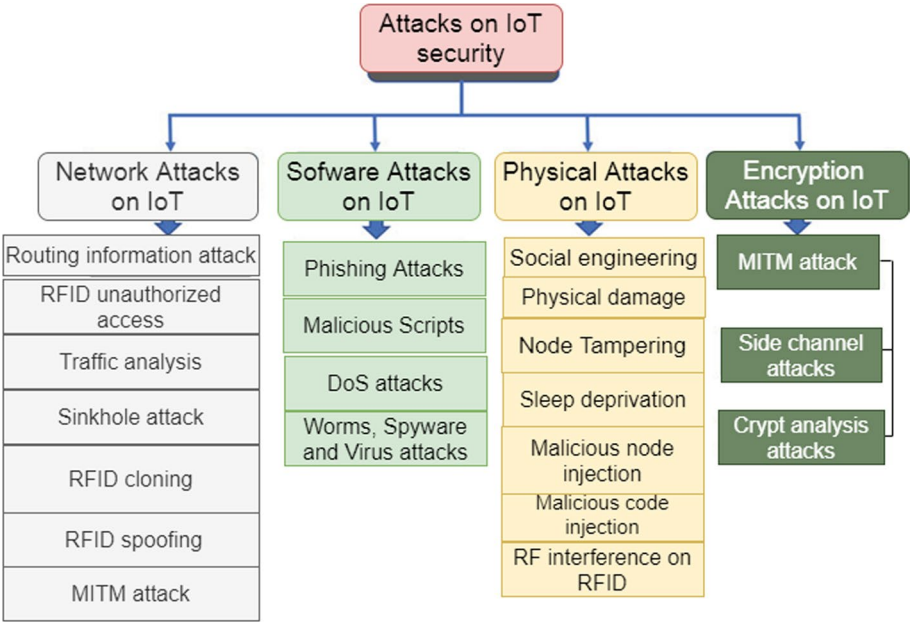

Fig. 3 Classification of IoT attacks

IoT devices provided by their organizations. When a breach occurs and data is compromised, an enterprise reputation would be affected. In light of such challenges, privacy is one of the key IoT security challenges that must be addressed.

13. Heterogeneity of connected devices and Environment

More importantly, the connected system's heterogeneous environment makes management of IoT complex, especially concerning security management [42, 43], and service functions [44]. Therefore, effective and efficient management becomes a problem due to IoT heterogeneity of connected devices and environment. While the IoT system brings the potentiality of improving people's quality of life due to its diverse applications, it comes with many challenges that require immediate addressing for broader adoption.

6 Proposed Solutions to the Security Challenges in the IoT

Many researchers have suggested solutions to the current IoT security challenges for improvement, especially in the areas related to software and hardware security challenges [45]. Suggested solutions include a software approach to IoT security [46], the use of trust management [47], multiple authentication models for IoT [48], and regulation solution [49]. Likewise, rule and signature-based intruder detection serve as one of the techniques for addressing security challenges in the commercial deployments of IoT [50]. The proposed solutions can be classified into eleven, as highlighted in Table 3.

Table 3 Classification of the proposed solutions

S/n	Problems	Proposed solutions	Authors in agreement
1	The risks and uncertainty involving the IoT	Trust management helps in overcoming the risks and uncertainty involving the IoT. Trust between each of the devices during communication for security and privacy	[47, 51–53]
2	The vulnerability of authentication schemes makes them remain insecure in its protection of user privacy	Multiple authentication models for IoT can help in securing and providing privacy services	[54–58]
3	Lack of privacy consideration in the design of the IoT devices	Help users possess the tools to manage their own data privately to secure sensitive information from the public domain	[53, 59]
4	Lack of policy enforcement role	A software approach to IoT security. It profers solution in security architecture to control and monitor the environment	[46, 60, 61]
5	Fault-tolerant security challenge	Assist the device to defend itself against any network failures and attacks. Likewise, enabling safe and ethical use	[53, 62]
6	Lack of adequate IoT protocol for secure communication	IoT protocol stack can match with the classical Internet hosts to generate an extended Internet to enable various existing security solutions to establish secure communication	[63, 64]
7	Lack of secure protocols for preventing routing attacks	It enhances protocols for securing routing in the IoT systems and prevent routing attacks	[65, 66]
8	DDoS attacks in IoT networks	Is useful in detecting, preventing or eliminating DDoS attacks in IoT networks	[57, 58, 67]
9	Spam prevention issue in IoT	Using digital signatures to sign the content in 2D barcodes can help counter spam issues in IoT	[68]
10	There is inadequate semantic logic for critical infrastructure in the IoT architectures	It provides a security model that uses semantic logic for critical infrastructure protection in the IoT. Also, to bridge the gap between the virtual entities and actual devices	[69–71]
11	Lack of regulation brings about security challenges in IoT	Regulation solution to guide device usage and punishment for cybercrime	[3, 49]

6.1 The Proposed Solutions

The classification of the proposed solutions described in Table 3 are discussed as follows;

(a) Trust management

Trust management is crucial in IoT security. The study by [39, 51] illustrated the vital role that trust management plays in the IoT system. Having trust management can be of help to people in overcoming the risks and uncertainty involving the IoT. Trust can be viewed as a concept that comprises of both security and privacy. A study by [53] discusses trust management as a necessity for IoT. Also, [53] agreed that trust is about how users feel when communicating in the IoT. That is to say, the users have the right to control their services at any time, anywhere, and have devices to understand their interactions with the IoT systems. More also, they mention that good management can promote trust in the IoT.

Likewise, a separate investigation by [47, 52] identified some trust correlations. There are needs for trust between each of the devices of the IoT. Communication and the process of changing between the devices must be secure and private. There are needs of trust for security and privacy; invariably in each layer, each IoT device must be protected, whatever may be the circumstance. Hence, there must be trust between the user and the IoT device.

Furthermore, [52] enumerated other areas of trust management in the IoT functionality. The research team stated that the core objectives of trust in the IoT are the capability of generating new models for shared trust. Establishing trust will enable the execution of trust paradigm for cloud computing and the design of applications based on node trust. They state that trust assessment should be automated and autonomous. Generally, it is necessary to have a security mechanism that limits data mismanagement and provide extensive information sharing to strengthen the IoT.

