THE INTERNET OF THINGS SECURITY: A SURVEY ENCOMPASSING UNEXPLORED AREAS AND NEW INSIGHTS

Abiodun Esther Omolara , Abdullah Alabdulatif ,
Oludare Isaac Abiodun , Moatsum Alawida , Abdulatif Alabdulatif ,
Wafa' Hamdan Alshoura , Humaira Arshad

PII: S0167-4048(21)00318-7
DOI: https://doi.org/10.1016/j.cose.2021.102494
Reference: COSE 102494

To appear in: *Computers & Security*

Received date: 29 May 2021
Revised date: 23 September 2021
Accepted date: 29 September 2021

Please cite this article as: Abiodun Esther Omolara , Abdullah Alabdulatif , Oludare Isaac Abiodun , Moatsum Alawida , Abdulatif Alabdulatif , Wafa' Hamdan Alshoura , Humaira Arshad , THE INTERNET OF THINGS SECURITY: A SURVEY ENCOMPASSING UNEXPLORED AREAS AND NEW INSIGHTS, *Computers & Security* (2021), doi: https://doi.org/10.1016/j.cose.2021.102494

THE INTERNET OF THINGS SECURITY: A SURVEY ENCOMPASSING UNEXPLORED AREAS AND NEW INSIGHTS

Abiodun Esther Omolara[1], Abdullah Alabdulatif[2], Oludare Isaac Abiodun[1,3], Moatsum Alawida[1,4], Abdulatif Alabdulatif[5], Wafa' Hamdan Alshoura[1], Humaira Arshad[6]

Department of Computer Science, University of Abuja, Gwagalada, Nigeria[1,3], Computer Department, College of Sciences and Arts, Qassim University, P.O. Box 53, Al-Rass, Saudi Arabia[2], School of Computer Sciences Universiti Sains Malaysia[1,3], Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi University United Arab Emirates, Department of Computer Science, College of Computer[4], Qassim University, Buraydah, Saudi Arabia[5], The Islamia University of Bhawalpur, Pakistan[6]

Corresponding Author: styleest2011@gmail.com

The cosmic evolution of the Internet of things (IoTs) in par with its realization in all spheres of life undertakings, mandates continuous research pursuits in IoT and its associated components. While the rapid evolution of IoTs has facilitated monumental opportunities for humanity, it has also acted as a catalyst precipitating diverse security issues. Cybercrimes have been on the rise as criminals and hackers continue to take advantage of IoT's security loopholes and vulnerabilities. The enormity of the attacks has not only been damaging to the quality of life, but it poses a disservice and an unquantifiable risk to human safety. Thus, a timely and comprehensive review, analysis and investigation of the security of IoTs is crucial. Through a systematic literature review of over 200 articles, we set out the latest findings and trends to provide new insights into the security of IoTs, taking cognizant of its social, economic, technical and legal implications, which will be beneficial to researchers, manufacturers, individuals, organizations, and governments. Although many studies reviewing the state of IoT exist in the literature, no studies shape the area of its security well. Hence, there is currently no study that provides an in-depth survey of the emerging security concerns of IoT from diverse perspectives and in tandem with the current condition of the global world today. Compared to other related reviews on the security of IoTs, this survey encompasses much more technical angles to the security of IoT. It begins with the review of the concept of IoTs, the assessments of its industrial development trends, revolutionary paradigms and updated security of the IoT. Key challenges in the security of blockchain technology, a recent spike in distributed denial of service (DDoS) attacks due to the COVID-19 pandemic are sensitive areas that have remained untouched by previous review works. Additionally, politics and security of electoral votes, forensic issues in the IoT era and much more are some of the new depths missing in the literature of IoT security. Thus, a huge divide in the total adoption and actualization of IoT in diverse areas of human endeavour. This review formalizes the IoT concept, illuminating deep insights into possible solutions to the heterogeneous nature of IoT's security challenges, emerging issues, gaps, opportunities, foresight, and recommendations.

Keywords: Security & privacy challenges and solutions of the Internet of Things, gaps in IoT research, forensic in the IoT Era, COVID-19 pandemic and IoTs, future development.

1. Introduction

Internet of Things (IoTs) creates an ecosystem of many associated devices communicating over network systems. IoTs can be seen as a collection of visible and intelligent systems with computational and communication ability capable of encapsulating information for the physical world utilization. Due to their ubiquity, the IoT has infiltrated every sphere of human lives. Thus, coining new paradigms like the internet of flying things (IoFT), the internet of everything (IoE), the internet of nano things (IoNT), the internet of medical things (IoMT), the internet of mission-critical things (IoMCT), the industrial internet of things (IIoT) and many others (Abiodun et al., 2021; Zaidi et al., 2020; Srinivasan et al., 2019). As a result, revamping every sector ranging from communications, smart city, smart agriculture, smart industry, environmental pollution monitoring, surveillance, disaster management, object tracking and others.

The pervasiveness, which has brought tremendous benefits to humanity, have triggered a lot of security issues. The IoT's major issue is mostly described with the two keywords ***security*** and ***privacy*** (Stoyanova et al., 2020; Sicari et al., 2020; Kagita et al., 2020; Yang et al., 2017; Razzaq et al., 2017; Maple, 2017; Babar et al., 2010). This problem starts with the IoTs architecture, which provides mini control even with numerous measures of security (Hassija et al., 2019; Weis et al., 2004). This little control makes users to be vulnerable to diverse malicious attacks. Thus, IoT's sophisticated electronic devices provide massive data that might be personal in detail with minimal users' involvement, control or knowledge, leading to privacy concerns.

The IoT's complexity is also a vital issue (Rafique et al., 2020; Konduru & Bharamagoudra, 2017; Jing et al., 2014; Bandyopadhyay & Sen, 2011). IoT systems are complex with regards to their architecture, implementation, maintenance, sustainability, and their utilization of massive enabling technologies. In addition, pliability is a critical IoT issue that needs to be addressed (Chakraborty et al., 2019; Dizdarević et al., 2019; Mukherjee et al., 2018; Frustaci et al., 2017; Weber, 2009).

Most experts are concerned about the IoT system's flexibility in integrating easily and effectively with other systems (Shi et al., 2020; Li et al., 2018; Atzori et al., 2017; Sajid et al., 2016; Da et al., 2014). Users are bothered about finding themselves in various locked or conflicting systems. Furthermore, compliance remains a critical issue of the IoT (Bicaku et al., 2020; Stuurman & Kamara, 2016; Zheng et al., 2011). Similar to other innovation in the business realm which requires compliance with regulations, the heterogeneous nature of IoT's architecture makes standard software compliance between the IoT systems and its interconnected applications to be challenging.

IoT is yet to function well for meaningful utilization of the fourth industrial revolution (i.e. Industry 4.0) due to the unresolved security challenges (Tewari & Gupta, 2020; Sha et al., 2018; Kumar et al., 2019; Heer et al., 2011). Thus, there is a growing consensus that if stakeholders and the government refuse to intervene, the IoT may remain dangerously insecure (O'Hara, 2019). Recently, an attempt to curtail some of the security challenges of IoT was made by the United States of America Senators when they designed a bill to improve IoT's security (Schneier, 2017). The IoT cybersecurity enhancement act 2017 is a modest piece of legislation meant to support the government's buying power to push the market. The legislation directs that any IoT product that the government procure needs to satisfy minimum security standards.

Likewise, vendors need to ensure that IoT devices cannot be patched only, but in an authenticated or certified and timely fashion, without invariable default passwords, and devoid of vulnerabilities. Although this great step of legislation by the USA senators could improve IoT's security considerably, it could add to the current IoT security challenges because many people, organizations, and governments would desire to be connected. IoT security will continue to be a risk via the connected devices and through major designs such as cars, routers, drones, cameras, etc.

Scalability is another huge issue as more and more equipment join the IoT network, raising concerns such as addressing services and data management (Aslanpour et al., 2021; Kouicem et al., 2018; Gamundani, 2015). As many things are connected to the Internet, devices themselves become one of the security problems. Even though IoT devices yield seamless communication between devices and automate objects that saves time and cost, users are still bothered by the level of privacy and security they get.

The accompanying issues of IoT's security have caused numerous havoc to individuals, businesses and the government. According to a study by the Altman Vilandrie & Company, in April of 2017, nearly half of the United States of America (USA) firms using IoTs have experienced cybersecurity breaches, which can cost up to 13% of smaller firms' annual revenues (Moin et al., 2019; Meagher, 2018).

Numerous reports of specific incidents cause trust or confidence challenges for people to fully enjoy and adopt IoT devices' benefit (Sicari et al., 2015; Sadeghi et al., 2015). Reports show that many computers, smart TVs, phones, and cash machines connected to the IoTs were hacked. In 2019, Fox 6 News reported a horrific incident in which unknown attackers breached a couple's Smart Home setup. According to the couple, hackers gained control of their smart home by compromising the connected devices. During the encounter, the attacker spoke to them via a camera in the kitchen while playing disturbing music from the video system and adjusting the room temperature to 90 degrees Fahrenheit by controlling the thermostat (Ashley, 2019).

Multiple reports revealed security flaws in smart bulbs. Hackers can compromise infrared-enabled smart bulbs by sending commands through the bulbs' infrared invisible light to exploit other connected IoT devices on the home network. Furthermore, a smartphone microphone can be used to launch an acoustic side-channel attack. SmartTVs are not left out, as hackers can use the integrated camera and microphone to not only control the owner's unsecured TV for changing channels or volume controls but also to spy on his/her daily movements and conversations. Identity and bank details can be stolen via a Coffee Machine when users shop using their cards. Smart Security Cameras**,** Connected printers, Internet-Connected Gas Station, Smart Speakers, Connected Fax Machines are IoT devices that provide tremendous easy ultra-modern life benefits but are dangerously insecure based on the current state of IoT security (Cisomag, 2020; Hilt et al., 2019; Greenberg, 2019; Khan et al., 2016; San, 2018).   Such occurrences have negatively affected the trust of not only individual consumers but also business organizations.

Another challenge is the weak security associated with low-cost devices and increasing devices that open more avenues to attackers. Different network devices like Ethernet, Wi-Fi, Bluetooth, Cellular Networks, Low-Power-Wide-Area Networks (LPWAN), Long-Term Evolution (LTE), sometimes called 4G LTE, are interconnected. At the same time, each of these options connected brings about a trade-off in bandwidth, power consumption, and connection range. Selecting suitable devices to disseminate information in the cloud exclusively relies on the application requirements of IoTs. The IoT era is accompanied by an easy life, such as using driverless cars and Mars rovers. As days pass by, one will continue to experience IoT seeping into the grassroots levels, like helping people in the agricultural sector, retail businesses, sport, domestic core and security. However, switching from information technology (IT) to IoT is not easy due to the unresolved privacy and security challenges.

Another issue is the requirements for its realization with associated software and applications. The massive implementation of IoT causes different security issues such as securing the devices, ensuring data is secure and securing communication lines to prevent unauthorized access. Moreover, the deployment of IoT in the future, which must uphold smart world green IoT enabled devices, is another significant issue that is yet to be addressed. As a result, securing the IoT has become a public opinion that includes all partners, ranging from the manufacturers of devices to service providers, organizations, clients, and vendors.

The concerns mentioned above and much more are discussed throughout this paper. Hence, this particular paper demonstrates the state of the art of various levels of security of the IoTs by analyzing existing research findings and highlighting some challenges, emerging issues and open research problems.

What distinguishes this study from other review papers is the diversity of information treated, its unique contributions and the novelty of the approach in terms of intersecting the emerging security concerns of IoT from diverse perspectives in tandem with the current condition of the world today. The context of security it explores encompasses a substantial boundary of IoT. Some of the in-depth explorations include, but are not limited to, the concept of IoTs, assessments of industrial development trends, revolutionary paradigms in IoTs, an IoT look-up manual, updated IoT security, security of blockchain technology with respect to IoT, a surge of distributed denial of service (DDoS) attacks resulting from the COVID-19 pandemic, security of electoral votes and digital forensics in the IoT era. All of these sensitive areas are yet to be explored by previous security audits of IoT. In summary, we can enumerate this paper's main contributions and novelty of approach as follows:

Create an understanding of the conceptualization of IoTs: This review describes the concept of IoT. It is beneficial because it can help newcomers in the field to understand the conceptualization and the essential characteristics of IoT terminologies used throughout the paper. Additionally, readers and researchers can gain knowledge of new ideas and development in the IoT infrastructure, devices and applications. Furthermore, this paper simplifies the technical terms used in IoT. It highlights vulnerabilities, experience and addresses security issues to an amateur's understanding of the whole IoT concept.

Assessment of industrial development trends and security of IoTs: The study assesses the safety of industrial development trends from the Industrial revolution phase 1, Industrial revolution phase 2, Industrial revolution phase 3 to Industrial revolution phase 4, which is Industrial 4.0. Previously, the industrial revolution transformed the basic side of the world industry. Likewise, an industrial revolution has transformed the industry globally, such as the current Industrial 4.0, which involves the IoT's innovation. Therefore, as discussed in the paper, this study seeks to assess industrial development trends and IoT's security issues.

An overview of updated security of the IoTs: This paper assembles, examines, evaluates and synthesizes enormous resources of many works concerning the IoT's security with the primary purpose of harmonizing the state of the art in the field. It highlights the efforts of other studies while converging the state-of-the-art in terms of what is attainable today in IoT and its security. Generally, it is an effort to guide users, newcomers, business owners, stakeholders and inform manufacturers and the government on the current state of IoT security. Notably, the urgency required to explore, deploy, navigate, understand new security problems and how they can be addressed. Ignoring emerging threats comes with a high cost and a deterrent to the effective and efficient adoption of the IoT infrastructure. Thus, this study is an update on the security and privacy issue of IoT. The security update from the defence advanced research projects agency (DARPA) was the discovery of a “security shield” for the IoT that is wider than the Internet.

Look-up manual: This study reveals major abstractions of the IoTs, which is paramount in deploying systems. It provides help to IT professionals, students, scholars, management professionals, stakeholders and customers that may need a fundamental knowledge of the IoT concepts. In addition, the researchers, analysts, experts, practitioners, and users exploring the IoT can seek clarity in understanding the aspect of security requirements in the adoption of IoT. Thus, this review can serve as a helpful reference or guide to other people in understanding critical and novel concepts of the IoT.

New insights of IoT compared to other literature reviews: New understandings of IoT security compared to other review papers were highlighted. Most specifically, the security challenges in its architectural design and functionality. IoT networks encounter risks such as illegal access, confidentiality, man-in-the-middle attack, integrity, destruction, eavesdropping, DDoS attacks, virus attack, etc. Hence this work discusses new insights on the security and privacy concerns of the IoT.

Security challenges of the IoTs: The Internet remains a valuable infrastructure and bedrock of the IoT. As much as the Internet is vulnerable to attackers due to insecurity of the entire system, there is a link of security issues that could also affect IoTs (Huda et al. 2018; Yang et al., 2017; Suchitra & Vandana, 2016). This review provides a thorough treatment of the security challenges of IoT.

Distributed denial of service (DDoS) attacks increased on IoTs during the current COVID-19 pandemic: The DDoS attack is a malicious intrusion that disrupts a network or server's trusted and smooth traffic. DDoS intrusion increased significantly during the covid-19 crisis last year and this year 2021. According to recent reports, cyberattacks against healthcare organizations doubled during the pandemic (Muheidat et al., 2020; Sardi et al., 2020; Kamal et al., 2020). There is a spike in cyberattacks, specifically against medical organizations and hospitals (Lallie et al., 2020; Pranggono & Arabo, 2020; Williams et al., 2020). Details on the cause and possible ways of curtailing such attacks are discussed succinctly in this study.

Security issues of blockchain in the IoT: Recently, blockchain innovation has drawn people from a variety of industries, including finance, which is particularly valuable in cryptocurrency, product traceability, healthcare, real estate, intelligent cars, smart homes, and smart cities, among others. This study goes into greater detail about blockchain technology and IoT. As blockchain is currently a hot theme worldwide, the knowledge could serve as a fundamental framework to guide newcomers and interested researchers in the field.

Politics and security of electoral votes in the IoTs Era: This study discusses current trends in politics and the security of electoral votes in the Internet of Things era. This investigation serves as a culmination of the contributions and limitations elucidating novel practices for Smart e-Voting that could further advance the intersection of smart devices of IoT and Politicing.