(b) Authentication

Designing of multiple authentication models for IoT can help in securing and providing privacy services. The work by [57, 58] shows authentication models for IoT security and privacy. The models may authenticate by security token, authenticate by a gateway, authenticate by trust chain or authenticate by global trust tree. That is, each model has its own merits and demerits. Similarly, [56] made a proposition of lightweight two-level session key management for end-user authentication in IoT. The paper contributes to a two-level session key (TKS) based authentication mechanism for IoT security. In addressing the challenge of user authentication in ubiquitous networks, [55] applied a password-based authentication to roam in ubiquitous networks to improve security. A subsequent study by [48], attempted to fix the security flaws in the work of [55] by introducing the biometric-based authentication scheme using bio-hash to implement a three-factor authentication. The result proved that the proposed scheme was appropriate for resource-constrained ubiquitous networking environments.

(c) Privacy Solutions

There are several solutions to privacy issues as identified in the literature. For example, the work by [53] provides unique solutions for privacy concerns in the IoT. Every user should pose the tools to manage their data. Thus, at the process of a design, privacy

issue is borne in mind; this is referred to as the principle of privacy by design. Also, there is a principle of transparency. In the context of IoT, transparency means that users need to know which body or structure is managing their data and how and when it is in use. Hence transparency policies must be put in place to fortify privacy. Data management is another proffered solution. That is, knowing who is responsible for managing the data kept in secret. There is a need for different policies on data management and likewise, policy-enforcement systems for privacy solutions. The study by [59] proposed a suitable solution to address privacy concerns of IoT data in cloud environments. The proposed solution, which was referred to as User-driven Privacy Enforcement for Cloud-based Services in the IoT (UPECSI), allows users to control their sensitive public information before uploading to the cloud space.

(d) Policy Enforcement

Nowadays, the policy enforcement role is viewed as an essential method to tackle any security problem in every society. According to the European Union (EU) legislation, data protection is critical to people's privacy; that is, privacy rights should be protected during every party's interaction in the digital world of IoT. The work by [61] focuses on a software approach to IoT security. It proffers solution in the security architecture comprising micro security functions known as μmboxes. The architectural solution has a centralized IoTSec controller that can monitor the environment and creates a general understanding of cross-technology policy enforcement. Network managers can represent and configure novel μmboxes and their transmission mechanisms from the created general understanding.

On the IoT design standardization, the paper by [46] proposed the design of a standardized network security policy for the IoT devices. It demonstrates that the network behaviour of massive consumers of IoT devices seems to be predictable, simple to profile, and constrain. Thus, there is a need to address the lack of generic policy frameworks for instrumentation and assurance of various execution policies for IoT services. The study by [60], proposed P4SINC as an implementation of a policy framework that addressed various functionalities of services deployed in software-defined machines for the IoT infrastructures.

(e) Fault Tolerance

Different requirements for IoT systems on fault-tolerant have been proposed. Due to the growing number of attacks on the Internet and its devices, [16] focuses on securing the IoT by cultivating a novel solution for safe and ethical use. In their approach, they listed diverse requirements for IoT devices to achieve fault-tolerance. According to them, it entails three requirements. Firstly, all devices should be secure by default. Secondly, all IoT devices should be activated to know the status of the network and services. Thirdly, every device or object must be able to defend itself against any network failures and attacks. Once an attack interrupts the service, the devices should respond fast and recover from or withstand any damage. An investigation by [62] presented learning automata (LA) and mixed cross-layered-based fault-tolerant routing protocol for IoT. The LA successfully delivers packets of data, even amid faults between a pair of source and nodes.

(f) Secure Communication

Several protocols for IoT systems have been proposed to address secure communication. For instance, the study by [63] discusses how the IoT protocol stack can relate to the classical Internet host to generate extended Internet, which will enable the utilization of various existing security solutions. Furthermore, the investigation by [64] established secure communication protocols by providing solutions based on asymmetric and symmetric pre-distributed keys for securing communication in IoT.

(g) Secure Routing

More also, many protocols exist on enhancing secure routing for IoT systems. The work by [66] presents secure routing protocols for preventing routing attacks. These routing protocols include a secure multi-hop routing protocol (SMRP), and a trust-aware secure routing framework (TSFR). In addition to two-way acknowledgement-based trust (2-ACKT), a collaborative lightweight trust-based routing protocol (CLT), and a group-based trust management scheme (GTMS) to address secure routing challenges in IoT. The research by [65] proposed secure routing for MANET connected IoT systems with a concentration on the standardized routing protocol for lossy networks and low power. Analysis of the result shows that some key research challenges identified in MANET-IoT connectivity were resolved using the proposed approach.

(h) Distributed Denial of Service (DDoS) Protection

In the literature, there are many solutions proposed to handle DDoS attacks in IoT networks. DDoS disrupts service by creating network congestion and then disabling normal functions of network devices. This disruption of services is even more unsafe for IoT devices and users. In 2015, [57] proposed a learning automaton (LA) to solve DDoS attacks in IoT systems. The LA is capable of intelligently computing the packet sampling rate from the environment. The DDoS prevention part in each device can monitor the requests the device receives, and once a pre-set maximum level is exceeded, it will issue out a DDoS alert to neighbouring nodes. As soon as the alert is issued, the devices will sample the IP addresses and attempt to detect the attacker. When the attacker is identified, other nodes can be notified of the attacker and would automatically drop any packets arriving from the attacker's IP.

Based on this technique, Zhang et al. [58] led the research team to propose their paradigm for detecting and preventing DDoS attacks in an IoT system. Aside from the Zhang et al., approach in tackling DDoS attacks, other approaches back-up the sink node, that is, a node that accepts the data collected by sensors. Then the new node will be a redundant channel to hold a portion of the sink node's responsibilities. However, this approach can be cost-effective. Likewise, at application-level, DDoS attacks through compromised devices of IoT is emerging as a critical issue. The application-level and legitimate nature of traffic make most current solutions ineffective and inefficient. Similarly, the distribution of traffic makes mitigation costly.

In addressing this problem, the work by [67] suggested a new approach that leverages edge computing to apply edge functions that collect information on in-coming traffic and communicate such information by a fast-path with a close-by detection service to handle such attacks. The investigation by [57] focuses on a preventive measure to avoid

DDoS attacks over IoT network. The idea uses a lightweight defensive algorithm for DDoS attack over the IoT network environment to test against several scenarios and dissect the interactive communication among types of network nodes.

(i) Spam Prevention

In providing a solution to IoT insecurity, spam prevention is another option. The use of digital signatures to sign the content in 2D barcodes can be effective. For example, recent work by [68] concentrated on spamming the IoTs; the result of the study recommends that to prevent IoT's spam is to utilize digital signatures to sign the content in 2D barcodes. Technologically, the barcode would have the original content, the barcode creator's public key, and digitally signed content. The certificates authenticating the creator's identity can be placed in the uniform resource locator (URL) where the barcode points. An application would then verify the quick response (QR) code's integrity and also verify the certificate chain.