Forensics in the IoT Era: Digital forensics becomes more complex as computing devices and computer-enabled paradigms proliferate. Hence, posing new challenges to distributed digital data processing, evidence acquisition and much more. Interesting details are given in the dedicated section as part of the contribution of this study.

Advantages and Disadvantages of the IoT: There are many advantages and disadvantages of the IoT. Benefits include saving time, as it minimizes human effort. It also enhances data collection: Moreover, it improves security; currently, if we have a system that things are interconnected, then one can make the system more secure and efficient. Many disadvantages of the IoT include serious security, privacy, over-dependence, complexity, loss of jobs etc. Hence this study discusses how security and privacy issues could be found in both advantages and disadvantages in IoT.

Security Challenge's Solutions: IoT solutions benefit users, manufacturers and facilitate new businesses' generation. It also enhances the entire intelligent communication system. IoT offers solutions that help connected devices manage tasks, analyze diverse opportunities, and communicate information. However, security and privacy issues have limited its safe realization and feasibility as practical solutions in real-world use-case. Hence, technical solutions to security challenges are part of the details explored in this study.

Perspectives and Future Directions of the IoTs: Comprehensive analysis of constraints, trends, security concerns, potential solutions, perspectives and future directions of the IoT are discussed. This study spotlights the research contribution and limitations of other works by delineating new ideas in IoT security and underpinnings work of the future. It described the state of the art levels of security of the IoTs by analyzing different proposals and discovering problems, identifying issues regarding open research, and future development in the IoT system.

Paper Organization

This paper is arranged into various sections. Section 2 presents the review methodology adopted in this study. IoT and its associated components are discussed in section 3. Section 4 highlights and further discusses the security challenges of IoT. Meanwhile, the current security solution to IoT is discussed in Section 5. Diverse areas intersecting IoT alongside other security issues and solutions are detailed in Section 6. Section 7 describes IoT open research issues and opportunities needing urgent investigation. Section 8 showcases recommendations. Section 9 discusses future research perspectives and directions of the IoTs. Finally, Section 10 presented the conclusion based on the new findings and research requirements that can improve the security of the IoT.

2. Review Methodology

This study dissects the current status of the IoT by investigating the literature on its security requirements, architecture, methodology, applications, findings and more. Reviewed works of literature were extracted from large resources and databases of published papers from popular journals, books, conferences and proceedings, thesis, symposiums, edited volumes, magazines, gray literature, and preprints. In addition, relevant organization's publications, government, and lecture notes, amongst others, were explored.

The extant literature was identified by searching using terms like "Security of Things", "Internet of Things", "Security Challenges of the Internet of Things", "Forensic in the IoT Era". Other keywords used are; "Security and privacy challenges in the IoT", "Solutions to IoT security and privacy challenges", "Weakness of IoT "Security and privacy challenges in the IoT", and "Vulnerabilities in the IoT". Additional keywords used include; "Problems and Solutions to the IoT's Security", "Prospect of IoT and Security", "Perspective of the IoT", and "Future of the IoT". The output papers were downloaded, examined, synthesized, analyzed, critiqued and collated. The reputable scholarly databases searched include:

→ ACM Digital Library,
→ IEEE Xplore,
→ Scopus,
→ Elsevier,
→ Springer,
→ EBSCO Host,
→ Taylor and Francis,
→ World of Science (WoS)
→ PubMed,
→ Wiley
→ Google Scholar and
→ Others

In summary, about 200 articles were used for the study. The articles processed is presented in Tabular form as depicted in Table 1.

Table 1: Summary of the number of articles processed in the review

Indexer	**Results**	**Profiteered**	**Relevant**
IEEE Xplore	119	18	65
ACM Digital Library	35	13	18
Scopus	30	16	10
Elsevier	65	24	32
Springer Link	23	10	13
EBSCO Host	24	9	14
Taylor and Francis	20	8	9
World of Science (WoS)	22	7	11
PubMed	19	5	9
Wiley	10	3	4
Compendex	10	4	5
Google Scholar	10	3	5
Others	10	2	5
Total	**397**	**122**	**200**

Thus, Table 1 presents articles processed for the study. Generally, 200 relevant articles were used for the survey.

The methodology of the study began from the goal and analysis of current works published regarding IoT. Many aspects considered include IoT security requirements, existing security solutions, IoT security challenges, security issues and solutions, research gaps, open research issues and opportunities, future works, and conclusions. The research methodology adopted in this review is represented in Figure 1.

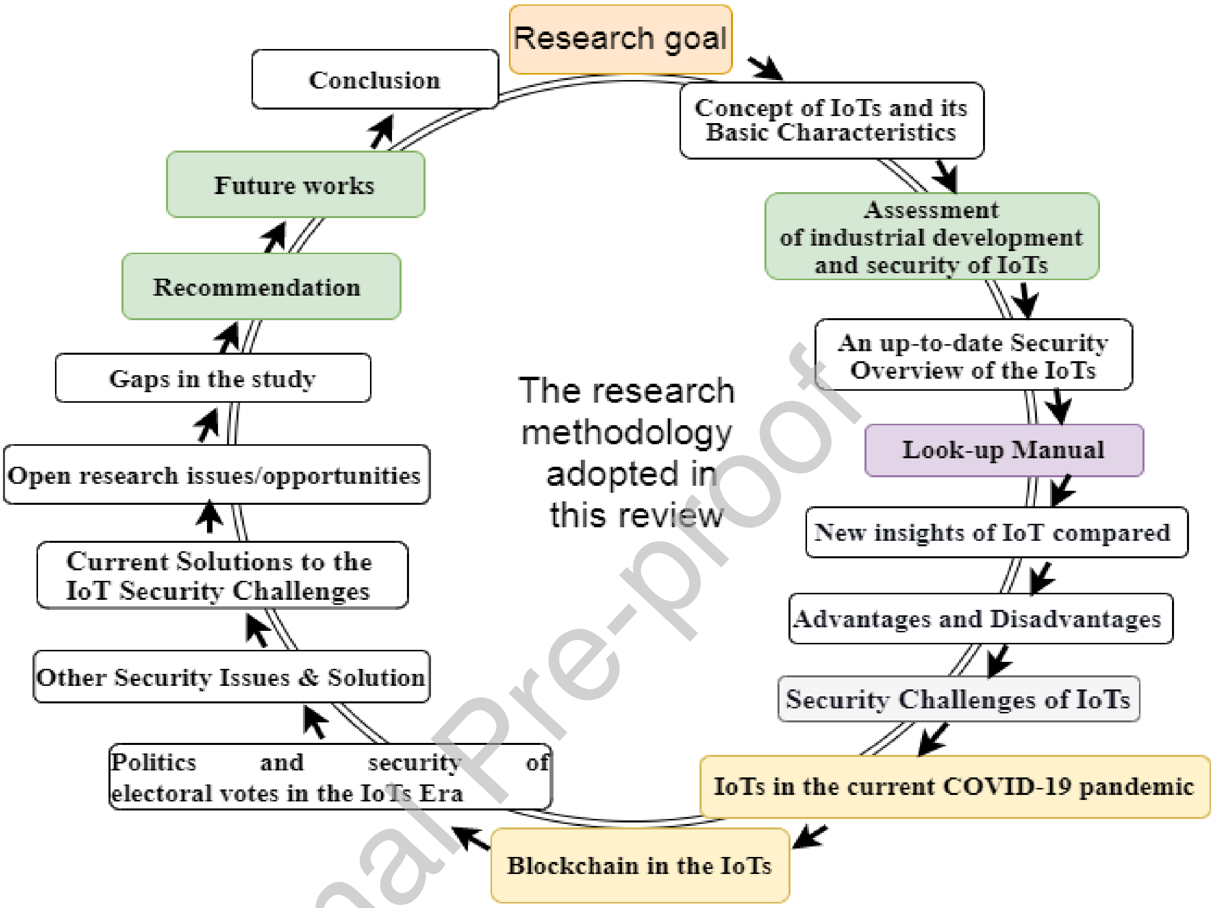
Research goal
Concept of IoTs and its Basic Characteristics
Assessment of industrial development and security of IoTs
An up-to-date Security Overview of the IoTs
Look-up Manual
New insights of IoT compared
Advantages and Disadvantages
Security Challenges of IoTs
IoTs in the current COVID-19 pandemic
Blockchain in the IoTs
Politics and security of electoral votes in the IoTs Era
Other Security Issues & Solution
Current Solutions to the IoT Security Challenges
Open research issues/opportunities
Gaps in the study
Recommendation
Future works
Conclusion
The research methodology adopted in this review

Figure 1. The research methodology adopted in this review

3. The Internet of Things and its Associated Components

(i). The Concept of IoTs and its Basic Characteristics:

The concept of IoTs outlines the connection of visible devices, “things” implanted with sensors, software, and technologies for communication and exchange of data together with other objects on the Internet. Whereas heterogeneity in the IoTs is the main characteristic that causes insecurity. Systems on the IoTs is made up of diverse networks of hardware and software which interact with other systems by separate networks. The IoT design needs to aid face to face network interconnectivity among heterogeneous systems. An overview of the IoT is represented in Figure 2.

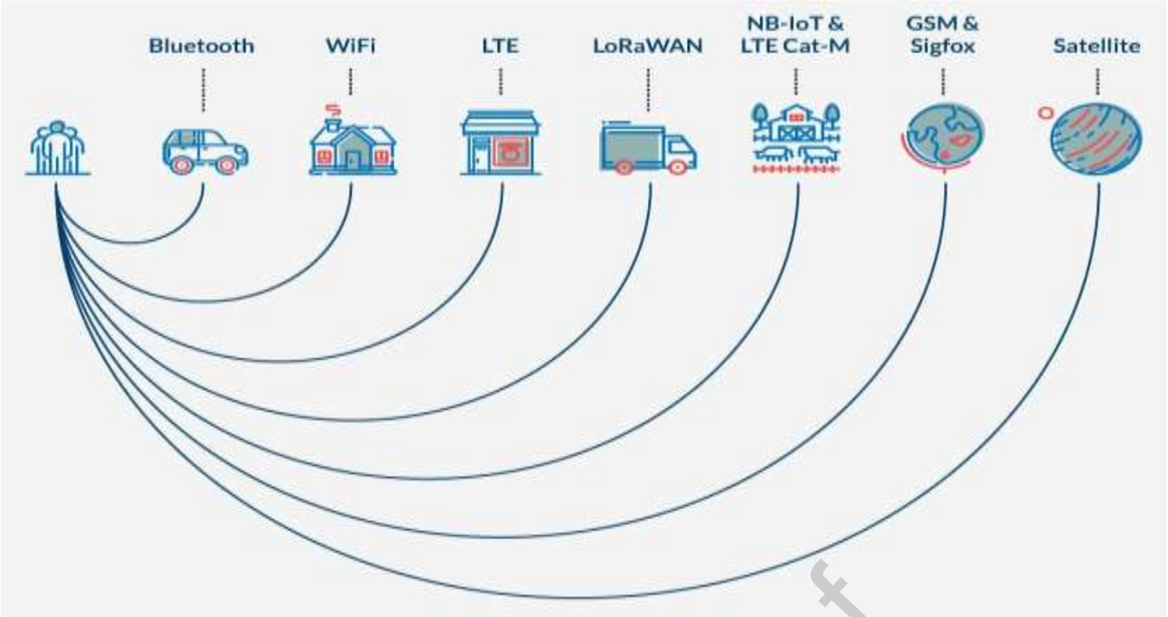

Figure 2. IoTs overview

Figure 2 illustrates an overview of the IoTs, which describes the connected devices' association with man, as the benefactor.

IoT has three essential characteristics: comprehensive awareness (consisting of sensors), M2M terminal, and RFID. The aforementioned attributes are used to get information about the object and also a dependable transmission. The purpose of the dependable transmission is to achieve high accuracy at minimum time. It has smart processing; the central objective which is to collect useful information that can be analyzed to meet users' expectations. Hence, this review first seeks to understand the concept and fundamental characteristics of IoT's security and privacy issues.

(ii). Assessing industrial development and security

The digital revolution can be viewed from the perspective of the world’s industrial development phases. It began from the Industrial revolution phase one, Industrial 1.0, up to Industrial revolution phase four, which is Industrial 4.0. The evolution of the phases of the industrial revolution transformed the industry development in the whole world. Recently, Industrial revolution phase 4 came into existence, and today machines can interact with themselves in the production process even on a large scale. Interestingly, machines and computers can be integrated to communicate together alongside intelligent connections, permitting rational, intelligent decisions. This era of intelligent connection of machine-to-another machine, and also, machine-to-man, even connection of machines to animals is unique in this IoT’s world. The Industrial revolution phase 4 enables expeditious and innovative transformations in virtually all aspects of life. Some of the transformations involve enhancing customers' experience using a product, increasing marketing, and minimising costs.

Industry 4.0 practices are spreading to various science and technology domains, including big data in healthcare. As such, the physical and the virtual worlds are interconnecting over the planet. The Internet of Things and cyber-physical systems (CPSs) have rapidly enabled the movement of Industry 4.0. The prospects of Industry 4.0 brings about the possibilities of billions of people interconnected by mobile devices, with high-speed processing power, unlimited storage capacity, and access to knowledge. This interconnectivity will be multiplied by successfully incorporating emerging technology such as nanotechnology, artificial intelligence (AI), 3D printing, robotics, biotechnology, and autonomous vehicles into the IoT.

Likewise, the connection will be multiplied in medical science, energy storage, quantum computing, materials science, sport, agriculture, commerce, education, engineering, and so on. The next Industrial 5.0 revolution will be marked with the customization of the cyber-physical cognitive system. Nevertheless, security challenges remain a big issue as all these things are customized, and cyber-physical cognitive system emerges in the nearest future. The industrial development phases are presented in Figure 3.

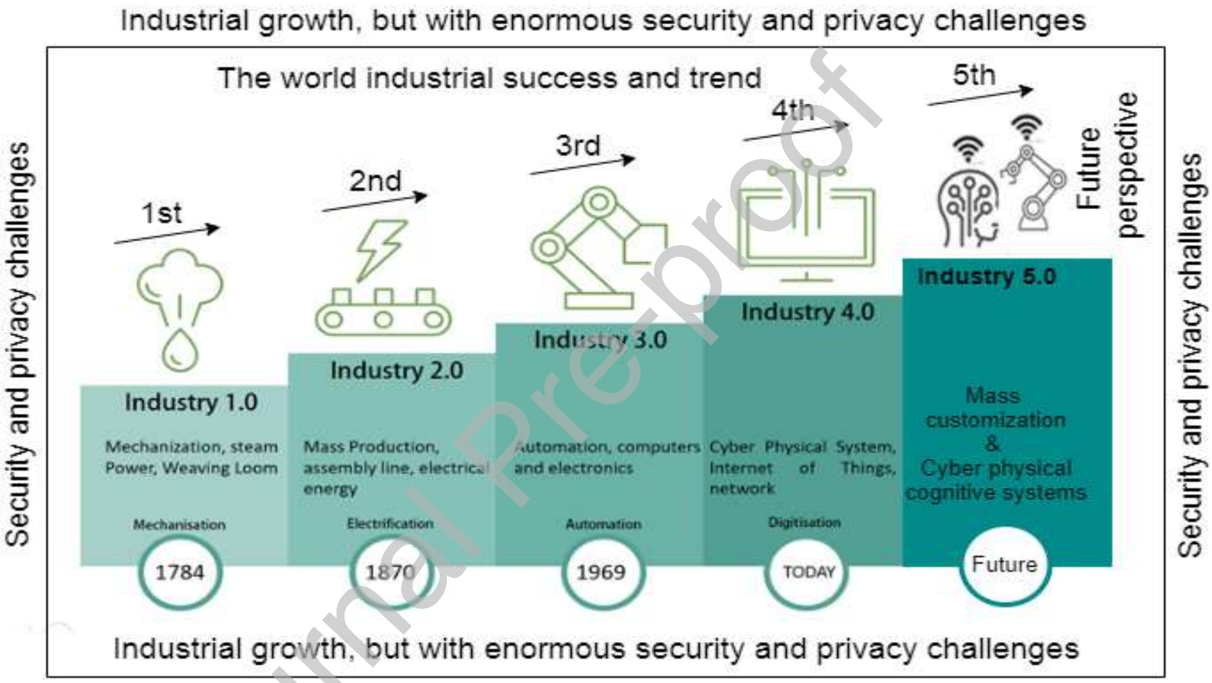
Industrial growth, but with enormous security and privacy challenges
The world industrial success and trend
Security and privacy challenges
1st
2nd
3rd
4th
5th
Future perspective
Industry 1.0
Mechanization, steam Power, Weaving Loom
Mechanisation
1784
Industry 2.0
Mass Production, assembly line, electrical energy
Electrification
1870
Industry 3.0
Automation, computers and electronics
Automation
1969
Industry 4.0
Cyber Physical System, Internet of Things, network
Digitisation
TODAY
Industry 5.0
Mass customization & Cyber physical cognitive systems
Future
Security and privacy challenges
Industrial growth, but with enormous security and privacy challenges

Figure 3. The World Industrial Development Phases

Figure 3 highlights the growths and phases with regards to industrial development that started between Industry 1.0 and Industry 4.0 revolution.