(j) IoT Architectures

IoT devices are rapidly increasing, and the connectivity option varies along with the evolution of information and communication technology. Companies are implementing various IoT architectures. However, the architectural technology of IoT is still evolving. Indeed, architecture plays a critical role in the IoT security challenge. Most recent work by [69] in 2019, presents an architecture for behavioural-based device identification. The result demonstrates a security model that uses semantic logic for critical infrastructure, and it played a major role in evaluating the infrastructure's security.

The survey work by [70], presents the four most dominant IoT architectures and analyzed their security and privacy components regarding the requirements. The analysis demonstrates a common area of security and privacy requirements for IoT in addressing the challenge of IoT architectures, especially from the angle of security, privacy, and trust. The result showed the IoT architecture bridging the gap between the virtual entities and actual devices that bring about services.

Moreover, the paper by [71], describes an overall architecture for IoT and analyzes some known and unknown threats for the trust (SPT) security, and privacy at different levels of architecture. Notably, the outcome presents a tentative layered view of security architecture.

(k) Regulation Solutions to the IoT insecurity

The regulation solution is the first step of consideration for addressing the security challenge of new technology such as the IoT. Law and policies should guide devices usage and punishment for cybercrime. In the year 2013, RAND was asked by the European Commission to establish rules for the IoT. The RAND reported that the best regulation for IoT is "soft law", that must have standards, supervision, and moral support while ensuring freedom for the industry. Legislation must embrace the right to information, provisions to restrict or prohibit the utilization of mechanisms of the IoT.

There should be law and policy measures to ensure the architecture's resilience of attacks, data authentication, authorization, access control and user's privacy. The robust legal framework should consider the underlying IoT technology and should be established

by a national and international legislator. Likewise, there can be an establishment of a special task force comprising of computer professionals, judicial and law experts researching the security, privacy, and legal challenges of the IoT. Current security solutions are not yet satisfied with the growing number of IoT devices as there are a plethora of security and privacy challenges facing the IoT industry.

The work by [49] focuses on IoT standardization in terms of challenges, perspectives, and solutions. It introduces a security framework for the organization to bridge the lack of guidelines in the IoT industry. In [3], the researchers recommended efficient mechanisms for collecting, processing, and delivering data generated from medical equipment, sensors, wearable devices, and humans to advance healthcare services. They implemented a framework that is a flexible policy based on the IoT paradigm to face security and quality threats of massive dynamic scale and heterogeneity in smart healthcare environments.

7 Research Gaps in IoT Security

There are some identified research gaps in IoT security, most chosen articles emphasize those topics under its focus; however, some pointed out more general research gaps. [72] reported that they observed two issues that need further research in the study by [4]. They mentioned swarm attestation in the next generation of IoT devices and secure management for IoT devices.

1. Swarm attestation

Attestation of the device is a great and promising solution to the peremptory operational requests of embedded devices, particularly those extensively utilized in IoTs and cyber-physical systems [73]. The swarm attestation approach was proposed to efficiently detect illegitimate changes in a vast network such as cooperative remote attestation scheme by [74]. Also, Carpent et al. [75–77], proposed lightweight swarm attestation and also remote attestation via self-measurement in 2018. Notwithstanding, most of the methods do not enable scalable identification of detected systems, which is vital in keeping a swarm network trustworthy in practice.

In solving this scalable identification problem, the paper by [54] introduced a lightweight attestation approach with efficient, scalable identification of some targeted devices. The proposed method was referred to as "Collective Attestation for Manageable IoT Environments (CAMIE). The result demonstrates that CAMIE can facilitate the management process. However, it still has challenges, because it assumes that the network topology was static at the attestation process, and it might not be in the like condition for high mobility environments. This is a loophole in the system's practical functionality since to support high mobility swarm network systems; there is a need to address frequent modifications of region members.

Likewise, there is a need to improve the membership management in the attestation and operational phases as future work. More research attention is required on swarm attestation in IoT without the assumption that the network topology is static at the attestation process or otherwise to achieve better success. Therefore, the attestation of these systems, referred to as swarm attestation in IoT, is still an open research problem.

2. Secure management for IoT devices

The humongous increase in the proliferation of IoT devices in every sphere of human lives continues to make device management extremely complicated. Several propositions have been made to handle the complexity of device management in the IoT. A paper by Perumal et al. [78] applied a lightweight IoT device management framework to home services. Although the framework can be deployed at home gateways and consumer smart devices. Notwithstanding, there is a need for practical implementation and performance assessment for secure IoT management. The research by [79, 80] recommended the need for a secure privacy-preserving solution for the IoT. They noted that the current solutions are computationally extensive for the resource-constrained gadgets that largely constitutes the IoT. They agreed that IoT applications require a solution that is not based on expensive bilinear pairing but enable short signatures and is easy to deploy in memory-constrained devices.

A study by [16] opined that there had been little advances in managing access control law and policies in the distributed IoT. The current access control law and policies cannot be used in distributed environments due to consistency and scalability issues. Likewise, role-based access control policies using certificates require an urgent infrastructure to authenticate the certificates in a cross-domain environment.

The work by Singh et al. [81] highlighted multiple research aspects that are yet unexplored in the IoT and cloud environments. These aspects of unexplored IoT and cloud environments include in-cloud data sharing, auditing cloud security, composite service responsibility, data combination, and the impact or effect of cloud decentralization. These are a few amongst many other areas requiring further research to provide better security for IoT systems.

3. Identifying sensitive data

In managing IoT devices, there is a need to identify sensitive data by distinguishing between sensitive and non-sensitive data. In the context of IoT, data is perceived as been sensitive since data will summarise different areas of the physical environment, such as highly critical data about an individual, groups, organizations, and government. Also, data may have physical consequences, like actuating commands. The security paradigm must be designed to take account of the potential sensitivity of the data. Hence, it is necessary to conduct research that handles the IoT security paradigm to cater for potentially sensitive data.

4. In-cloud data security

Future research is required for in-cloud data protection, as most cloud service providers cannot protect data within their services to prevent data leakage. There is no cloud data security put in place during data transmission, during data processing, even at data storage in the cloud platform. Regrettably, data leakage to cybercriminals continues to be a problem given the incessant attacks that continue to ravage our infrastructures [82, 83]. There are no complete mechanisms for protecting unauthorized parties (such as cloud insiders and cloud users) from data leakages. Hence, more investigations are required to address security challenges in IoT to mitigate in-cloud data insecurity.

5. In-cloud data sharing

Currently, cloud computing offers services such as data sharing without means of securing the data. The current cloud service providers may also have no means of protecting the data from multiple processing streams. To offer such a service, the IoT system needs to be designed to control multiple applications. Therefore, there is a need to protect data when in transit, storage, and during sharing. The paper by [84] proposed applications that allow the reuse of highly distributed IoT resources, and the result granted secure access to the data shared by devices. Nevertheless, more works are required to address insecurity in-cloud data sharing.

6. Data combination

In the Internet of things, the word "things" like the connected devices often act as data producers and consumers, thereby generating or processing data of different levels of sensitivity. Some streams might be inherently sensitive, such as an individual's heart-rate sensor, or a location sensor on someone's device. Nevertheless, even if individual data streams are harmful, data combination applications could cause critical privacy and security issues.

7. Auditing cloud security

The recent stream in cloud activities, and the evolving IoT commerce has indicated a need for work on the audit. Trustworthy audit services are necessary for cloud providers, clients or tenants, and end-users. Users and tenants can be assured that the cloud is performing as it ought to be, that is, getting value for money spent and getting protection from data leaks, misconfigurations, and other security challenges. Also, auditing is relevant for confirming compliance with policy guidelines and law. As such, information is useful in reinforcing accountability.

More also, such information would be helpful to bodies charged with responsibility for enforcing information that is related to the policy framework on auditing. [85] proposed a framework where a cloud provider could generate an audit log for cloud tenant to show compliance with policy regulation. It is important that audit mechanisms are developed, not only to address the scale of the IoT objective. But for ensuring that all relevant areas are captured and that access to audited information is appropriately regulated. Hence, research is required in the area where data can be used and reused for various purposes and successes without compromising its security.

8. Composite service responsibility

Normally, there are three models of cloud service that can be compared relatively. The three models of cloud service are Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). Each of these models of cloud service has its benefits and variances. Therefore, it is vital to know the differences amongst IaaS, SaaS, and PaaS, to effectively select a suitable one for oneself or an organization.

Cloud service providers often leverage several third-party services. For example, a platform as a service (PaaS) is usually regarded as a cloud computing model whereby a third-party provider offers hardware and software tools, especially those required to develop an

application for people on the Internet. PaaS provides computing platforms that usually include the operating system (OS), web server, database, programming language execution environment, etc. Examples of PaaS are Google App Engine, AWS Elastic Beanstalk, Heroku, Force.com, OpenShift, Apache Stratos, and Windows Azure. Unfortunately, the legal obligations that can enable security of service integration among these cloud service providers are not yet properly harmonized.

Also, some third-party services might be involved in providing analytic tools and log archiving. Observably, the legal obligations between providers, tenants or clients, end-users, and the whole supply chain providers could be unclear. However, some recent studies handled these concerns. Henze et al. [59] proposed an annotation, negotiation, and audit system for the multi-party layered cloud that provides (SaaS, PaaS, and IaaS) to support tenant or clients specified requirements. Such concerns become more multi-complex in an IoT context, whereby services can be composed dynamically to a greater degree. Thus, future work is needed to address multi-complexity in cloud computing models in the context of IoT both technically and in legal provision for a better security purpose.

9. Impact of cloud decentralization

The concept of cloud decentralization attracts security solution. Cloud decentralization could mitigate the attack surface of the cloud model, and also reduce the vulnerability of DDoS since fewer 'things' will directly connect with cloud services in a remote area. On the other hand, the smaller, decentralized entities may be less reliable, especially about security mechanisms that can be used, and more vulnerable to DDoS, due to the absence of resource elasticity. Moreover, decentralization could be susceptible to regular attacks, which can be directed against a person, cloud provider, data flows, cloud infrastructure. These attacks could cause more management concerns and cost implications. All these concerns call for future research to provide improvement for more adoption of IoT.

10. Certification of cloud service providers

Certification could mean system configuration, and the related management processes such as risk management, either at a human point of view, that is, engineer's involvement, or regulating physical access. Then to a more technical angle, that is adherent to security standards, etc. Government and health regulated sectors may only consider cloud service offerings that are certified as being compliant over the relevant control landscape. Currently, certification is always the only option to show compliance with regulations [86]. The automation of certification processes has been considered [87, 88]. Notwithstanding, certification is a human-centred protocol that evaluates system behaviour during the auditing. Modifications to deployment could trigger the necessity for recertification, that attract time and cost process.

The installation of new software or gadgets requires going through a certification process; hence, constituting inefficiencies. Generally, such constraints do not tally with the flexible vision of cloud computing, or IoT-Cloud. Thus, a more technical approach of demonstrating compliance and defining the cloud provider's behaviour is urgently required to strengthen security in the IoT.

11. Malicious ‘things’ protection of provider

The cloud provider often maintains different access, and other controls, in protection against targeted attacks, for instance, a criminal ‘thing’ trying to exploit the service, may be using injection attack. Assuming the attacks are successful, cloud isolation mechanisms provide containment by limiting their fallout. Hence, there is a need to explore superb DoS techniques taking cognizant that IoT expansion can increase the chance of such an attack, especially as ‘things or devices’ become substantially integrated on cloud services.

12. Malicious ‘things’ protection of others

Since the cloud would function as a coordinator and mediator between ‘things’; it provides potential in enhancing security over the IoT ecosystem. This security enhancement is because the cloud offers a natural “choke-point” between ‘things’, where security policy could be developed, executed, and enforced. Hence, thereby requiring input data to go through an authentication process, enabling the cloud to actively disconnect or disregard inputs from ‘things’ discovered or detected as malicious.

Also, this detection can help to ensure the integrity of data, as only valid data in the form of rate or format instead of those from a faulty, malicious (compromised), or inappropriate probably from non-malicious ‘thing’ can penetrate a possibly shared database or transmit to others through the cloud. A fundamental consideration is in ascertaining the ‘things’ that were compromised as affirming malicious things could be relevant at various levels, considering the situations. The methods can involve knowing the malicious or untrusted areas in a network. Also, compromised things may be determined by patterns of behaviour, analysis of the data outputs, or reputation of a ‘thing’ or perhaps involve human intervention, such as reporting a device missing. Therefore, future work is required on creating such techniques, that can determine malicious things by new advancements in technologies and their applications.

13. Security for WSN

WSN is a sensor network representing a crucial component in IoT environments. For instance, WSN can cooperate with RFID systems to enhance tracking, obtain information about movement, position, temperature, etc. Sensor networks are usually composed of a high number of sensing nodes, that can communicate in a wireless multi-hop fashion. Special nodes, such as sinks are typically employed to collect results. WSNs could provide different useful data in areas such as healthcare and environmental services like natural disaster forecasting.

It provides data helpful in defence such as in military target tracking and surveillance, useful data in seismic sensing, hazardous environment exploration, government, etc. Nevertheless, sensor networks face several challenges concerning their communications, i.e. short communication range, mobility, reliability, security, privacy, etc.