The IoT revolution is helping the emergence of new industries and technologies; no wonder there are billions of heterogeneous devices, gadgets, objects, systems, and items in the markets. This revolution brings novel business models. Other new terms associated with Industry 4.0 are the IoT, big data analytics, cyber-physical system, artificial intelligence, cryptocurrency (blockchain), three-dimensional (3D) printing, cloud computing, etc. Therefore, this subsection ends with discussions on the advantages and disadvantages regarding IoT, which includes;

(a) The IoT Advantages:

(i) Enabling easy access to information: One could comfortably access data which is a distance away in real time. Data access is easy due to a network of connected objects; one gets whatever data at any place in the world. Access to data anytime and anywhere brings convenience for everyone performing their work with available data, without necessarily physically being present at the location.

(ii) Ensuring faster communication: It is possible to maintain faster and better communication across a network of connected technologies, ensuring transparent systems to reduce inefficiency. That is, the mechanism for machines to communicate is more efficient with faster output. A typical scenario is a piece of machinery put in place at a production or manufacturing plant.

(iii) Ensuring information sharing: It ensures effective information sharing between systems and users across a network. Information sharing is a secure way of monitoring the connected devices to ascertain that they are in good condition. The mechanism for machines to communicate and share information between devices and users is more efficient with high-speed output.

(iv) It minimises cost: The IoT system provides an opportunity for cost-effectiveness. Accessible communication and data sharing between objects are smooth with lower financial cost implications. Dissemination of data packets across a network can reduce time and money. Likewise, similar data that may take time to be transferred could be achieved at high speed with the revolution of the IoT.

(v) It provides automation: Automation uses machines to manage everyday tasks with little or no human interference. Machines used during business operations assist in improving services and minimizing errors made by people.

(b) The IoT Disadvantages:

Aside from some of the major concerns accompanying the Internet of Things, ranging from the breach of security, privacy, over-reliance on technology, complexity, to the loss of jobs; other critical disadvantages are described as follows;

(i) Problem securing objects – The IoT brings about successful connection and communication, allowing helpful information sharing between objects and people. Regrettably, this advantage comes with the problem of securing the objects.

(ii) Longevity of device life and expired support – Although IoT devices could have a long life service, notwithstanding, the long life of devices might outlive support. This is unlike the conventional devices that usually provide upgrades and support for a long time, even when they are no longer in use. Obsolete devices and abandoned wares do not possess the same security features as new devices because of technology evolution and improvement over time.

(iii) No room for upgrading devices – Most IoT devices such as small devices and mobiles are not manufactured to support upgrades. Therefore, the devices cannot be upgraded to support new technology or functionality on the platform of IoTs. Moreover, some old devices offer complicated upgrades that most users may not notice or ignore due to the complexity required for upgrading the device.

(iv) Transparency problem – Most IoT objects do not enable visualization of operations. There is no transparency during function, making it impossible for users to see processes.

Thus, one cannot tell about how devices work. Likewise, users do not have control of data collection or undesirable operations. More also, as the manufacturer is in charge of updating the device, it might lead to more undesirable operations from the users' side.

(v) Lack of alerts –IoT can provide remarkable operation without obstruction. However, such benefits are enjoyed at the expense of the users' unawareness, as they may be unable to monitor devices to know if anything goes wrong. As a result, security challenges may go undetected for an extended period.

4. Security Challenges of IoTs

Security, as well as privacy challenges, are the common issues of ubiquitous computing. As data security continues to affect IoT devices and cloud platforms, serious privacy concerns remain. These concerns remain as there is a tremendous continuous increase in the number of connected devices to the Internet (Doshi Song et al., 2018; Song et al., 2014; Emmerson, 2010). In 2015, a little over 15 billion devices were found on the Internet. It later increased to 23 billion connections in the year 2018. As of 2020, it has become 25 billion. Thus, access to the Internet has expanded and confidentiality in the IoT is indeed a global issue mandating a timely exploration.

Indeed, the IoT is changing the world, for instance, from how one drives a vehicle to how one does business, carries out purchases, and gets energy for home activities. Advanced sensors could detect environmental changes and respond to the output of other devices. Sensors and chips are implanted in the IoTs, and each transmits data. The transmitted data help one understand how devices work and how they function together. Notwithstanding, not everything is perfect in the world of IoT. The data exchange over the Internet comes with security issues such as:

1. Insecure Web Interfaces: Insecure web interfaces such as weak passwords, poor network services, unsafe ecosystem interfaces, and unprotected update mechanisms. In addition to the obsolete devices, other issues are weak privacy protection, unprotected data transfer, unsafe storage and improper management of devices.

2. Insufficient Authentication/Authorization: Authentication is the recognition of identity with required credentials. However, insufficient identification may lead to the vulnerability of devices on the IoT. Meanwhile, authorization means enabling consent on actions to entities, such as granting permission to users, devices, or applications. Therefore, when there is insufficient authorization, it can also lead to the vulnerability of the IoT's system. Previously, the work by Shahzad & Singh (2017) stressed the need for ceaseless authentication and authorization of the IoTs. Current practice helps authenticate an entity only if a period is ascertained, then keep it validated until the period or session is closed, or some timeout occurs. A study by Shone et al. (2015) suggested advanced authentication methods to improve current approaches. Most of the conventional techniques are deficient or were not structured to be used frequently. Passwords can be used, but people are reluctant to memorize unique or lengthy ones, so they usually stick to a particular password by reusing it.

3. Insecure network services: Allowing default login passwords and credentials of the devices to remain online exposes and invites malicious intrusion. That is, the exposure of multiple layers such as hardware, applications, and data without adequate protection could invite malicious attackers to any of the open ports at any time. The security challenges of the

IoT materials depend majorly on the manufacturers that do not manufacture material of high-quality standard. Likewise, security challenges partly fall on users that ignore utilizing the available security feature.

4. Lack of transport encryption: Unencrypted data is noticed or viewed as it travels over local networks or the internet. This plaintext viewing situation of data flow serves as a threat agent to the network device connected, serving as an attack against the network devices from internal or external users.

5. Privacy concerns with the stored data: The data stored on IoT are easily viewed or accessed by anyone on the network because of privacy challenges. IoT envisions everything in the physical world connection and real-time data. Also, stored data need to be in the dual active clustering mode.

6. Insecure cloud interfaces: Cloud of the IoT (CIoT) and Cloud of Things (CoT) ideas introduces confidentiality, security challenges, configurability, software/firmware and inadequate physical security problem. Most devices are interconnected over the Internet via web-based interfaces that are not secure. Cloud services are critical to IoT devices. It promotes data exchange between devices of the IoT and related mobile or including applications. It is important to secure cloud interfaces; otherwise, it might lead to a huge loss of data and attackers may use the loophole to maliciously control every device in the cloud.

7. Unprotected mobile interfaces and networks: There are two techniques for controlling or administering IoT objects. One technique is by a web interface, and another, by a mobile interface, via an application on a Windows operating system (OS), Android, or iOS. Similar to web interfaces, mobile interfaces should possess solid identification and permission tools. When intruders try to access devices of the IoT, he/she can take over the IoT devices, then manipulate processes, disconnect the electrical power supply, and consequently shut down supporting networks.

8. Security Configurability Problem: Most objects have configurable security problems. One could decide characters' requirements for authentication of passwords.

9. Software and Firmware Issue: Some systems do firmware updates at restart points or at time intervals via unsafe network protocols such as trivial file transfer protocol (TFTP). TFTP is a simple lockstep mechanism that enables a client to get a file from a remote host or put a file to a remote host. Unfortunately, TFTP may not be encrypted or may lack a robust verification protocol. Thus, making it vulnerable to network attacks such as man-in-the-middle attacks. When a remote intruder can discover firmware updates to exploit the network systems, it can embark on a modification attack to perform his/her malicious objectives. If modification is successful, the update of the network can be obtained to achieve control. Assuming the device network is a hub that communicates with other IoT devices, the intruder may likewise take over those devices. These man-in-the-middle attacks are usually performed in the local area network (LAN). Nevertheless, it is possible to execute a malicious update through a wide area network (WAN), such as the Internet-based attacks similar to domain name server (DNS) hijacking. A typical DNS hijacking is represented in Figure 4.

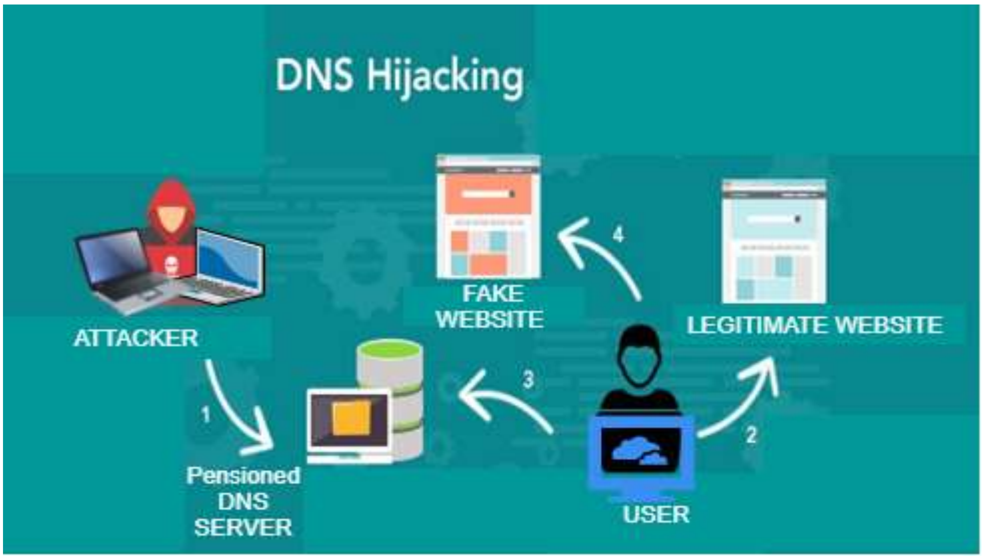

Figure 4. An illustration of DNS hijacking

Figure 4 demonstrate the working strategies of DNS hijacking in a real-world scenario. Notably, the Internet should give the device the ability to do security updates. However, if the device cannot update itself, it may not restrict remote accessibility and attack. DNS is utilized to connect user domain names to commensurable Internet protocol addresses. Usually, the computer uses a DNS from an internet service provider (ISP). DNS belong to the ISP or other private business party. Some DNS services are provided by popular firms such as GoDaddy and Google.

However, they may not guarantee safety as hackers can gain access to the computer network and change the setting of DNS. When this happens, the computer will use an untrusted DNS server. Thus, when a user types a specific uniform resource locator (URL), it will link to a counterfeit website. DNS altering Trojans can be utilized unknowingly to change automatic DNS servers to manual fake DNS servers from a trusted ISP. DNS servers for routers may be modified by capitalising on the weakness of the firmware from a remote location.

10. Physical Security Problem: When IoTs are easily compromised, they destroy the ownership of devices. Although, devices of the IoT have great potential to make lives easier and beautiful. Notwithstanding, if the security challenges are not considered and addressed, the connected devices could lead to devastating trouble than they are worth.

4.1 Access and Confidentiality in the IoT

Nowadays, many technologies and underlying IoT networks, such as wireless sensor networks (WSN), near field communication (NFC) and radio frequency identification (RFID), provides great benefit. However, they also present a significant set of challenges.

(i) The RFID technology- RFID systems consist of one or more readers and many tags (labels attached for identification purposes and to provide information). These readers and tags assist the automatic recognition of things connected to it and enable devices to be designated with special recognition. Tags usually are inactive; that is, it does not require a power supply on board. However, it is powered through batteries. RFID technology is part of the IoT networks that ensure that IoT gadgets are fortified with smart tags and identifiers that coordinate and manage them. Likewise, RFID technology provides IoT gadgets with intelligent chips that help them sense information in their surroundings. It can then have the ability to transmit with gadgets or human beings identified in the IoT platform.

The RFID is liable to scanning, DDoS, relay, side-channel attacks and eavesdropping (Omolara et al., 2019), which could maliciously affect the network of IoT (Khattab et al., 2017; Rehman et al., 2016; El Mouaatamid et al., 2016; Halevi et al., 2012; Mitrokotsa et al., 2010). Therefore, the IoT builds on the pervasiveness of bringing many things into use, such as sensors, RFID tags, actuators, and mobile phones capable of interacting with each other and working with other services to achieve a common goal. Meanwhile, some authentication protocols for RFID tags to secure IoT devices are presented in terms of authors, description, novelty and shortcomings in Table 2.

Table 2: Security techniques of RFID

References	Research description	Research Novelty	Research limitations
Maarof et al. 2018; He, & Zeadally, 2014; Chen et al. 2011	An authentication design to secure IoT application.	The server executive needs a single decryption to get actual tags identity without requiring any linear search. Likewise, it can generate a random number.	The scheme does not ensure privacy; thus, unsafe for countering traceability intrusion because the intruders might exploit the tag's location. Likewise, it suffers from forgery and repeated attacks.
Yeh et al. 2010	RFID networks security match electronic product code category 1 creation 2 benchmark.	Able to detect denial of service intrusion. It also efficiently improves general execution.	Inability to defend impersonation attack on the server and data integrity check due to server data transmission in a coding manner.
Cho et al. 2011	Security to counter brute-force intrusion by Hash-based protocol for verification.	Permit continuous modelling of different reply text excluding intercession through deliberate or vain requests created by the attacker, and same time secret parameter not communicated directly.	Inability to defend an attack by resynchronization, label and reader fraud.
Burmester-Munilla 2006	Authenticating server and tag by trade-off 3 or 5 successive numbers from the pseudorandom number generators (PRNG)	Prevent session from connecting, forwarding and backwards security. Each tag shares a synchronized PRNG with the server.	Effective and efficient performance problems as the PRNG requires refreshing, especially when it is suspected that PRNG might be breached.
Liao and Hsiao’s 2013	Elliptic curve cryptosystem based RFID validation paradigm and identity verifier transfer protocol to achieve mutual authentication	It reduces time complexity.	Vulnerable to both masquerade and tag attacks. Also prone to server spoofing attacks. More also, it is susceptible to location tracking attacks. Furthermore, users may be victims of label cloning intrusion.
Chou’s protocol 2014	An Elliptic curve cryptosystem based on RFID validation protocol by random and prime numbers	It has little calculation difficulty, and all the texts can communicate by the hash operation because the	It has tag data privacy issues, including backward and forward traceability problems.

		passageway can be regarded as unsafe.	
Yang et al. 2012; Avoine et al. 2011, Tu et al. 2007	A validation scheme for period incorporated protocol via smart card.	It provides a password key compatibility, allowing the user to modify the password if there is any malicious activity.	It is vulnerable to impersonation attacks.

(ii) Wireless Sensor Network (WSN): WSN is an essential IoT module that gathers environmental data and transmits it to the central server for implementation. It aids remote detection of applications and collect data from the IoT devices due to their effectiveness and efficiency. It has a low power consumption rate with high computational intelligence and data processing abilities. Furthermore, WSNs are affordable, as they are not so expensive in the market. However, they are vulnerable to threats, wormholes, ICMP, ping flood, flood, neighbour discovery, and syn flood attacks.