Likewise, sensor networks face several challenges in resources: power considerations, bandwidth availability, processing capabilities, storage capacity, etc. Besides, WSN has its design and resource constraints such as application and environment and depend heavily on the environment’s size under monitoring. Scientifically, many issues in the WSN have been deeply addressed, including concerns associated with sensor networks

at various layers such as reliability, energy efficiency, scalability, robustness, etc. Nevertheless, more research is still needed in WSN to tackle reliability, energy efficiency, scalability, and robustness issues, especially those requiring security and privacy.

14. Legal framework establishment

The development, establishment, and implementation of the adequate legal framework in the IoT requires a systematic approach associated with the legislative process. Thus, the research about RFID using scenarios is systematically conducted to prove relevant and sufficiently understood facts before an adequate legal framework could be drafted. Potential legal problems and occurring legal challenges can be addressed systematically by coordinating along with four technical angles, that is, ubiquity, vertically, technically, and globally. The legal framework of IoT and RFID security and privacy require qualitative and quantitative harmonization. Notably, the question of how much privacy civil society is ready to accept to increase connectivity needs addressing. Significant legal solutions should be considered for security and privacy, not as against, but as rules that influence each other.

Uploading or transferring data to the Internet is a source of many problems to information technology (IT) organizations as hacking increases. Transferring data on the Internet, especially data associated with a sensitive device, could be unsafe. Many IoT devices need to consider security as an important aspect, then ensuring that any leaks are prevented before hackers discover it. Hence, research is necessary to put a security mechanism in place in the manufacturing of IoT devices.

8 Future Directions

Recently, various security architectures and models were proposed as a solution to IoT security and privacy challenges. Most of these propositions are focused on securing a specific area of IoT and they require additional investigation. They include:

1. Architecture—that is, the cyber physical, social-based security model [89, 90]. The studies concentrated on Unit IoT and Ubiquitous IoT (U2IoT) architectural model, and the grid of security method to protect the software-defined networking (SDN) based architecture. SDN is a method for utilizing open protocols, like OpenFlow, to control the nodes or edges of the network in accessing networking switches and routers that usually can make use of closed and proprietary firmware.
2. Things- such as object-based security architecture (OSCAR) [91–93] was introduced. OSCAR is used to secure communication between constrained application protocol (CoAP) nodes [94–96]. Likewise, to secure physically unclonable functions (PUFs) based verification protocol [97, 98] for securing RFID system.
3. Security architectures and models on networks include a lightweight security mechanism for IPsec, DTLS, and IEEE 802.15.4 link layer requires further research attention for more successes [99, 100]
4. Security architectures and models on applications require further study for more successes. Examples are media-aware security frameworks for a diverse multimedia service [101–103]. Notwithstanding, most of these studies are focused mainly to secure the "things", systems, networks, and applications in terms of point-to-point defences. Exam-

ple, connection and communication over the IoT systems are secured through traditional network security protocol like LDAP, Kerberos, IPSec, RADIUS, Diffie-Hellman SSH, etc.

Meanwhile, the traditional access control systems (ACS) is applied to control data access by authenticating the user's credentials. With the diversification of IoT architecture, the traditional security paradigms which are limited to point-to-point defences for "things", systems, networks, and applications is inefficient to address the emerging cyber advanced persistent threats (APT) and malicious insider attacks. The malicious attack can be directed towards identified sensitive points in the infrastructure of IoT. An example, a multi-hop wireless broadcast communication in the IoT network is susceptible to intruding. These scenarios become dangerous in an environment of Bring Your Own Technology (BYOT) or Bring Your Device (BYD).

Furthermore, the exponential growth of heterogeneous connected devices from many networks becomes worrisome based on the issues of scalability and interoperability of traditional security mechanisms. It was observed from the literature that there are no single security and privacy model that can address all the issues in the IoT networks and applications. Therefore, future work should explore an alternative to secure IoT architecture, applying a data centric security method directed to protecting the data wherever it transits to throughout its lifecycle (i.e. data-in-transform, data-in-transit, and data-at-rest).

9 Recommendations

Aside from the earlier possible solutions to IoT insecurity as discussed in prior sections, both parties need to consider certain things, that is, IoT users should ensure a safer approach while leveraging the IoT devices. The recommendations for IoT service providers and users are outlined as follows;

1. *Social Engineering* With the tremendous impact of social media platforms, many end-users share their private details publicly on social media sites like Instagram, WhatsApp, Facebook, Twitter, etc. With such a massive user-base, the cyber-hawkers see social media as a lucrative or new place to spread malicious malware. Hence, IoT users should not disclose their private information to an unknown individual either across social media sites, on the phone or by email.
2. *Software Installation Updates* There is a need to ensure that the mobile app and IoT devices are updated. Also, end-users must desist from downloading any malicious or untrusted software or clicking on any adware program link to avoid inviting the dangerous malware into their devices. For example, end-users may receive any health or bytes promotion ads by clicking on the adware link or downloading a targeted malicious app. IoT users could allow the cyber-attacker to gain access to their devices, and they will be able to monitor the user's privacy remotely. After the attacker compromises the user's mobile device, they can secretly acquire private information without the user's knowledge. Therefore, before downloading any app or clicking on such adware links, IoT users should verify the authenticity or source of the links to prevent the installation of malicious malware into either their mobile app or IoT devices.

3. *Firmware/Application Updates* Cybercriminals are often searching for weak links to attack targeted victims, which could be through IoT users or mobile apps. For example, obsolete mobile apps are the most vulnerable to security threats. Therefore, there is a need for regular updating on mobile apps to ensure the IoT device's latest firmware to mitigate the zero-day attacks; such as the latest security threats unknown to security systems. End-users should update their device apps and firmware to prevent malicious security breaches [104].
4. *Creation of Awareness Program* IoT service providers should create awareness against attackers. By putting these countermeasures into practice, the possibilities of security and privacy threats targeted toward the IoT environment can be mitigated or averted, therefore enabling a safe and secure remote caregivingprograms like online training workshops or surveys to keep educating the IoT users regularly to be familiar with the latest information on cybercrimes, hacking, tactics, and to know possible countermeasures.
5. *Fixing broadband Internet* I suggest that broadband Internet should be fixed globally to balance accessibility inequality between low-income earners and high-income people. That is, using unique town-level data on broadband adoption and quality with security and privacy in mind for safe utilization.

10 Conclusion

Taking cognizance and understanding the volume and value of data generated from the stacks of connected devices (known as the Internet of Things) enables merchants and organizations to build effective solutions that can scale, preserve their data and perform at an optimum in this accelerating data driven IoT market. It also helps in understanding diverse trends in the consumption, usage and storage of data. However, public and private safety concerns, ranging from security in the form of confidentiality, integrity, accessibility amongst others has hindered the strong, rapid and extensive adoption of the IoT even with the great potential it offers.