In contrast to the regular WSN, the IoT based WSN is more sophisticated and intelligent (Alavi et al., 2018; Din et al., 2018; Zhong et al., 2018). IoT-based WSN implements typical tasks by gathering data from the environment and performs significant operations with the slightest human connection. Also, administering heterogeneity of IoT sensing devices leads to numerous challenges concerning economic utilization and processing. Thus, intelligent algorithms are necessary to enable elasticity in the process of dynamic IoT devices.

(iii) Near Field Communication (NFC)- NFC is one of IoT's core technologies that aids communication in the distance using low power required for the transmission by access control and smart cards. NFC is susceptible to many kinds of attacks such as a relay, phishing, data forging attacks, and user tracking (O'Gorman, 2017; Haselsteiner & Breitfuß, 2006).

(iv) Authentication – It involves confirming that data requests come from a legitimate place and that the information is supplied by an actual user.
(v) **Authorization**- It means granting access to the user that is assumed to be the right owner after authentication is ensured.

4.2 Distributed denial of service (DDoS) attacks increased on IoTs during the current COVID-19 pandemic

A DDoS attack is a malicious intrusion that disrupts a network or server's trusted and smooth traffic. The attack could overwhelm the target network, server or its surrounding infrastructure with congested traffic, which could provide an opportunity for further damage. Unlike other cyberattacks, DDoS attacks aim to bombard an organization's defence mechanisms with a vast wave of service requests from numerous sources. The decentralized and complex nature of the attack makes it difficult to defend against, as the victim cannot simply block requests from one source.

DDoS attacks continued to increase during the covid-19 crisis last year and this year 2021. As the pandemic accelerated the transition to the internet for almost every human's endeavours, ranging from education, healthcare to consumer shopping and office work, intruders gained access to more targets than ever before. Many organizations struggle to support the remote workforce during the current lock-down and work-from-home period (Cviti et al., 2021;

Lallie et al., 2021; Chigada et al., 2021; Evans, 2021; Pecchia et al., 2020). Attackers are taking advantage of the lockdown period by distracting people from their work. Network administrators and cyber-experts are unable to protect their systems owing to the difficulty of maintaining best security methodologies and practices in the emergency that the world has found itself (Babur, 2021). Experts and users are less concerned about their organization's network functionality because they are forced to deal with prevalent health issues. Employees pay less attention to organizational activities, allowing attackers to exploit vulnerabilities. As a result, cybercriminals have evolved in their methods, and their base of attacks has been expanded. They take advantage of their idle time and the hard times the world faces to create new tools and techniques for breaking into their target organization's network. Simultaneously, the ongoing rollout of 5G technologies has expedited the proliferation of IoT and smart devices globally, allowing botnet attackers to launch massive attacks on unsuspecting users.

A Comcast finding showed that the average number of households affected could be up to 104 threats monthly (Krishnamurthy et al., 2020). The most vulnerable devices affected are desktop computers, laptops, servers, smartphones, network cameras, digital storage systems, tablets, and streaming video objects (Lallie et al., 2020; Buil-Gil et al., 2020; Singh Lallie et al., 2020). These vulnerable devices cause attackers to exploit vulnerabilities and launch more attacks on IoT, especially during this current covid-19 crisis. Amazon Web Services (AWS) reported the largest DDoS attack at 2.3 terabits per second (Tbps) in the first quarter of 2020. Google disclosed details of a much larger DDoS attack, which reached its peak at 2.5 Tbps (Babur, 2021).

More also, according to recent reports, cyberattacks against healthcare organizations doubled during the pandemic (Muheidat et al., 2020; Sardi et al., 2020; Kamal et al., 2020; Lallie et al., 2020; Pranggono & Arabo, 2020; Williams et al., 2020). Several variants of DDoS attacks, including the Mirai botnet attack, remains a challenge for secure and seamless deployment of IoT and its associated components.

Preparation is critical for envisioning variants of regular and seasonal attack vectors, particularly complex multi-vector DDoS attacks. More exploration is needed on developing intelligent, proactive measures with less human interaction in emergency scenarios. Currently, there is a trade-off between dealing with two critical issues, a potential health challenge and a serious network attack. Developing an intelligent, proactive defence system can help address such loopholes. Thus, it will be beneficial for cases like this when humans have other life-threatening issues to attend to and cannot be bothered by another severe matter. Furthermore, a piece of up-to-date information on DDoS attackers' tactics that could jeopardize user's experience and brand must be made readily available.

There is also an urgency to identify new tools and tactics DDoS attackers use on IoTs during this COVID-19 pandemic.

4.3 Other Issues Plaguing IoT Security and Research Gaps

Other security issues that have limited the optimal use of IoT are:

- Unforeseeable Malicious Behaviour – The behaviour of a large number of objects are uncertain. A particular object might have been securely designed and well managed but may not interact with other systems.

- IoT Objects Similarity – IoT objects are relatively similar with the same connected technologies. If a particular technology is compromised, others could be affected.

- Problem Encountered in the IoT Deployment –One goal of the IoT is to let modern networks analytics achieve more success from their current stage. Regrettably, this creates the issue of physically ensuring the safety of the IoT devices.

- Longevity Life of Device and Expired Support –longevity of the life of IoT devices is a great benefit. Notwithstanding, the longevity of device support may outlive their normal life. Therefore, research is required to enable the detection of expired devices to create awareness to users that they are no longer usable.

- Devices Without Upgrade Support – Most IoT objects, such as mobile devices, were not meant for modifications and upgrades. Some devices provide tedious upgrades, which most users refuse to comply with.

- Lack of Transparency in Task Execution – Most IoT objects does not enable transparency concerning functionality. Thus, making it impossible for users to note or access their service delivery. Meanwhile, some devices do not have control over data gathering and un-useful products. Unfortunately, if the manufacturer updates a device, it might lead to other un-useful products.

- No Security Alerts Over Intrusion into the IoT Objects – IoT provides remarkable tasks without obstruction, which may lead to the problem of user's unawareness of specific issues. Infringement can be prolonged without been detected. Hence, more research is needed on creating alerts to enable users to be aware of impending intruders.

- Challenges of IoT development – This includes object interoperability, identification, mobility, addressing, energy efficiency, massive scaling, management, etc.

4.4 Other threats to IoTs are Malware, Passive wiretapping, Zero-day exploits

Aside from the denial of service threats to IoTs, malware attacks are another major threats to IoT. It became sophisticated as vulnerable kits and materials are shared over Web platforms and Dark Web. Passive wiretapping is also another challenge that measures or analyzes traffic and disseminate messages. The eavesdropper analyzes the traffic, finds the location, discovers transmitting hosts, and monitors the length and frequency of exchanged texts. Likewise, Zero-day exploits are cyber-attacks on IoTs that target software weakness that may be unknown to both software and antivirus vendors. Such exploits are likely to succeed as there is no protection available, thus making zero-day vulnerability a dangerous threat on IoT devices.

4.5 Blockchain Technology Security Issues

In recent years, blockchain innovation has attracted people across various industrial settings, thus, creating immense opportunities in cryptocurrencies, product traceability, health, real estate, smart cars, smart homes, smart cities, and so forth (Reyna et al., 2018; Zheng et al., 2018). The industrialization of blockchain help its adoption in various application contexts and, now, in the IoTs.

Major security issues of blockchain innovation are standardization, managing of distributed databases or ledgers and data synchronization. Standardization is an essential issue in executing the innovation of blockchain via the IoTs (Saberi et al., 2019; Vasilomanolakis et al., 2015; Mills et al., 2016).

Standards play a significant role in ensuring interoperability, efficiency and security. Standards for interconnected things entail device confidentiality, integrity, authorization, authenticity, and availability (Vasilomanolakis et al., 2015; Sompolinsky & Zohar, 2015). Importantly, object confidentiality needs to be provided to prevent leakage of data on the IoT. Nevertheless, ensuring protection for each layer of IoT might compound complexity. New privacy enhanced technologies need to be designed specially to achieve aims like transport layer security (TLS), internet protocol security (IPSec), and virtual private networks (VPN). IPsec or IP security refers to a safe network protocol that validates and converts data packets to ensure secure encrypted transmission between two computers across the IP network.

Another key blockchain innovation security issue is the administration of shared databases such as ledgers. The task of ledgers involves keeping data of connected objects with the expeditious increase in datasets. This increase in the datasets occurs by global connectivity of shared ledgers. As a result, there are no tangible security plans in the blockchain scale concerning various heterogeneous systems. The heterogeneity of systems can lead to some critical security challenges in this present time. For instance, using some software with poorly designed security features for different data. Poorly designed security features are vulnerable to malware or backdoor installation (Zhu et al., 2010). Significantly, heterogeneity cause compatibility issues. Compatibility is required to maintain data integrity.

Likewise, data synchronization has become a time delay challenge in the blockchain due to the complexity in identifying, storing, and calculating enormous datasets' header-header. Therefore, there is a need for well-defined smart contrasts to tackle data synchronization time-consuming issues. Likewise, a valid agreement needs to provide anonymity by an express increase in the blockchain system. Therefore, talented software developers need to find innovation to tackle challenges of system speed that grow fast because of the shared ledger regarding the IoTs blockchain technology.

4.6 Politics and security of votes in the IoTs Era

Many countries have witnessed political election processes with massive security flaws over the years. An example is the South Wales state election, which was cast online in Australia, with 280,000 votes marked with massive security flaws (Cortier et al., 2019; Kremer & Rønne, 2016). Although e-voting is safe, convenient for voters, and helps to check vote duplications, IoT technologies unveil avenues for attackers to gain access illegally.

e-Voting is one of the real-life applications of blockchain. The e-voting system is liable to confidential credentials exploit on the IoTs because many devices are interconnected without maximum protection. Therefore, it is an issue in blockchain to ensure transparency and reliability of elections (Swan, 2015). The trust needs to continue by the electoral agency, like setting third party access to voters' credentials and the chance of vote cast (Abbasi & Khan, 2017). However, if the confidential data is in each node, one will not access the entire credentials. Blockchain security of the distribution nodes is a major challenge in politics.

However, innovative techniques of real-time tracking, democratic partnership of electoral agencies and government need to be used to prevent unauthorized intruders and security risks in digital politics. It is difficult to hack into voting systems except through internet-connected objects to attack political information sites, prevent people from casting votes, or exploit the confidential personal data these IoT devices capture to manipulate voters. Therefore, there is a need to study how IoT intruders should be monitored, detected, or prevented from tampering with political votes.

4.7 Forensic in the IoT Era

Forensics and the rule of law practices of IoT focus on locating, obtaining, and analyzing digital evidence from IoT devices for legal or investigative purposes. Digital evidence is information that has been stored or transmitted in binary form and can be used in court. It can be found on a computer hard drive, as well as a mobile phone. Electronic crime, or e-crime, such as credit card fraud and child pornography, is frequently associated with digital evidence. Digital forensics becomes more complex as smart devices and computer-enabled paradigms proliferate. According to an official survey conducted by The Office for National Statistics, there were an estimated 3.6 million cases of fraud and two million computer misuse offences each year (MacDermott et al., 2018; BBC, 2017).

IoT data could be a rich source of evidence. However, forensics professionals must deal with a wide range of issues ranging from the vast array of IoT devices, non-standard formats to the multi-tenant cloud infrastructure and the resulting multi-jurisdictional litigation (Stoyanova et al. 2020). There is also the issue of end-to-end encryption, which represents a trade-off between the right of users to privacy and the success of the forensics investigation. Furthermore, there are challenges for IoT-based forensic investigations, such as the growing number of objects of forensic interest, the relevance of identified and collected devices, blurry network boundaries, and edgeless networks.

Another challenge is the dramatic increase in the volume of digital evidence, as well as the development of new technologies that make digital evidence more difficult to obtain. As a result, it is challenging for digital crime investigators to locate sophisticated users who commit illegal acts on the Internet while concealing their identities. Similarly, challenges are arising from the need for close coordination among law enforcement agencies, as well as the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases.

The combination of cloud-native forensics and client-side forensics (i.e. forensics for associated devices) can allow researchers to study and develop the ontology to support practical digital examinations and address emerging issues in digital forensics. However, it introduces other challenges, such as distributed digital data processing, data acquisition (physical and logical), extraction, and data analysis problems (Arshad et al., 2020).

It is becoming increasingly difficult to prevent an IoT breach as evidence is no longer limited to a mobile device or a personal computer (PC) but can also be found in vehicles, RFID cards, and smart devices.

The impact of IoT devices on forensics investigations is that they will complicate matters further due to the nature of the devices being analyzed. Data at a crime scene may be overwritten or compressed if the devices cannot communicate with a cloud service provider to store their data and collect more data than they can store. Data that has been overwritten or compressed cannot be used as evidence in a court of law for justice. Hence, presenting digital forensic evidence in court has proven difficult for investigators due to a variety of factors such as an insufficient chain of custody, failure to follow legal procedures, and insufficient evidential integrity.

It is critical to conduct research to identify methods for performing IoT-based digital forensic analysis. Long-term goals include creating digital forensic standards that can be used as part of the overall IoT and Internet of Anything (IoA) security and aid in IoT-based investigations (MacDermott et al., 2018).
More also, following legal procedures in gathering evidence at a digital crime scene is critical for admissibility and prosecution, which is a huge challenge in the age of IoT.

5. Current Security Solution to the IoTs

In addressing the IoT's security issues, Brumfitt et al. (2014) suggested shifting from the conventional security approach, as it hinders the secure workability of the IoT and its associated components. The Brumfitt team stated that a novel safety framework is needed to address the challenge of the IoT's security. In comparison, Chen et al. (2014) used data fusion method to secure IoT connections. Meanwhile, Ding et al. (2019) introduced an approach that allows IoT objects to protect themselves against threats. Different research has been performed to address some of the security challenges related to IoT. For example, research done in the area of intentional attacks.

Intentional attacks on IoT infrastructure pose threats to the network's operations, thereby severely disrupting systems and disabling connections, leading to damages and communication problems in the IoT operations. In 2014, Chen et al. investigated the susceptibility of IoT structure under malicious attacks by correlating resilience to percolation connection. Then an information defence paradigm was initiated to minimize the destruction perpetrated by attackers.

In summary, Chen et al. explored the approach used in the biological and medical discipline to improve the security of IoT networks. Although, the result demonstrates that the approach significantly improves the robustness of the IoT infrastructure. However, optimal data fusion approaches on the IoT infrastructure are still required to improve the weak local detection ability and protect the damaged network structure. Some common solutions to IoT security issues are discussed in the following sub-section.

5.1 Common solutions to IoT security issues

Secure the IoT network - By implementing traditional endpoint security features such as firewalls, antivirus, anti-malware, detection systems and intrusion prevention, one can protect and secure the network that connects IoT devices to back-end systems on the internet.

Authenticate the IoT devices - users can authenticate IoT devices by implementing robust authentication mechanisms such as digital certificates, two-factor authentication, and biometrics on a single IoT device.

Make use of IoT data encryption – To protect users' privacy and prevent IoT data breaches, there is a need to encrypt data at rest and in transit between IoT devices and back-end systems using standard cryptographic algorithms. Likewise, the need to fully encrypt key lifecycle management processes to improve overall user data and privacy security. The use of IoT PKI security methods such as cryptographic keys, X.509 digital certificates, and life-cycle capabilities like private/public key generation, revocation, distribution, and management may significantly help ensure a secure connection between an IoT device and app.

Make use of IoT security analytics - Use IoT security analytics solutions to detect IoT-specific attacks and intrusions that may evade detection when traditional network security solutions such as firewalls are used. The use of real-time security analytics on IoT data generated continuously is critical for increasing IoT security. When used at scale, security analytics can detect anomalies in data transmissions that may indicate security threats.

Make use of IoT Application Programming Interface (API) security methods - IoT API security methods like tokens, encryption, signatures, gateway quotas and throttling should be used to protect the integrity of data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. Likewise, IoT API security methods should be utilized to ensure that only authorized developers, apps, and devices communicate with APIs or detect possible threats on certain APIs.

The IoT hardware test- Set up a solid testing framework to ensure the security of IoT hardware. This includes rigorous testing of the range, capacity, and latency of the IoT device. The chip manufacturers of IoT devices also need to strengthen the processors for greater security and lower power consumption without making them too expensive for buyers or too impractical to use in current IoT devices, given that the majority of IoT devices available today are cheap and disposable with minimal battery power. In addition, IoT device manufacturers must conduct extensive testing on all third-party components and modules used in their IoT devices to ensure proper operation with their IoT applications.

Create secure IoT apps - Given the immaturity of current IoT technology, IoT application developers must focus on the security aspect of their IoT applications by strictly implementing all of the aforementioned IoT security technologies. Before creating any IoT applications, developers must conduct extensive research on the security of their IoT applications and strive to achieve a perfect balance between the user interface, architecture and the security of their IoT apps.

Avoid rushing the release of IoT devices- Manufacturers of IoT devices are frequently in a rush to launch their products on the market at the lowest possible price to stay ahead of competitors. In the process, they fail to provide adequate security updates and patches. In the long run, this poses a serious threat to the security of their IoT devices. To address this issue, IoT device manufacturers should avoid releasing products without thorough test running and proper long-term support for the security of their IoT devices and applications.

Take cognizant of the latest IoT security breaches & threats - Device manufacturers and app developers must be aware of the most recent IoT security threats and breaches to ensure the security of IoT devices and applications. Both IoT device manufacturers and IoT app developers must be prepared for security breaches and have a proper exit plan in place to secure as much data as possible in the event of a security attack or data breach. Finally, both IoT device manufacturers and IoT app developers must take the initiative to educate their employees and users on the most recent IoT threats, breaches, and security solutions.

Intelligent algorithms to curtail DDoS and other attacks: As recent trends demonstrate, the DDoS attack will continue to thrive as online activities throughout diverse sectors increases, thus increasing sophisticated strategies and new opportunities for cybercriminals. Organizations must pursue a more proactive defence approach by closing unnecessary terminals and access points using AI to monitor potential signs of compromise and obstructing traffic from network devices or proxy servers that are known to have engaged in prior illegal behaviour.

6. Diverse Areas intersecting IoT: Other Security Issues and Solutions of the IoT

The current state of the art of commercially or entrepreneurially off-the-shelf IoT objects is often accompanied by software solutions that are inadequate to secure all IoT systems (Porras et al., 2018; Wurm et al., 2016). The software-level security is weak as a result of the IoT's various usage patterns. Some authors like Alaba, 2017; Díaz et al., 2016; and Rashid & Rehmani, 2016, focus on IoT security because it is a real problem that the new technology faces.

The study by Airehrour et al. (2016) stated that diverse networks communicate ultra-sensitive data over the Internet with many challenges to mobile communications sensor networks. Therefore, it is paramount to comprehend security concerns when implementing IoT technologies. The main security concerns identified by the research community in recent times can be classified. There are nine classes of concerns in primary studies. However, for the simplicity of information, they were further classified into four subgroups. The main elements are devices vulnerability, functional constraints, data privacy, and surrounding constraints.

Similarly, there are enforcement processes which include cross-device reliance, recognition, permission and validation. Moreover, there is a control variable like Legislation. Furthermore, there are attacks which include threats and modes. The classes are associated with each other and other classes can be considered and discussed as follows;

(a) Environmental Constraints

Environmental constraints are part of the challenges of IoT security (Hossain et al., 2015). These ecological constraints include hardware limitations; that is, devices are constrained by the battery, memory, and computational power. It is not easy to compute a complex memory of IoT devices, which means complex memory with thorough operations is not suitable for the IoT. Another environmental constraint is software limitations; that is, the operating systems (OS) in IoT gadgets pose thin network stacks that are not remotely re-programmable. Constraining software architecture of safety modules can provide security patches for the operating systems.

More also, there are network constraints, that is, the size, heterogeneity, mobility and network value-added constraints and challenges to the security design of IoT. Roman et al. (2011) concluded that network and computational weakness are environmental challenges in IoT security. Hence research is urgently required to address environmental constraints to IoT security, inclusive of novel approaches to its ethical use and safety.

(b) Vulnerable Devices

Susceptibility of devices is part of the security challenges of IoT. Researchers such as Zhang et al. (2015) and Yu et al. (2015) highlighted that device security is significant to IoT's security. The work by Yu et al. demonstrates numerous known vulnerable devices that have issues such as passwords, hardcoded, open domain name system (DNS) resolvers, and administrative usernames, which could be leveraged for distributed denial of service attacks. In 2012, Airehrour et al. introduced a case whereby live footage via Trend net IP cameras was made public to Internet users without a password. The research by Patton et al. (2014) looked at vulnerabilities of IoT devices. The study reveals that a small percentage of insecure devices could create significant vulnerabilities. The vulnerabilities of IoT are extensively discussed subsequently.

(c) Vulnerabilities of IoT

Nowadays, there are numerous vulnerabilities in IoTs. With information being sensitive and vulnerable to attacks, sharing data and services in the IoT can pose significant security challenges (Ferretti et al., 2021). Large IoT devices and a massively complex IoT ecosystem may have increased vulnerabilities from extreme to cloud security challenges (Torres et al., 2021; Jain & Singh, 2020). Security is a significant issue when IoT devices are integrated with centralized management platforms and legacy systems (Wang et al., 2018). Users can inadvertently introduce security flaws, particularly at the application layer. The vulnerabilities are weak encryption protocols, compromised authentication controls, unoptimized input and output filtering, and many other flaws. The following are some examples of IoT vulnerabilities:

1. Weak, hardcoded, or guessable passwords: The use of easily brute-forced, publicly available, or unchangeable credentials, such as backdoors in client software or firmware that allow unauthorized access to deployed systems (Chandavarkar, 2020, Verma et al. 2019; Ferrara et al. 2019). Hard-coded and embedded credentials pose a risk to information technology systems and are equally dangerous to IoT devices. Guessable or hard-coded credentials are also a boon for hackers looking to attack the device directly. Furthermore, the malicious attacker may already know the machine's password with default passwords, leading to vulnerability. IoT devices should have flexible, secure default settings and optional mechanisms such as password expiration, password complexity, and one-time password account lock-out, which forces users to change the default credentials when configuring the

device. As a result, manufacturers should secure IoT devices with unique passwords right out of the box to address vulnerabilities.

2. Insecure Network Services: Vulnerable IoT runs unnecessary or insecure network services on the device itself, particularly those that connect to the Internet and compromise the confidentiality, integrity, authenticity, or availability of information (Ferrara et al., 2021). Similarly, unneeded or insecure network services that allow unauthorized remote control (Neuman & Steiner, 1988) can lead to IoT vulnerabilities.

3. Vulnerable ecosystem interfaces: Vulnerabilities of IoTs include insecure web, backend application programming interface (API), cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components (Jiang et al., 2020; Thilakarathne, 2020; Visoottiviseth et al., 2020; Ferry & Nguyen, 2019). Vulnerabilities in IoT can also be caused by a lack of authentication and authorization (Kim & Lee, 2017; Shahzad & Singh, 2017), a lack of encryption or weak encryption (Grabovica et al., 2016), and a lack of input and output filtering (Li et al., 2019). Device authentication is one solution that can secure access to a connected device and generate data. In addition, the use of digital certificates allows a digital entity (IoT device, computer, etc.) to transfer data to authorized parties securely.

4. Insecure update mechanisms: the inability to securely update the device may result in IoT vulnerabilities (Chandavarkar, 2020; Choi et al., 2018; Doddapaneni et al., 2017). This includes a lack of firmware validation on the device (Basnight et al., 2013), a lack of secure delivery (i.e. unencrypted in transit), and a lack of authentication (Babar et al., 2010). Others include a lack of anti-rollback mechanisms (Bachy et al., 2019; Minoli et al., 2018) and failure to notify users of security changes caused by updates (Bertino & Islam, 2017; Snoeren & Balakrishnan, 2000). Secure update mechanisms should include adaptable features such as password complexity, which forces users to change the default credentials when configuring the device.

5. Insecure or deprecated software components and libraries: The use of insecure or deprecated software components and libraries that could allow the device to be compromised may lead to vulnerabilities in IoTs (Abiodun et al., 2021; Al Hayajneh et al., 2020). This includes insecure operating system platform customization and the use of third-party hardware or software components from a tainted supply chain.

6. Inadequate privacy protection: When a user's personal information is stored on the device or in the ecosystem and is used insecurely, improperly, or without permission, it can easily lead to vulnerabilities in IoTs (Abiodun et al., 2021; Yu et al., 2020; Xiong et al., 2019; Yin et al., 2017). As a result, adequate privacy protection for IoT devices is required to avoid vulnerabilities.

7. Insecure data transfer and storage: Inadequate access control or encryption of sensitive data anywhere within the IoT ecosystem, including at rest, in transit, and during processing (Lamport, 1981). While many IoT vendors and users focus on secure storage, ensuring data security during transfer is frequently overlooked. As a result, research is needed to secure data transfer and storage in IoTs to avoid unusual vulnerabilities.

8. Lack of device management: A lack of security support on production-deployed devices (Maloney et al., 2019; Perumal et al.,2015) could lead to IoT vulnerabilities. Asset management (Brous et al., 2019), update management (Surya, 2016), secure decommissioning (Yaqoob et al., 2017), systems monitoring (Choi et al., 2018; Sajid et al., 2016), and response capabilities are examples of such capabilities (Condry & Nelson, 2016). Though IoT devices are small, inexpensive, and widely deployed, that does not mean they should not be managed. In fact, it makes managing them even more critical to avoid vulnerabilities, even if managing is not always convenient, easy, or cheap.

9. Insecure default settings: Devices or systems that are shipped with insecure default settings or that lacks the ability to make the system more secure by restricting operators from modifying configurations (Barcena et al., 2015) may be vulnerable. In order to avoid malicious vulnerabilities, insecure default settings should be avoided.

10. Lack of physical hardening measures: A lack of physical hardening measures (Chandavarkar et al., 2020; Bossler & Holt, 2009) allows potential attackers to gain sensitive information that can aid in a future remote attack or take local control of the device (Zeng & Li, 2020; Naumovski & Taneski, 2019; Saeed et al., 2013; Steinberg & Speed, 2005). Secure physical hardening measures include password complexity, account lock-out, and a one-time password that requires anyone setting up a device to change the default credentials. As a result, physical hardening measures such as security paradigms are required to prevent attacker penetrations and vulnerabilities in IoTs.

(d) Data Privacy

Most studies reveal that data privacy is a challenge to IoT security due to the high possibility of insecurity (Malina et al., 2016; Henze et al., 2015; Fink, 2015; Roman et al., 2013). These risks include eavesdropping, data modification, unauthorized access, illegal remote access, and data forgery involving devices (Omolara et al., 2019). For example, collected data, in the form of names, phone numbers, addresses, bank names, and insurance policy numbers, are always vulnerable and more problems can occur if such data are available in the cloud environments. Likewise, many IoT systems and applications enable critical detail, which may leak to attackers and enable penetration into the system. Consequently, unprotected and unsecured personal information that is sensitive may become available to an unauthorized third party.

(e) Enforcement Mechanisms

The legislation and enforcement of IoT is presently lacking or not effective to address security challenges. Some researchers like Yu et al. (2015) identified that conventional enforcement mechanisms of IoT deployment are unlikely to be effective. Currently, there is no provision for host-based defences like antiviruses. IoT is devoid of automatic updates of software to devices of conventional networks. Although susceptibility of repair occurs mostly through firmware updates, however, it is carried out by the manufacturer for each device. The present IoT security apparatus also heavily depends upon powerfully fixed object defences, like using firewalls. Nevertheless, when devices are compromised, the defences' technique will not be effective.

Kumar et al. (2016) investigated the security of IoT and discovered the absence of safety updates of IoT objects. Most of the conventional enforcement mechanisms are unlikely to be effective in IoT deployments for several reasons.

(f) Cross-device dependencies

The interconnected nature of the IoT represents another security risk. Normally, IoT objects could pass on data to each other. For example, a networked thermostat like NEST can control an air conditioning system operating in a smart home. However, this cross-device dependency may be prone to more security risks. A study by Yu et al. (2015) noted that the nature of IoT connection depicts additional security risks. A typical security risk scenario is that if an adversary disabled operating air conditioning in a room, it could cause the temperature to rise. Disabling of the operating air conditioners by the adversary may cause the temperature to rise. Thus, influencing another system to open the closed windows. The opening of closed windows may lead to an atmosphere of security risk. Hence, cross-device dependencies may further increase the IoT security challenge.

(g) Identification, authentication, and authorization

Lack of identification, verification, and permission to the network are part of the IoT device's security challenge. Recently, many researchers (Cisar and Cisar, 2016; Basu et al., 2015; Abomhara and Køien, 2014) said security is the key issue of IoT devices such as identification, authentication, and authorization. Numerous IoT devices do not permit unique identification, authentication, and authorization of a single device, making it extremely complex.

Likewise, there exists an authentication problem. A certain level of access control is needed to prevent everybody from accessing everything in a network. The study by Nguyen et al. (2015) was a survey on communication protocols for IoT. It highlighted the fact that currently, few protocols provide security and privacy to users. Therefore, there is a need for further studies on a framework that can offer security and privacy to users of the IoT devices.

(h) Intrusion Detection using Edge Computing

IoT applications can use fog/edge computing to improve scalability and energy efficiency, as well as to take full advantage of computational node resources to analyze collected data and meet latency requirements. Edge computing is a novel infrastructure that can be used for attack and intrusion detection in IoT devices (Roman et al., 2018). It takes place on-site or close to a specific data source, reducing the need for data to be processed in a remote data center. Edge computing, in other words, is a distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers. This proximity to data at its source can result in significant business benefits such as faster insights, faster response times, and increased bandwidth availability. Edge computing captures and processes data as close to the source of the data or the desired event as possible. It collects data using sensors, computing devices, and machinery and sends it to edge servers or the cloud. Thus most data calculations are now performed in the cloud or at a datacenter.

The computing is done at or near the source of data, rather than relying on the cloud at one of a dozen data centers to do all of the work. As a result, edge computing processes this data within the network rather than sending all data collected by IoT sensors directly to the cloud and only relevant data or information is sent, reducing latency issues. Analysts define Edge as a method of bringing data processing closer to the business, connecting millions of IoT devices, and placing containers of equipment in fields, all of which are enabled with the speed of 5G networks. Edge computing dates back to the 1990s when Akamai launched its content delivery network (CDN) (Chen, 1998). Back then, the idea was to put nodes in locations geographically closer to the end user to deliver cached content like images and videos.

While some of the discussed challenges of IoT ranges from security, privacy concerns, reliability, availability, costs, data and information management, amongst others, edge computing is better able to withstand these obstacles by processing data closer to where it is created or needed, culminating in not only faster processing but also other advantages such as better security, cost-efficiency, improved privacy, advanced analytics, actionable data insights, and much higher reliability.

Nevertheless, in order to obtain the maximum benefit of fog computing for IoT, a number of complex challenges must be remedied. The majority of computational nodes in edge computing are battery-operated, making them unsustainable. Furthermore, the efficient provisioning of computing resources to latency-sensitive IoT applications like connected autonomous driving, AR/VR, haptic technology, as well as the full integration of fog computing with cloud computing to proffer scalable services requires further investigation.

(i) A legislative solution to IoT security challenges

Legislative solutions to IoT security challenges became complex due to the heterogeneity of connected devices and the nature of their guarantee. Weber (2010) focused on new security and privacy challenges and suggested regulatory frameworks to safeguard users' privacy. Weber opined that the current regulation is insufficient to ensure both security and privacy. He further noted that global regulation would be necessary because IoT is global. Hence, a worldwide regulatory framework is required to secure IoT and its devices.

One of the first cohesive global standards for IoT cybersecurity is ETSI EN 303 645. The standard establishes a single, attainable goal for manufacturers and IoT stakeholders to achieve. Consumer confidence in the security of everyday products connected to the internet is also aided by ETSI EN 303 645 (Ng, 2019) and IoT standards such as NISTIR 8259 (Fagan et al., 2020). The Mosaic Web browser was identified as the Internet's killer app in the early

1990s (Galindo et al., 2008). Netscape, Napster, Friendster, Google search, customized and real-time healthcare, and others quickly followed. In contrast, considering the terms filler app and app killer. As more military drones are developed, the software that powers them may be used to bomb and destroy targets, which frequently include people. Other financial and accounting programs had been around for a while, but VisiCalc was the first to use a modern spreadsheet interface. It is widely regarded as the first "killer app".

The study by Suo et al. (2012) focused on the necessity for security law and regulations that protect IoT systems. Suo argued that if IoT is associated with privacy, business secrets, and national security, it requires adequate legislation support to promote its development. The proposed solutions to the security challenges of IoT are categorised as in Table 3.