Leveraging on the above insights, this paper explores literature to identify the security and privacy problems in the IoT revolution. It presented IoT security and privacy issues, concerns, challenges and possible approaches of mitigating the identified insecurity problems and achieving secure networks. Likewise, open issues, research gaps, future works and recommendations were highlighted.

It was found that the security and privacy challenges of the IoT are still new and increasing daily due to more connected devices. To address future challenges, it is necessary to promote a better understanding of the IoT network's challenges. Also, the awareness of the effects of attacks on the IoT must be investigated to prepare potential solutions. Therefore, it is our interest that this paper makes significant contributions to security and privacy in the IoT networks.

Funding This paper was partially supported by the Center for Cyber Safety and Education, Internal Revenue segregated fund of $(ISC)^2$, Code. EIN: 45–2405127 via the (ISC)2 graduate cybersecurity scholarship award, 311 Park Place Blvd. Suite 610 Clearwater, FL 33759, USA.

Code Availability This article contains no source code.

Availability of Data and Material This article contains no data or material other than the articles used for the review and which have been referenced.

Declarations

Conflict of interest All authors declare that there are no conflicting interests of whatsoever.

Human and Animal's Rights This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent Informed consent was not required in this article as no human or animals were involved.

References

1. International Data Corporation. (2019). *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast.* Retrieved October 06, 2020, from https://www.idc.com/getdoc.jsp?containerId=prUS45213219.
2. Schneier, B. (2017). IoT security: What's plan B? *IEEE Security & Privacy, 5,* 96–96.
3. Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security- and quality-aware system architecture for Internet of Things. *Information Systems Frontiers, 18*(4), 665–677.
4. Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference on—DAC* '15 (pp. 1–6).
5. Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Wiley.
6. Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and security challenges and solutions in IOT: A review. In *IOP conference series: Earth and environmental science* (Vol. 322, No. 1, pp. 012013). IOP Publishing.
7. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28.
8. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82,* 395–411.
9. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312.
10. Alrajeh, N. A., & Lloret, J. (2013). Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks. *International Journal of Distributed Sensor Networks, 9*(10), 351047.
11. Abduvaliyev, A., Pathan, A. S. K., Zhou, J., Roman, R., & Wong, W. C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 15*(3), 1223–1237.
12. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks, 76,* 146–164.
13. Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine, 55*(1), 26–33.
14. Yi, S., Qin, Z., & Li, Q. (2015). Security and privacy issues of fog computing: A survey. In *International conference on wireless algorithms, systems, and applications* (pp. 685–695). Springer, Cham.
15. Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. *IEEE Access, 5,* 19293–19304.
16. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78,* 680–698.
17. Barrow, P., Kumari, R., & Manjula, R. (2016). Security in Cloud computing for service delivery models: Challenges and solutions. *Journal of Engineering Research and Applications*, *6*(4), 76–85.
18. Hepsiba, C. L., & Sathiaseelan, J. G. R. (2016). Security issues in service models of cloud computing. *International Journal of Computer Science and Mobile Computing, 5*(3), 610–615.

19. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11.
20. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access, 7,* 82721–82743.
21. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38,* 8–27.
22. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers, 17*(2), 243–259.
23. Kamin, D. A. (2017). *Exploring security, privacy, and reliability strategies to enable the adoption of IoT*. Minneapolis, MN, United States of America: Walden University.
24. Prasad, A. V. (Ed.). (2017). *Exploring the convergence of big data and the internet of things* (Vol. 13, pp. 1–23). IGI Global.
25. Waraga, O. A., Bettayeb, M., Nasir, Q., & Talib, M. A. (2020). Design and implementation of automated IoT security testbed. *Computers & Security, 88,* 101648.
26. Davis, G. (2018). 2020: Life with 50 billion connected devices. In *2018 IEEE international conference on consumer electronics* (ICCE) (pp. 1–1). IEEE.
27. Saha, H. N., Mandal, A., & Sinha, A. (2017). Recent trends in the Internet of Things. In *2017 IEEE 7th annual computing and communication workshop and conference* (CCWC) (pp. 1–4). IEEE.
28. Nordrum, A. (2016). The internet of fewer things [news]. *IEEE Spectrum, 53*(10), 12–13.
29. Chase, J. (2013). The evolution of the internet of things. *Texas Instruments, 1,* 1–7.
30. Yinbiao, S., Lee, K., Lanctot, P., Jianbin, F., Hao, H., Chow, B., & Desbenoit, J. P. (2014). Internet of things: Wireless sensor networks. White Paper, *International Electrotechnical Commission*, http://www.iec. ch, 11.
31. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. In *2012 international conference on computer science and electronics engineering* (Vol. 3, pp. 648–651). IEEE.
32. Banafa, A. (2019). Three major challenges facing IoT. *IEEE Internet of Things Newsletter*, *4*(3), 12–23.
33. Pham, C., Lim, Y., & Tan, Y. (2016). Management architecture for heterogeneous IoT devices in home network. In *2016 IEEE 5th Global Conference on Consumer Electronics* (pp. 1–5). IEEE.
34. Van den Abeele, F., Hoebeke, J., Moerman, I., & Demeester, P. (2015). Integration of heterogeneous devices and communication models via the cloud in the constrained internet of things. *International Journal of Distributed Sensor Networks, 11*(10), 683425.
35. Vargas, D. C. Y., & Salvador, C. E. P. (2016). Smart IoT gateway for heterogeneous devices interoperability. *IEEE Latin America Transactions, 14*(8), 3900–3906.
36. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, *80*, 1–50.
37. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78,* 964–975.
38. Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2017). A review on internet of things (IoT): Security and privacy requirements and the solution approaches. *Global Journal of Computer Science and Technology*, *16*(2), 1–11.
39. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for internet of things. *Journal of Network and Computer Applications, 42,* 120–134.
40. Ahlgren, B., Hidell, M., & Ngai, E. C. H. (2016). Internet of things for smart cities: Interoperability and open data. *IEEE Internet Computing, 20*(6), 52–56.
41. Alansari, Z., Anuar, N. B., Kamsin, A., Belgaum, M. R., Alshaer, J., Soomro, S., & Miraz, M. H. (2018). Internet of things: Infrastructure, architecture, security and privacy. In *2018 International conference on computing, electronics & communications engineering (iCCECE)* (pp. 150–155). IEEE.
42. Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous Internet of Things build our future: A Survey. *IEEE Communications Surveys & Tutorials, 20*(3), 2011–2027.
43. Bao, F., Chen, R., Chang, M., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE transactions on network and service management, 9*(2), 169–183.
44. Kumarage, H., Khalil, I., Tari, Z., & Zomaya, A. (2013). Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling. *Journal of Parallel and Distributed Computing, 73*(6), 790–806.
45. Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017). Security challenges in IoT development: A software engineering perspective. In *Proceedings of the XP2017 scientific workshops* (pp. 1–5).