Table 3: The Proposed Solutions Classification

S/n	Problems of the IoT	Solutions to the Problems	Authors in agreement
1	The danger and unimaginable challenges involving IoT	Trust handles the danger and unimaginable challenges of IoT. Trust of the devices in communication regarding privacy and security	Andrea et al., (2016), Hossain et al., (2015), Yan et al., (2014), Abomhara et al., (2014) and Roman et al., (2011)
2	The weakness of validation models causes insecurity and user privacy issues.	Several validation models for IoT could assist in safeguarding and providing privacy.	Lee et al., (2018), Chaudhry et al., (2017), Mahmood et al., (2016), Zhang et al., (2015)
3	Lack of privacy plan in the design of the IoT objects.	Allow users to have the tools for controlling private data in securing critical information from the environment.	Henze et al., (2016), Roman et al., (2011)
4	Lack of plan for legislative implementation role.	It is a software solution to the IoT security challenges.	Barrera et al., (2018), Phung et al., (2017), Yu et al., (2015).
5	Fault-tolerant security challenge.	There should be a defence strategy for the IoT devices to counter network intrusion or failure.	Misra et al., (2012), Roman et al., (2011).
6	Inadequate preliminary plan for IoT network protocol to secure communication.	There is a need for classical Internet hosts to generate an extended Internet that will enable the utilization of different security solutions to establish protective transmission.	Kumar et al., (2016), Nguyen et al., (2015)
7	Inadequate plan to secure protocols for preventing routing attacks.	Help improve protocols to secure routing for IoT objects and counter routing intrusion.	Karlsson et al., (2018), Airehrour et al., (2016)
8	DDoS intrusion in the IoT infrastructure.	Useful in recognition, protecting or reducing DDoS intrusion in the IoT	Bhardwaj et al., (2018), Zhang et al., (2015),

		system.	Zhang, & Green, (2015)
9	Spam prevention issue of the IoT.	Digital signatures to secure 2D barcodes in countering spam issues in IoT.	Razzak (2012)
10	Shortage of semantic logic for vital system of IoT devices.	Security model that applied semantic logic for essential protection of IoT infrastructure.	Zamfiroiu et al., (2019), Vasilomanolakis (2015), Kozlov et al., (2012).
11	The absence of policy causes insecurity of the IoT structure.	Policy solution to protect objects and judgement for cyber intruders.	Saleem et al., (2018), Sicari et al., (2017).

Besides understanding the types of threats and intruders, it is necessary to assess IoT security challenges.

(j) Behavioural authentication in mobile devices

Behavioural authentication in mobile devices identifies a person based on unique features such as biometric authentication, which uses patterns displayed when interacting with a device such as a tablet, smartphone, or computer that includes a mouse and keyboard. Every perspective from finger pressure on the keypad to the angle at which a person holds their phone, is taken into account.

A secure authentication scheme is required to control access to smart watches, smartphones, e-readers, laptop computers, tablets, and handheld gaming consoles. Devices such as smartphones, tablets, and laptop computers are now more than just personal assistants for people. These devices have opened up new ways to play, work, and socialize. They are small in size, making them easy to handle and store in users' bags, purses, or pockets. Mobile devices, on the other hand, are prone to a variety of issues. One of the most serious issues is the possibility of a breach of security and privacy if the device falls into the wrong hands. Threats may come from both friends and strangers. Similarly, due to the portability and mobility of mobile devices, they are easily lost. If a thief gains access to them, the details of users may be exposed, and their private lives may become public. They may also be prone to blackmail or been extorted.

A biometric scheme seeks to detect and identify the user. The United States National Science and Technology Council's Subcommittee on Biometrics divides biometrics into behavioural and physiological categories (Alzubaidi & Kalita, 2016; Shepard et al., 2006). Behavioural biometrics is the study of patterns in human activities that are uniquely identifying and measurable. On the other hand, physiological biometrics refers to physical measurements of the human body, such as the face or facial recognition, nose, fingerprint, hand geometry, retina, iris recognition, and heart-rate sensors. The physiological characteristics-based recognition system has relatively high accuracy.

The distinction between physiological and behavioural biometrics is that physiological biometrics refers to physiological features on the human body, such as a fingerprint or retina scan. In contrast, behavioural biometrics refers to behavioural features on the human body. Behavioural biometrics examines parameters such as a user's typing keystrokes, navigational patterns, screen pressure, typing speed, mouse or mobile movements, gyroscope position (human motion recognition), and much more.

Behavioural Biometrics identifies a subject by using behavioural traits such as how a person touches a screen, walks, talks, signs a signature, and types. When analyzed using one or more of these features, each subject is expected to differ from all others. Keystroke dynamics, touchscreen, gait analysis, handwaving, voice ID, signature analysis, mouse use characteristics, profiling, cognitive biometrics, electroencephalogram (EEG), and an electrocardiogram are some other human factors behavioural biometrics traits and verification methods (ECG). One compelling argument for behavioural biometrics is that it can help with continuous and passive authentication without the need for additional hardware (Alzubaidi & Kalita, 2016). As a result, using behavioural biometrics is likely to be less expensive than using physiological biometrics.

Physiological biometrics detects people's physical make-up and employs resources such as retina or iris scans, face recognition, and fingerprints. Behavioural biometrics is based on a user's behaviour and include analyzing features or information such as handwriting shape and flow, keystroke timing, and unique patterns inherent in a person's gait and speech. Similarly, it involves analyzing user behavioural features, stylus usage, and other aspects of a person's general behaviour. Biometrics applications are classified into two types based on their use: identification and authentication. A combination of authentication methods may be able to provide a more secure system. Password/pin, pattern-based authentication, fingerprint recognition, facial recognition, vocal recognition, and iris-based authentication are among the authentication schemes discussed as follows;

(i) Password/pin: The current authentication method for smartphones, laptop computers, and tablets is entry-point authentication, which can be either a secret pattern or a personal index number (PIN). To use a PIN, a user must typically select four (or more) digits for validation. Users must correctly enter this code; otherwise, they will be unable to pass the entry-point to their device.

(ii) Fingerprint recognition: The use of a secret gesture is the second current method for fingerprint recognition. A secret gesture is defined as moving a finger across the screen in a specific pattern. This pattern can be used as biometric authentication to allow the user to enter the device. A biometric is a unique physical or behavioural characteristic of an individual. Biometrics is a technical aspect used to distinguish one person from another. That is, it is one of the methods for determining a person's identity. Different types of biometric sensors and how they work is presented in Figure 5.

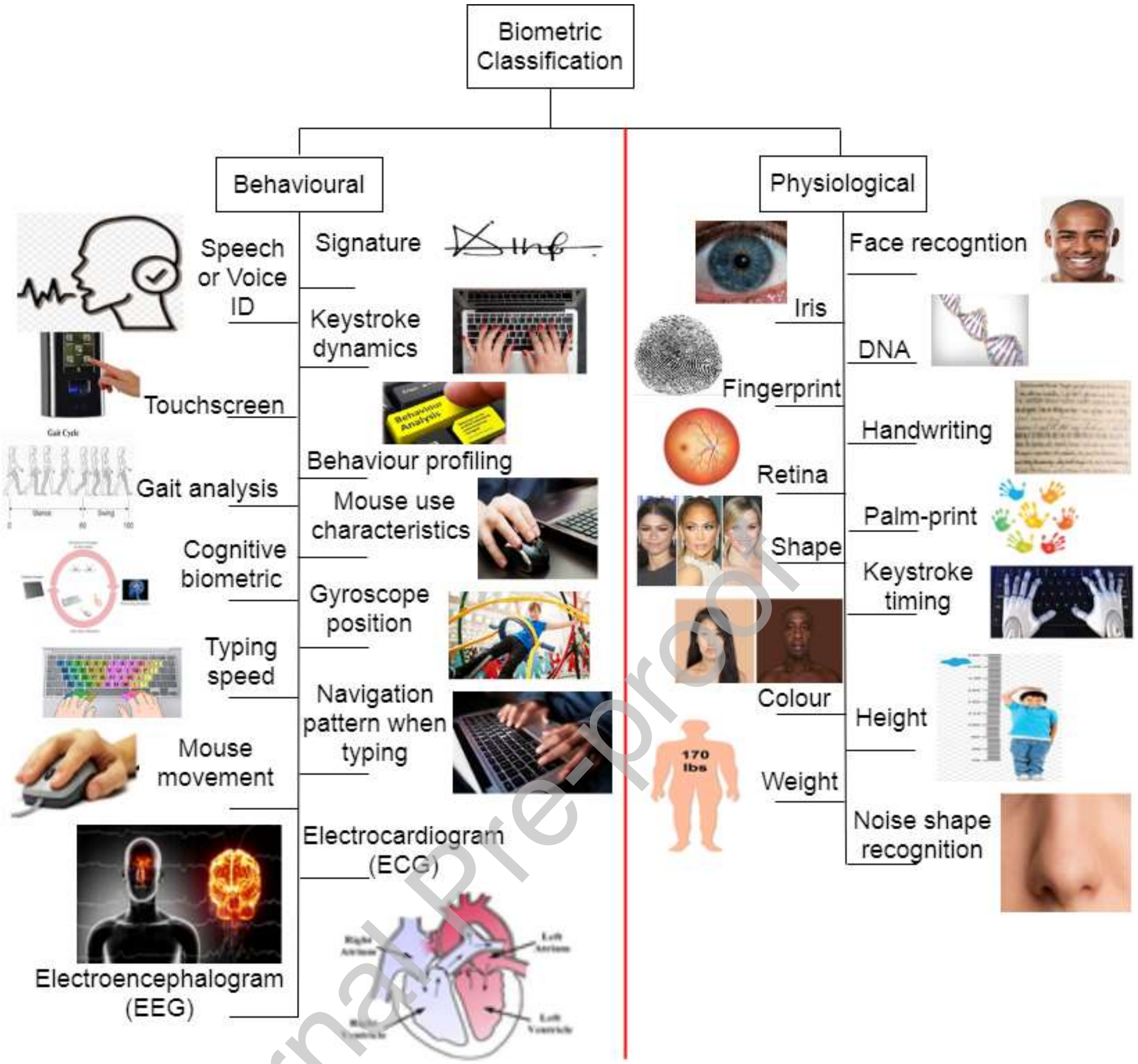

Figure 5. Different Types of Biometric Sensors and Its Working

(iii) Keystroke: Keystroke recognition is a behavioural biometric that authenticates a person based on how they type rather than what they type. A large body of research in the field has accumulated over the last 30 years, establishing its potential as a standalone biometric as well as an addition to traditional username/password authentication schemes. It is an excellent candidate for increasing the security of authentication systems because of its transparency, low deployment cost, and seamless fit into existing commercial and governmental applications.

Existing biometric gait recognition tools are classified into machine vision-based, floor sensor-based, and wearable sensor-based. In machine vision-based gait recognition, cameras are used to collect data, which is then analyzed using image processing techniques. Wearable sensor-based gait recognition systems detect and record gait activities using wearable devices equipped with sensors such as accelerometers, gyroscopes, and force sensors. Most smartphones now include accelerometers that can detect a user's gait-related data. The researchers' system does not require additional hardware to function, so upgrading existing smartphones does not incur additional costs. It functions by continuously analyzing gait-related data collected by the smartphone's built-in accelerometer and notifying the smartphone's owner via e-mail when unusual changes in gait patterns are detected. Performance biometric technology is described in Table 4.

Table 4. Performance Biometric Technology

S/n	Biometric type	Device use	Social acceptability	Transparency nature	Cost	Performance (Accuracy)
1	Facial recognition	Camera, camera can be built into mobile devices such as smartphones or wearables	High	High	Medium	Medium-low
2	Voice recognition	Microphone, telephone	High	High	Medium	Medium
3	Fingerprint	Scanner, camera can be built into mobile devices such as smartphones or wearables	High	High	Medium-low	Medium-low
4	Signature recognition	Optic pen, touch panel	High	High	Medium	Low
5	Retina scan	Camera	Low	Low	High	High
6	Iris recognition	Camera	High	High	High	High
7	Hand geometry	Scanner	High	High	Low	Medium-low
8	Gait analysis	Smartphones will have built-in accelerometers or wearable devices with sensors	High	High	High	High
9	Touchscreen	Mobile phones, touch panel	High	High	Medium	Low
10	Keystrokes dynamics	Computer and laptop or Smartphones	High	High	Low	High- medium
11	DNA	Laboratory equipment	High	High	High	High

(iv) Iris: The iris is the coloured area of a person’s eye surrounding the pupil. It is a highly trusted biometric. The complex and random patterns in each person's iris are unique, making testing accurate, simple, and quick. Because the eye is a visible organ, the iris can be matched using a photograph. Iris scanners were introduced at several UK airports in 2004, including Heathrow, Gatwick, Birmingham, and Manchester. They eventually phased out because they were thought to take longer than standard passport checks. According to companies like EyeLock, iris scanning will be helpful in applications like the internet of things and driverless cars. It is a fixed feature, which means that each person can only have two distinct iris images. The equipment used for iris scanning can take up a lot of space. It also necessitates a close proximity.

(v) Fingerprint: Fingerprint scanning is one of the most cost-effective biometrics because the technology required is not prohibitively expensive. It is also very portable; all that is needed to capture the fingerprint image is a small camera to be built into mobile devices like smartphones or wearables. As a result, it is a good authentication method for mobile applications on devices that have this hardware. Password authentication on mobile devices is generally inconvenient due to the devices' limited typing capabilities. It is also not a good biometric for children whose fingerprints change.

(vi) Facial recognition: Facial recognition is a low-cost, non-intrusive technology. The smartphone is fairly well-suited for performing facial recognition; due to the general public's penchant for taking selfies. Thus, device manufacturers have invested heavily in the front-facing camera on smartphones. People can look at the device's screen to see if the camera is capturing an image of the correct part of their face. Facial recognition is now used at e-Passport gates at some UK airports. It is also used in MasterCard's self-service payment app. A potential disadvantage is that changes in lighting can affect the image. It is also dynamic, meaning that it changes as a person ages, cuts their hair, or wears glasses. There is a high possibility of it changing due to plastic surgery on the face. Numerous face recognition algorithms have been evidenced to fail to recognize faces following plastic surgery, posing a new challenge for automatic face recognition. More also, attackers may use face recognition to their advantage (Nappi et al., 2016; El-Said., 2014).

(vii) DNA: Given that 0.10 percent of a person's entire genome is unique to them, DNA testing is extremely difficult to deceive and likely to be accurate. If 26 different bands are studied, the chances of two people having the same DNA profile are less than one in a hundred billion. Even a simple DNA test, on the other hand, necessitates sophisticated and costly technology. Because it requires a physical sample, it obviously necessitates the person being physically present with the testing equipment and can be a very intrusive method of testing. However, steps have been taken to develop portable DNA testing equipment. Researchers presented a low-cost platform for detecting Chlamydia that integrates sample preparation, DNA amplification, and data processing in an instrument the size of a coffee mug at a 2015 American Association for Clinical Chemistry meeting. The analysis unit connects to a smartphone, allowing the user to control the platform and process data through an app. While it is a different application, the invention suggests that a portable testing unit could be built even on the IoT’s platform. Voice is a dynamic biometric, which means that it changes over time for each individual. Unlike a person's DNA, their voice will change dramatically as part of the natural aging process. One inherent advantage is that voice authentication does not require physical proximity. People frequently say the same words in different ways, which means that the voice biometric shifts even on a daily basis. However, voice biometrics experts argue that saying the same words in different ways does not change or alter the underlying physical characteristics of the voice (Vittori, 2019).

(k) Energy problem in IoT

The battery life and power consumption of IoT devices is an area that requires further investigation in order to achieve significant success. At the moment, IoT devices are inefficient in terms of energy supply (Rana et al., 2021). The energy consumption of a device is heavily dependent on whether it is continuously sensing, processing, and transmitting/receiving potential data (Perkovi et al., 2020). IoT-connected devices frequently generate a large amount of electronic waste and consume a significant amount of energy when performing various tasks (Abedin et al., 2015). This will eventually pose a challenge in the near future in terms of reducing energy consumption, as well as developing new methods of developing green communication across the network. As a result, along with the current emanating challenges, energy consumption reduction and the deployment of green IoT should be considered as future challenges in IoT.

Energy consumption is acute in heterogeneous devices because it actively correlates with the cost and availability of the IoT network. Energy consumption has become a critical issue in the future of the Internet. Various algorithmic approaches, such as complementing hardware or different system-based approaches, have been initiated for more effective solutions. The most frequently mentioned energy-efficient methodologies include defining systems with two or more states using the ALG-P algorithm. Other features include various power-down mechanisms, scheduling with deadlines or minimizing response time, and multiple states using the ALG-P algorithm (Abedin et al., 2015; Albers, 2010). Albers' study's main contribution is a proposed system model capable of resolving the challenges of IoT energy-efficient mechanisms for heterogeneous devices. That is, devices that adhere to the proposed IoT system model in order to promote G-IoT and extend the life of the IoT network.

Since IoT devices have limited energy sources and frequently operate on batteries with limited energy capacity, the deployment of green communication and system models in IoT has been a major challenge. More sensor samples mean better data interpretation, but it also means more power consumption. Prior to deciding on further actions, it is necessary to determine: (i) how long the device will be sensing and (ii) the strategy for manipulating and communicating with respect to the received data.

To deal with the power consumption and data transmission issues, it is necessary to understand which technologies can be used to deliver data in a timely manner. Communication technologies for deploying low power wireless solutions for IoT can be divided into low and large ranges.

Low Range- Low power local networks are typically used for short-range solutions (less than 1000m). However, they can be considered for transmissions over larger areas when organized in a mesh topology. Popular examples include Radio Frequency Identification (RFID), which allows low-power devices such as tags to communicate over distances of up to 100 meters. Despite being primarily intended for identification, recent RFID devices can be used for sensing and transmitting sensed data via the same protocols.

Bluetooth Low Energy (BLE) is a bluetooth technology used to connect devices that uses a low data rate (i.e., up to 1Mbps) and consume information over a short distance range (in theory, up to 100m). Bluetooth 4.0 (i.e. BLE) was introduced after improvements, with simpler pairing functions, higher data rates (maximum of 24Mbps), and low power consumption, with the goal of connecting IoT devices. Zigbee is a technology similar to Bluetooth in that it can cover similar distances (i.e. up to 100m). The updated version (3.0) is primarily intended for industrial environments and has a data rate of 250 kbps. Its design is rugged, with low power consumption, and is intended for occasional data transmission.

Long range - Low power wide area networks (LPWAN) can connect devices over distances of up to 1000m. This technology applies to low-power radio communication networks, in which a single base station can power thousands of end devices. DASH7, a multi-layered architecture LPWAN radio technology, aims to provide communication over a range of up to 2km while operating in the 433MHz, 868MHz, and 915MHz bands. Low latency, 128-bit AES encryption, mobility support, and data rates up to 167Kbps provide an appealing advantage for IoT applications.

Sigfox creates wireless networks to connect low-power objects like electricity meters and smartwatches that must be constantly on and emitting small amounts of data. Sigfox is a cellular system that uses Sigfox operator base stations to cover areas (Mekki et al., 2018). It is a French global network operator founded in 2010. Likewise, the Binary Phase Shift Keying (BPSK) modulation connects end-devices to base stations (Lee & Kim, 2010). The system operates in the 868MHz band, utilizing the available spectrum of 400 channels with a bandwidth of 100Hz.

In rural areas, the achievable range can be 30-50 km, and in urban areas, it can be 3-10 km. Every base station can cover approximately one million end devices, while each device is limited to approximately 140 messages sent per day at a data rate of 100bps. LoRaWAN The network architecture is referred to as a "star of stars" topology, with long-range (LoRa) enabling long-distance radio communication. LoRa is a low-power wide-area network modulation technique that is proprietary. The protocol governs network capacity, quality of service, and security. It employs Chirp Spread Spectrum modulation, which can achieve data rates ranging from 290bps to 50kbps while remaining extremely power efficient. Depending on the power of the radio, the range can be from 2-5 km in urban areas to 45 km in rural areas. Indoor applications are the primary focus of Narrow Band-IoT (NB-IoT). It is based on LTE-M and is designed to connect a wide range of low-power sensor devices in IoT networks.

(l) Forensic issues in IoT

As the number of IoT-connected devices grows, it has become necessary to develop a new process for investigating IoT-connected security breaches and crimes. Addressing security concerns will necessitate a new era of digital forensics and analysis, best practices for verifying and leveraging physical and digital evidence in the context of a changing regulatory landscape. While there are no set rules for IoT forensics, mechanical and electrical investigations will be heavily relied on. Since identifying evidence requires the physical nature of the smart device, obtaining sources is a significant challenge. Currently, computer forensics and Cyber security investigators are looking into the IoT from various perspectives of a computer forensic analyst on evidence handling, evidence extraction, and evidence analysis data gathered. Therefore, evidence could be gathered using fixed sensors in homes and buildings, healthcare organizations, moving sensors integrated into automobiles, wearables, communication devices, cloud storage, Internet service provider (ISP) logs and so on.

7. IoT Open Research Issues/Opportunities

A growing number of interconnected systems have continued to bring about traffic, even modern traffic models. Some of the issues are due to the increasing demands of data processing and storage; consequently, privacy and security risk surfaces. While considerable research has been done regarding IoT security, many challenges remain unresolved and new challenges continue to emerge.

The security of IoT devices' endpoints is vital since it is connected with a huge number of intelligent objects. Therefore, effective and efficient authentication standards are required to address the areas of encoding, privileges, profiles, time-stamping protocol, explicit trust relationship, and so forth (Sfar et al., 2018).

Likewise, research interest should be focused on IoT ecosystems. A colossal data ecosystem registry is required to track areas that could affect the security of IoT components in their life cycle. Furthermore, interactions of IoT require discussion among IoT security issues. An incident relating to security and event management repository could help address IoT logs for real-time, historical, and predictive analysis.

The main concern is that security dominates over the ease of utilizing IoT systems (Alansari et al., 2018). The main communication channel of the IoT remains the Internet. Internet apps need to counter passive and active intruders. Additionally, the IoT domain must ensure the security of intranet hardware, software, physical, and data. The popularity of IoT could gain cybercriminals' attention to launch attacks on the data points, network nodes, commands domain, and input areas. Therefore, there is a need for research to ensure security for the points.

Security breaches of the IoT include illegal use of network and data with intrusion that could disrupt services. Even though people are connected digitally and increasingly, data associated with their activities and locations privacy seems to be disappearing. Security and privacy are common challenges of the IoT. Likewise, confidentiality, integrity, the transmission of data, data stored, validation, and licensing procedures are required to counter users' unauthorized usage.

On the 7th May 2021, Colonial Pipeline company in the United States of America faced a malicious ransomware attack on its computer networks. That is, the company can no longer access their data to continue normal operation. The attack forced the company to temporarily close operational activities and freeze IT networks so as to isolate the malicious software infection into its network. Unfortunately, the company reportedly paid the ransomware attackers responsible for the cyberattack close to $5 million to decrypt blocked systems.

The attack on Colonial Pipeline may have occurred possibly through an old unpatched vulnerability in a network; a phishing email that successfully deceived an employee, using purchased access credentials or gotten from another place that was leaked previously, or some tactics used by cybercriminals to penetrate the company's network. It is evident that DarkSide criminals targeted the business side of the victim more than operational systems, which mean the purpose was based on money rather than aimed to crash the pipeline. This type of ransomware attack can also occur on IoT devices that deny user access and prevent device functionality. Hence, more research focus on securing IoT devices against ransomware attacks is open and timely. Also, intelligent models are needed to automatically ensure that organization's own devices are not being recruited as bots.

8. Recommendations

Aside from the previous solutions to IoT security challenges discussed earlier in the sections, certain things also need to be considered, such as the following recommendations;

(i) Use an accepted IoT cybersecurity framework from industrial experience, standard and right practices, such as those given through regulatory agencies.
(ii) IoT devices need not depend on the network firewall alone to block malicious communication.
(iii) It is of utmost importance to create an IoT/Cybersecurity incident response plan and give the router a name.
(iv) It is crucial to perform a weakness examination of devices connected to remote systems.

(v) It is always necessary to change default usernames and passwords and check the setting for devices.

(vi) There is a need for the compartmentalization or separation of IoT systems to reduce attack surfaces.

(vii) There is a need to monitor and share threat intelligence. Furthermore, it is vital to scan all software to avoid vulnerabilities in the networks.

(viii) It is essential to install security software, add objects and containers to digitally fence networks and devices.

(ix) Individuals, organizations and governments must monitor and share threat intelligence.

(x) Multiple IoT protocols parsing can be added as an extension to the firewall protection. Some examples are message queuing telemetry transport (MQTT), extensible messaging and presence protocol (XMPP). XMPP is a public XML innovation for real-time dissemination of information that powers widespread applications like instant messaging, presence and partnership.

(xi) Likewise, support for other attack detection mechanisms like Distributed DoS (DDoS) and Internet Protocol (IP) spoofing can be added.

(xii) Need to ensure regular updating and patching weakness of devices and networks.
(xiii) Desist from incorporating devices into the network using default passwords and familiar weaknesses.

(xiv) It is necessary to ascertain access privileges for device applications and controls.

(xv) Powerful validation should be used and probably biometrics as access control.

(xvi) Apply machine validation if connected to a system, and IoT messages encryption, particularly for transit data.

(xvii) Powerful firewalls should be used as current firewalls are designed to protect local area networks (LAN) from remote Internet hosts.

(xviii) Implementing a two-way firewall can help in securing IoT infrastructure. By adding support for the IoT datagram transport layer security (DTLS) and constrained application protocol (CoAP) popularly utilized for communication in the IoT networks.

(ixx) Use secure routers and WIFI and also use strong, unique passwords for Wi-Fi communications and device accounts. Likewise, it is essential to utilized powerful encryption for Wi-Fi operation.

(xx) Use many cybersecurity protections, like antivirus.

(xxi) It is vital to back up all data when possible. Connected devices should not be reachable through inbound connections by default.

(xxii) All data should be secured in transit and at rest, and systems should be protected against unauthorized operation and access.

(xxiii) Data storage objects must be easily removed or rejected from devices. Systems should not have vulnerable external interfaces, for example, unsecured universal serial bus (USB) ports.

(xxiv) Engage security experts, and also one can take cloud security professional.

(xxv) Continuous auditing and the use of real-time analytics, including predictive analytics

(xxvi) The implementation of security awareness training for all organization staff and public exposure to hackers and intruders tricks, dynamism and tactics is of great essence.

(xxvii) IoT objects should be restrictive to intruders rather than permissive in communicating. It is recommended that IoT objects communicate only with trusted endpoints.

(xxviii) IoT systems should be developed with an explicit focus on reducing security risks such as illegal operation or hacking, tampering, environmental hazards, and system faults.

(xxix) Restraining the potential attacker's impact from a security breach like enabling personal identity information and ensuring swift detection and quick management of any compromises.

Even though various efforts are being made to secure the Internet of Things, the goal has not yet been fully achieved. Securing IoT remains a daunting problem. Nevertheless, the implementation of great cybersecurity tools which leverages by artificial intelligence paradigm can significantly mitigate intruders.

9. Future Perspectives and Directions of the IoTs

Future development includes current events, changes, perspectives, and areas of possible solutions in digital technologies.

(a) Quantum-resistance

Most IoT systems that are deployed today could remain functional for years. With the advancements made in quantum computers, many quantum computers may easily cryptanalyze the current cryptographic algorithms in the near future.

Recently, a group of Chinese researchers unveiled the world's most powerful quantum computer, a super-advanced 66-qubit quantum computer which they called Zuchongzhi (Wu et al., 2021). The innovation establishes an unambiguous quantum computational advantage that is infeasible for classical computers in a reasonable amount of time. Zuchongzhi's performance is undeniably impressive. It completed a designated quantum benchmark task in about 70 minutes, a task that would have taken the world's most powerful classical supercomputer over eight years to compute. Using this high-precision and programmable quantum computing platform, researchers can investigate novel many-body phenomena and put complex quantum algorithms into operation. Thus, leading to dramatic success in a broad spectrum of applications. However, it opens several new security challenges, starting from the seamless trust transactions most applications currently leverage. Devices incorporated with current cryptographic primitives becomes vulnerable to diverse cryptanalytic attacks.

Encryption schemes such as the Rivest, Shamir, and Adelman (RSA) are leveraged in sensor networks with the help of trusted platform module (TPM) that is not expensive compared to familiar sensor nodes (Stergiou et al., 2018; Hu et al., 2010). However, the functionalities provided by such schemes may not be secure anymore as Shor's algorithm (which works on quantum computers) would become readily functional for attacking current conventional schemes.

More also, the security condition of symmetric algorithms would decrease. For instance, the security of block cipher of a key size of b bits would only offer b/2 bits of security as a result of Grover's algorithm. This decreasing security scenario becomes more urgently needed when one considers a "harvest and decrypt" attack where an attacker begins to harvest (store) encrypted data before a quantum computer is available. Then decrypt it in the future once a quantum computer is available. Hence, such kind of "harvest and decrypt" malicious attacks might not be new as it was applied during the VENONA project (i.e. United States of America counterintelligence programme used during World War II) (Frazier, 2010; Esther et al., 2020; Abiodun et al., 2020).

Most IoT technologies that are being used currently will continue to be operational for a decade or more. In that period, digital signatures for signing software updates could become outdated, thus, bringing more challenges to update of securing IoT devices. The situation would require the users to migrate to quantum-resistant alternatives precisely for those operationalities involving public key encryption, key exchange, and signatures. Therefore, before quantum computers become more available to resolve complex problems of humankind, necessary steps must be taken to transition to cryptographic algorithms that can offer security even in the presence of quantum computers. While future planning may be quite difficult, it is mandatory to resolve some critical security areas of IoT implementations that are expected to last for decades or more (Garcia-Morchon et al., 2019).

(b) Costs will decrease with future technology

The concept of Industry 4.0 will reduce the costs of living. The new era can be attractive and flourish with the IoT cyber-physical products, virtual reality, cybersecurity, metadata, network integrations, cloud systems, artificial intelligence. All these systems can become big, then Industry 4.0 could virtually mitigate damaged products, environmental hazards, workers cost, auditing, ease control, and reduce waste of resources. Thus, in this era of IoT, the realization of the Industry 4.0 idea can generate great businesses rather than unemployment.

There is a need to balance the gap between developed countries and underdeveloped countries in technology growth. For instance, in most advanced nations, the minimum upload speed can be 20 Mbits; the download speed can be 50 Mbits. Contrarily, the average upload speed can be 2 Mbits, and then the download speed can be 10 Mbits in underdeveloped countries. Therefore, researchers should focus on balancing the existing wide gap between developed countries and undeveloped countries, especially on the inequality access in the broadband Internet to secure communication.

(c) Industry 5.0 -Human less Innovation for the Society

With the Industry 5.0 concept of integration with the current Industry 4.0 or IoT, the evolution to advance intelligent society will undoubtedly be accompanied by more complex security challenges. Industry 5.0 revolution can change human factor of production to machine-dependent nature, which is also called co-laboratory industries (Gorodetsky, 2019; Özdemir, & Hekim, 2018; Skobelev, & Borovik, 2017).

The idea of a digital ecosystem is an open one, self-organizing and which can share resources. It is a system of smart services that can intelligently coordinate tasks and automatically address conflicts in several ways. Recent developments of driverless cars have sparked off new debates, especially with regards to their security. Artificial intelligence incorporated into IoT is currently revolutionising conventional vehicles by leveraging complex models and algorithms to innovate self-driving cars. Highly robust intelligent algorithms aid the operation of self-driving cars, reducing many of the problems associated with driving, such as drunken drivers. Hence, reducing road accidents. The World Health Organization reported that approximately 1.35 million people die in road traffic crashes every year (Lade et al., 2021; Bhalla et al., 2020). Many well-known brands in the automotive industry (including BMW, Tesla, Audi, Volvo, and others) have incorporated this technology into their latest releases. Thus, many driverless cars will hit the road shortly (Dan, 2017).