46. Barrera, D., Molloy, I., & Huang, H. (2018). Standardizing IoT network security policy enforcement. In *Workshop on decentralized IoT security and standards (DISS)* (Vol. 2018, p. 6).
47. Andrea, I., Chrysostomou, C., and Hadjichristofi, G. (2016). Internet of Things: Security vulnerabilities and challenges. In *Proceedings—IEEE symposium on computers and communications* (pp. 180–187).
48. Lee, H., Lee, D., Moon, J., Jung, J., Kang, D., Kim, H., & Won, D. (2018). An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLoS ONE, 13*(3), e0193366.
49. Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IoT standardisation: Challenges, perspectives and solution. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1–9).
50. Coulter, R., & Pan, L. (2018). Intelligent agents defending for an IoT world: A review. *Computers & Security, 73,* 439–458.
51. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. *IEEE World Congress on Services*, 21–28.
52. Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *2014 international conference on privacy and security in mobile systems* (PRISMS) (pp. 1–8). IEEE.
53. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.
54. Lee, J. (2018). Collective attestation for manageable IoT environments. *Applied Sciences, 8*(12), 2652.
55. Chaudhry, S. A., Naqvi, H., Mahmood, K., Ahmad, H. F., & Khan, M. K. (2017). An improved remote user authentication scheme using elliptic curve cryptography. *Wireless Personal Communications, 96*(4), 5355–5373.
56. Mahmood, Z., Ning, H., & Ghafoor, A. (2016). Lightweight two-level session key management for end user authentication in Internet of Things. In *2016 IEEE international conference on internet of things* (iThings) and *IEEE Green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing* (CPSCom) and *IEEE Smart Data* (SmartData) (pp. 323–327). IEEE.
57. Zhang, C., & Green, R. (2015). Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th symposium on communications & networking* (pp. 8–15).
58. Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM symposium on information, computer and communications security* (pp. 1–6).
59. Henze, M., Hummen, R., & Wehrle, K. (2013). The cloud needs cross-layer data handling annotations. In *2013 IEEE security and privacy workshops* (pp. 18–22). IEEE.
60. Phung, P. H., Truong, H. L., & Yasoju, D. T. (2017). P4SINC-an execution policy framework for IoT services in the edge. In *2017 IEEE international congress on internet of things* (ICIOT) (pp. 137–142). IEEE.
61. Yu, T., Sekar, V., Seshan, S., Agarwal, Y., and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices. In *Proceedings of the 14th ACM workshop on hot topics in networks—HotNets-XIV* (pp. 1–7). ACM Press.
62. Misra, S., Gupta, A., Krishna, P. V., Agarwal, H., & Obaidat, M. S. (2012). An adaptive learning approach for fault-tolerant routing in Internet of Things. In *2012 IEEE wireless communications and networking conference* (WCNC) (pp. 815–819). IEEE.
63. Kumar, S. A., Vealey, T., and Srivastava, H. (2016). Security in Internet of Things: Challenges, solutions and future directions. In *49th Hawaii international conference on system sciences* (HICSS) (pp. 5772–5781). IEEE.
64. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks, 32,* 17–31.
65. Karlsson, J., Dooley, L. S., & Pulkkis, G. (2018). Secure routing for MANET connected Internet of Things systems. In *2018 IEEE 6th international conference on future internet of things and cloud* (FiCloud) (pp. 114–119). IEEE.
66. Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications, 66,* 198.
67. Bhardwaj, K., Miranda, J. C., & Gavrilovska, A. (2018). Towards iot-ddos prevention using edge computing. In *{USENIX} workshop on hot topics in edge computing* (HotEdge 18).
68. Razzak, F. (2012). Spamming the Internet of Things: A possibility and its probable solution. *Procedia Computer Science, 10,* 658–665.

69. Zamfiroiu, A., Iancu, B., Boja, C., Georgescu, T., & Cartas, C. (2019). IoT Architectures for Critical Infrastructures Protection. In *European conference on cyber warfare and security* (pp. 613–XII). Academic Conferences International Limited.
70. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the security and privacy of Internet of Things architectures and systems. In *2015 International workshop on secure internet of things (SIoT)* (pp. 49–57). IEEE.
71. Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. In *BODYNETS* (pp. 256–262).
72. Porras, J., Khakurel, J., Knutas, A., & Pänkäläinen, J. (2018). Security challenges and solutions in the internet of things. *Nordic and Baltic Journal of Information and Communications Technologies, 2018*(1), 177–206.
73. Arias, O., Rahman, F., Tehranipoor, M., & Jin, Y. (2018). Device attestation: Past, present, and future. In *2018 Design, automation & test in europe conference & exhibition* (DATE) (pp. 473–478). IEEE.
74. Moon, Y. H., & Jeon, Y. S. (2016). Cooperative remote attestation for IoT swarms. In *2016 International conference on information and communication technology convergence (ICTC)* (pp. 1233–1235). IEEE.
75. Carpent, X., Rattanavipanon, N., & Tsudik, G. (2018). Remote attestation of iot devices via smarm: Shuffled measurements against roving malware. In *2018 IEEE international symposium on hardware oriented security and trust (HOST)* (pp. 9–16). IEEE.
76. Carpent, X., Eldefrawy, K., Rattanavipanon, N., Sadeghi, A. R., & Tsudik, G. (2018). Reconciling remote attestation and safety-critical operation on simple iot devices. In *2018 55th ACM/ESDA/IEEE design automation conference (DAC)* (pp. 1–6). IEEE.
77. Carpent, X., Rattanavipanon, N., & Tsudik, G. (2018). Remote attestation via self-measurement. *ACM Transactions on Design Automation of Electronic Systems (TODAES), 24*(1), 1–15.
78. Perumal, T., Datta, S. K., & Bonnet, C. (2015). IoT device management framework for smart home scenarios. In *2015 IEEE 4th global conference on consumer electronics (GCCE)* (pp. 54–55). IEEE.
79. Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks, 102,* 83–95.
80. Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., & Fujdiak, R. (2019). A secure publish/subscribe protocol for internet of things. In *Proceedings of the 14th international conference on availability, reliability and security* (pp. 1–10).
81. Singh, D., Tripathi, G., & Jara, A. J. (2014). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In *2014 IEEE world forum on Internet of Things* (WF-IoT) (pp. 287–292). IEEE.
82. Abiodun, E. O., Jantan, A., Abiodun, O. I., & Arshad, H. (2020). Reinforcing the security of instant messaging systems using an enhanced honey encryption scheme: The case of WhatsApp. *Wireless Personal Communications, 112,* 1–24.
83. Omolara, A. E., Jantan, A., Abiodun, O. I., Dada, K. V., Arshad, H., & Emmanuel, E. (2019). A deception model robust to eavesdropping over communication for social network systems. *IEEE Access, 7,* 100881–100898.
84. Benazzouz, Y., Munilla, C., Günalp, O., Gallissot, M., & Gürgen, L. (2014). Sharing user IoT devices in the cloud. In *2014 IEEE world forum on internet of things* (WF-IoT) (pp. 373–374). IEEE.
85. Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B., & Villari, M. (2011). A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures. In *2011 IEEE international symposium on parallel and distributed processing workshops and PhD forum* (pp. 1510–1517). IEEE
86. Sunyaev, A., & Schneider, S. (2013). Cloud services certification. *Communications of the ACM, 56*(2), 33–36.
87. Kunz, T., Selzer, A., & Waldmann, U. (2014). Automatic data protection certificates for cloud-services based on secure logging. In *Trusted cloud computing* (pp. 59–75). Springer, Cham.
88. Muñoz, A., & Maña, A. (2013). Bridging the gap between software certification and trusted computing for securing cloud computing. In *2013 IEEE ninth world congress on services* (pp. 103–110). IEEE.
89. Sharma, T., Bambenek, J. C., & Bashir, M. (2020). Preserving privacy in cyber-physical-social systems: An anonymity and access control approach. *CEUR WS, 25*(30), 16–30.
90. Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things, 2*(01), 1.

91. Thampi, S. M., Pérez, G. M., Westphall, C. B., Hu, J., Fan, C. I., & Mármol, F. G. (Eds.). (2017). *Security in Computing and Communications: 5th International Symposium*, SSCC 2017, Manipal, India, September 13–16, 2017, Proceedings (Vol. 746). Springer.
92. Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks, 32,* 3–16.
93. Bose, P., Gąsieniec, L. A., Römer, K., & Wattenhofer, R. (Eds.). (2015). Algorithms for Sensor Systems: 11th International Symposium on Algorithms and Experiments for Wireless Sensor Networks, Algosensors 2015, Patras, Greece, September 17–18, 2015, Revised Selected Papers (Vol. 9536). Springer.
94. Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018). An analysis of CoAP as transport in an Internet of Things environment. In *2018 IST-Africa week conference (IST-Africa)* (pp. Page-1). IEEE.
95. Rahman, R. A., & Shah, B. (2016). Security analysis of IoT protocols: A focus in CoAP. In *2016 3rd MEC international conference on big data and smart city* (ICBDSC) (pp. 1–7). IEEE.
96. Chen, X. (2014). *Constrained application protocol for internet of things*. Retrieved January 3, 2021, from https://www.cse.wustl.edu/~jain/cse574-14/ftp/coap.
97. Qureshi, M. A., & Munir, A. (2020). PUF-IPA: A PUF-based identity preserving protocol for internet of things authentication. In *2020 IEEE 17th annual consumer communications & networking conference (CCNC)* (pp. 1–7). IEEE.
98. Yilmaz, Y., Gunn, S. R., & Halak, B. (2018). Lightweight PUF-based authentication protocol for IoT devices. In *2018 IEEE 3rd international verification and security workshop (IVSW)* (pp. 38–43). IEEE.
99. Abdul-Ghani, H. A., & Konstantas, D. (2019). A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *Journal of Sensor and Actuator Networks, 8*(2), 22.
100. Raza, S. (2013). Lightweight security solutions for the internet of things (Doctoral dissertation, Mälardalen University, Västerås, Sweden).
101. Mazurczyk, W., & Szczypiorski, K. (2014). Advances in digital media security and right management. *Multimedia Systems*, *20*(2), 102–103.
102. Zhou, L., & Chao, H. C. (2011). Multimedia traffic security architecture for the internet of things. *IEEE Network, 25*(3), 35–40.
103. Joshi, J. B., Shyu, M., Chen, S. C., Aref, W., & Ghafoor, A. (2008). A multimedia-based threat management and information security framework. In *Multimedia technologies: Concepts, methodologies, tools, and applications* (pp. 509–526). IGI Global.
104. Sadek, I., Rehman, S. U., Codjo, J., & Abdulrazak, B. (2019). Privacy and security of IoT based healthcare systems: Concerns, solutions, and recommendations. In *International conference on smart homes and health telematics* (pp. 3–17). Springer, Cham.

Oludare Isaac Abiodun holds a Ph.D. degree in nuclear and radiation physics from the Nigerian Defence Academy, Kaduna. Also, a second Ph.D. in Computer Science, from the Universiti Sains Malaysia, Penang, Malaysia. His research interests include; artificial intelligence, robotics, cybersecurity, digital forensics, nuclear security, terrorism, national security and IoT's security.

Esther Omolara Abiodun has Ph.D. degree in the School of Computer Sciences, Universiti Sains Malaysia. Her research interests include; computer & network security, cyber-security, cryptography, artificial intelligence, natural language processing, network & communication protocol, forensics and IoT security.

Moatsum Alawida received the B.Sc. degree from Mutah University, Jordan, in 2005, and the M.Sc. degree in information systems from the University of Jordan, in 2010. He has a Ph.D. degree with the School of Computer Sciences, Universiti Sains Malaysia. His research interests include chaotic system, chaos-based applications, multimedia security, and cryptography.

Rami S. Alkhawaldeh received the B.S. degree in computer information systems from Yarmouk University, Irbid, Jordan, in 2007, the M.Sc. degree in computer information system from The University of Jordan, Amman, Jordan, in 2010, and the Ph.D. degree in computing science from Glasgow University, U.K., in 2017. From 2010 to 2012, he was a Lecturer with The University of Jordan. Since February 2016, he has been an Assistant Professor with the Computer Information Systems Department, The University of Jordan. His research interests include artificial intelligence, machine learning, information retrieval, VOIP, and wireless networks.

Humaira Arshad is an Assistant Professor in the Department of Computer Sciences & Information Technology at the Islamia University of Bahawalpur, Pakistan. She has a Ph.D. degree in Digital Forensics in the school of Computer Sciences, Universiti Sains Malaysia. Her areas of interest are digital & social media forensics, information security, online social networks, cybersecurity, intrusion detection, reverse engineering, semantic web and IoT security.