Additionally, automated supermarkets that could be run by collaborative robots operating without human supervision is also in the pipeline. Therefore, 85 percent of the manufacturers expect synergy with robots in production capacity. Nevertheless, the issue of security in such innovation remains a huge hindering block from its full actualization. An attacker may control the network of a driverless car to cause an accident, steal the car or even direct the car to their hideouts to kidnap passengers and ask for ransom before their release. They may also use the car to commit other atrocious acts for as long as they can control it. The same attack applies to an automated supermarket. A cybercriminal may take old of the network and conveniently shop free of charge without paying. The enormous benefits of IoT, when incorporated into the latest technology, also comes with a huge security risk that needs addressing before its realization in human endeavours.

Security will be a foreseen issue in the next digital world of the 5.0 revolution. Hence, resolving security and privacy-related issues must run concurrently with the concept of Industry 5.0.

(d) Security of the healthcare domain in the IoTs

More novelty is required to secure the healthcare domain in IoT as more devices are expected to be connected as we progress into the future. Thus, research must continue to address the challenges presently limiting the IoT-based healthcare system from moving to a more advanced level with adequate security.

10. Conclusion

The Internet of Things is a new wave of technology that has revolutionized people's lives in diverse aspects, such as smart health, smart homes, smart cities, etc. On the other hand, security is frequently cited as a critical factor enabling the widespread adoption or rejection of any new technology. Security at the device level is a key player for the seamless operation of the IoT. In this study, a survey of current and emerging security issues of IoT was carried out, taking into consideration various viewpoints and in tandem with the current condition of the global world today. Several issues relating to the security of IoT-connected devices and their related domains that have been under-explored in literature were identified, and possible solutions were discussed succinctly. This survey is timely as there have been numerous reports of threats and vulnerabilities affecting IoT and its connected components. As a result, there is a pressing need to steer researchers/stakeholders in the right direction of existing and potential problems as well as proffer clear actionable steps to deal with them. Additionally, there is a need to create awareness and enlighten users of the impact of attacks against the IoTs.

The number of connected devices continues to increase geometrically on a daily basis. Hence, the security of IoT must be continuously reviewed and revisited at regular intervals to serve as a proactive measure before attacks happen and to prepare for better future solutions.

COMPLIANCE WITH ETHICAL STANDARDS

Conflicts of interest:
The authors have no competing interests whatsoever.

Human and animal's rights:
This paper has no animal or human investigation by authors.

Informed consent:
No informed consent is required in this paper, and also it has no animal or human involvement.

References

Abbasi, A. G., & Khan, Z. (2017). Veidblock: Verifiable identity using blockchain and ledger in a software defined network. In *Companion Proceedings of the 10th International Conference on Utility and Cloud Computing* (pp. 173-179).

Abedin, S. F., Alam, M. G. R., Haw, R., & Hong, C. S. (2015). A system model for energy efficient green-IoT network. In *2015 international conference on information networking (ICOIN)* (pp. 177-182). IEEE.

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(4), 2533-2556.

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. *Wireless Personal Communications*, 1-35.

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.

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, 66, 198

Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). Improving Internet of Things (IoT) security with software-defined networking (SDN). *Computers*, 9(1), 8.

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.

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.

Alavi, A. H., Jiao, P., Buttlar, W. G., & Lajnef, N. (2018). Internet of Things-enabled smart cities: State-of-the-art and future trends. *Measurement*, 129, 589-606.

Albers, S. (2010). Energy-efficient algorithms. *Communications of the ACM*, 53(5), 86-96.

Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioural biometrics. *IEEE Communications Surveys & Tutorials*, 18(3), 1998-2026.

Arshad, H., Omlara, E., Abiodun, I. O., & Aminu, A. (2020). A semi-automated forensic investigation model for online social networks. *Computers & Security*, 97, 101946.

Ashley, S. (2019). Felt so violated: Milwaukee couple warns hackers are outsmarting smart homes. Available online: https://www.fox6now.com/news/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes (accessed on 21 September 2021).

Aslanpour, M. S., Toosi, A. N., Cicconetti, C., Javadi, B., Sbarski, P., Taibi, D., ... & Dustdar, S. (2021). Serverless edge computing: vision and challenges. In *2021 Australasian Computer Science Week Multiconference* (pp. 1-10).

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122-140.

Avoine, G., Bingöl, M. A., Kardaş, S., Lauradoux, C., & Martin, B. (2011). A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security*, 19(2), 289-317.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications* (pp. 420-429). Springer, Berlin, Heidelberg.

Babur, K. (2021). DDoS attacks intensify — Driven in part by COVID-19 and 5G. Available online: https://www.securitymagazine.com/articles/94570-ddos-attacks-intensify-driven-in-part-by-covid-19-and-5g. (accessed on 16 September 2021).

Bachy, Y., Nicomette, V., Kaâniche, M., & Alata, E. (2019). Smart-TV security: risk analysis and experiments on Smart-TV communication channels. *Journal of Computer Virology and Hacking Techniques*, 15(1), 61-76.

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*, 58(1), 49-69.

Barcena, M. B., & Wueest, C. (2015). Insecurity in the Internet of Things. Security response, symantec.

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).

Basnight, Z., Butts, J., Lopez Jr, J., & Dube, T. (2013). Firmware modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, 6(2), 76-84.

Basu, S. S., Tripathy, S., and Chowdhury, A. R. (2015). Design challenges and security issues in the Internet of Things, IEEE Region 10 Symposium, *IEEE*, 90–93.

BBC (2017). Cybercrime and fraud scale revealed in annual figures. Available online: https://www.bbc.com/news/uk-38675683 (accessed on 16 September 2021).

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, 50(2), 76-79.

Bhalla, A., Nikhila, M. S., & Singh, P. (2020). Simulation of Self-driving Car using Deep Learning. In *2020 3rd International Conference on Intelligent Sustainable Systems* (ICISS) (pp. 519-525). IEEE.

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).

Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things. *International Journal of Distributed Sensor Networks*, 16(6), 1550147720922731.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1).

Brous, P., Janssen, M., & Herder, P. (2019). Internet of Things adoption for reconfiguring decision-making processes in asset management. *Business Process Management Journal*.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 1-13.

Burmester, M., Van Le, T., & de Medeiros, B. (2006). Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In *2006 SecureComm and workshops* (pp. 1-9). *IEEE*.

Chakraborty, S., Bhatt, V., & Chakravorty, T. (2019). Impact of IoT adoption on agility and flexibility of healthcare organization. *International Journal of Innovative Technology and Exploring Engineering*, *8*(11), 2673-2681.

Chandavarkar, B. R. (2020). Hardcoded credentials and insecure data transfer in IoT: National and international status. In *2020 11th International Conference on Computing, Communication and Networking Technologies* (ICCCNT) (pp. 1-7). *IEEE*.

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.

Chen, P. Y., Cheng, S. M., & Chen, K. C. (2014). Information fusion to defend intentional attack in internet of things. *IEEE Internet of Things Journal*, 1(4), 337-348.

Chen, S. (1998). Content Delivery Network. Cina: Springer-Verlag.

Chen, Y., Chou, J. S., Lin, C. F., & Wu, C. L. (2011). A Novel RFID Authentication Protocol based on Elliptic Curve Cryptosystem. *IACR Cryptol. ePrint Arch.*, *2011*, 381.

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, 23(1), 1-11.

Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer communications*, *34*(3), 391-397.

Choi, S. K., Yang, C. H., & Kwak, J. (2018). System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems* (TIIS), 12(2), 906-918.

Chou, J. S. (2014). An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, *70*(1), 75-94.

Cisar, P., and Cisar, S. M. (2016). General vulnerability aspects of Internet of Things, CINTI 2015 – 16th *IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, 117–121

Cisomag, 2020. 10 IoT Security Incidents That Make You Feel Less Secure. Available online: https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure/. (accessed on 21 September 2021).

Condry, M. W., & Nelson, C. B. (2016). Using smart edge IoT devices for safer, rapid response with industry IoT control operations. *Proceedings of the IEEE*, 104(5), 938-946.

Cortier, V., Gaudry, P., & Glondu, S. (2019). Belenios: a simple private and verifiable electronic voting system. In *Foundations of Security, Protocols, and Equational Reasoning* (pp. 214-238). Springer, Cham.

Cvitić, I., Peraković, D., Periša, M., & Jurcut, A. D. (2021). Methodology for Detecting Cyber Intrusions in e-Learning Systems during COVID-19 Pandemic. *Mobile networks and applications*, 1-12.

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243.

Dan, K. (2017). 10 Million Self-driving Cars will hit the road by 2020: heres ow to profit. Available online: https://lifeboat.com/blog/2017/03/10-million-self-driving-cars-will-hit-the-road-by-2020-heres-how-to-profit (accessed on 16 September 2021).

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer applications*, 67, 99-117.

Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access*, 7, 38431-38441.

Doddapaneni, K., Lakkundi, R., Rao, S., Kulkarni, S. G., & Bhat, B. (2017). Secure fota object for iot. In *2017 IEEE 42nd Conference on Local Computer Networks Workshops* (LCN Workshops) (pp. 154-159). IEEE.

El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internet of Things Security: Layered classification of attacks and possible Countermeasures. *electronic journal of information technology*, (9).

El-Said, S. A., & Abol Atta, H. M. (2014). Geometrical face recognition after plastic surgery. *International journal of computer applications in technology*, 49(3-4), 352-364.

Esther Omolara, A., Jantan, A., Abiodun, O. I., Arshad, H., Dada, K. V., & Emmanuel, E. (2020). HoneyDetails: A prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. *Health informatics journal*, 26(3), 2083-2104.

ETSI TS 103 645 V2.1.2 (2020-06). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

Evans, C. M. (2021). Towards a more accountable United Nations Security Council. BRILL.

Fagan, M., Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). Foundational cybersecurity activities for IoT device manufacturers. US Department of Commerce, National Institute of Standards and Technology.

Ferrara, P., Mandal, A. K., Cortesi, A., & Spoto, F. (2021). Static analysis for discovering IoT vulnerabilities. *International Journal on Software Tools for Technology Transfer*, 23(1), 71-88.

Ferrara, P., Mandal, A., Cortesi, A., & Spoto, F. (2019). Static Analysis for the OWASP IoT Top 10 2018. *Proceedings of SPIoT'19*.

Ferretti, M., Nicolazzo, S., & Nocera, A. (2021). H2O: Secure Interactions in IoT via Behavioural Fingerprinting. *Future Internet*, 13(5), 117.

Ferry, N., & Nguyen, P. H. (2019). Towards model-based continuous deployment of secure IoT systems. In *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion* (MODELS-C) (pp. 613-618). IEEE.

Fink, G. A., Zarzhitsky, D. V., Carroll, T. E., & Farquhar, E. D. (2015). Security and privacy grand challenges for the Internet of Things. In *2015 International Conference on Collaboration Technologies and Systems* (CTS) (pp. 27-34). IEEE.

Frazier, P. (2010). The Venona Project and Cold War Espionage. *OAH Magazine of History*, 24(4), 35-39.

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, 5(4), 2483-2495.

Galindo, D., Roman, R., & Lopez, J. (2008). A killer application for pairings: Authenticated key establishment in underwater wireless sensor networks. In *International Conference on Cryptology and Network Security* (pp. 120-132). Springer, Berlin, Heidelberg.

Gamundani, A. M. (2015). An impact review on internet of things attacks. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 114-118). IEEE.

Garcia-Morchon, O., Kumar, S., & Sethi, M. (2019). Internet of Things (IoT) Security: State of the Art and Challenges. RFC 8576. 2019. Available online: https://rfc-editor. org/rfc/rfc8576. txt (accessed on 27 November 2019).

Grabovica, M., Popić, S., Pezer, D., & Knežević, V. (2016). Provided security measures of enabling technologies in Internet of Things (IoT): A survey. In *2016 Zooming Innovation in Consumer Electronics International Conference* (ZINC) (pp. 28-31). IEEE.

Greenberg, A. (2018). Hackers found a not-so-easy way to make the Amazon Echo a spy bug. Available online: https://www.wired.com/story/hackers-turn-amazon-echo-into-spy-bug/ (accessed on 16 September 2021).

Halevi, T., Lin, S., Ma, D., Prasad, A. K., Saxena, N., Voris, J., & Xiang, T. (2019). Sensing-enabled defenses to rfid unauthorized reading and relay attacks without changing the usage model.

Haselsteiner, E., & Breitfuß, K. (2006). Security in near field communication (NFC). In *Workshop on RFID security* (pp. 12-14).

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.

He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal*, 2(1), 72-83.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), 527-542.

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.

Hilt, S., Kropotov, V., Mercês, F., Rosario, M., & Sancho, D. (2019). The internet of things in the cybercrime underground. *Trend Micro Research*.

Hossain, M. M., Fotouhi, M., and 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.

https://csrc.nist.gov/publications/detail/nistir/8259/final (https://www.mwe.com/insights/nist-guidance-on-internet-of-things/)

Hu, W., Tan, H., Corke, P., Shih, W. C., & Jha, S. (2010). Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks* (TOSN), 7(1), 1-25.

Huda, S., Yearwood, J., Hassan, M. M., & Almogren, A. (2018). Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Applied soft computing*, 71, 66-77.

Jain, A., & Singh, T. (2020). Security challenges and solutions of IoT ecosystem. In *Information and communication technology for sustainable development* (pp. 259-270). Springer, Singapore.

Jiang, X., Lora, M., & Chattopadhyay, S. (2020). An experimental analysis of security vulnerabilities in industrial IoT devices. *ACM Transactions on Internet Technology* (TOIT), 20(2), 1-24.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.

Kagita, M. K., Thilakarathne, N., Rajput, D. S., & Lanka, D. S. (2020). A Detail Study of Security and Privacy issues of Internet of Things. *arXiv preprint arXiv:2009.06341*.

Kamal, A. H. A., Yen, C. C. Y., Ping, M. H., & Zahra, F. (2020). Cybersecurity Issues and Challenges during Covid-19 Pandemic.

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.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2016). Enabling consumer trust upon acceptance of IoT technologies through security and privacy model. In *Advanced multimedia and ubiquitous engineering* (pp. 111-117). Springer, Singapore.

Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M. (2017). RFID security threats and basic solutions. In *RFID Security* (pp. 27-41). *Springe*r, Cham.

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IT Professional*, 19(5), 27-33.

Konduru, V. R., & Bharamagoudra, M. R. (2017). Challenges and solutions of interoperability on IoT: How far have we come in resolving the IoT interoperability issues. In *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (pp. 572-576). IEEE.

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, 141, 199-221.

Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. In *BODYNETS* (pp. 256-262).

Kremer, S., & Rønne, P. B. (2016). To du or not to du: A security analysis of du-vote. In 2016 *IEEE European Symposium on Security and Privacy* (EuroS&P) (pp. 473-486). IEEE.

Krishnamurthy, R., Rathee, G., & Jaglan, N. (2020). An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. *Wireless Networks*, 26(4), 2391-2402.

Kumar, K., Zindani, D., & Davim, J. P. (2019). *Industry 4.0: Developments Towards the Fourth Industrial Revolution*. Springer.

Kumar, S. A., Vealey, T., and Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions, 49th *Hawaii International Conference on System Sciences* (HICSS), IEEE, 5772–5781.

Lade, S., Shrivastav, P., Waghmare, S., Hon, S., Waghmode, S., & Teli, S. (2021). Simulation of Self Driving Car Using Deep Learning. In *2021 International Conference on Emerging Smart Computing and Informatics* (ESCI) (pp. 175-180). IEEE.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, 24(11), 770-772.

Lee, G. M., & Kim, J. Y. (2010). The Internet of Things—A problem statement. In 2010 *International Conference on Information and Communication Technology Convergence* (ICTC) (pp. 517-518). IEEE.

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).

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1-9.

Li, W., Logenthiran, T., Phan, V. T., & Woo, W. L. (2019). A novel smart energy theft system (SETS) for IoT-based smart home. *IEEE Internet of Things Journal*, 6(3), 5531-5539.

Liao, Y. P., & Hsiao, C. M. (2013). A secure ECC-based RFID authentication scheme using hybrid protocols. In *Advances in Intelligent Systems and Applications-Volume 2* (pp. 1-13). Springer, Berlin, Heidelberg.

Maarof, A., Senhadji, M., Labbi, Z., & Belkasmi, M. (2018). Authentication protocol for securing internet of things. In *Proceedings of the Fourth International Conference on Engineering & MIS* 2018 (pp. 1-7).

MacDermott, A., Baker, T., & Shi, Q. (2018). Iot forensics: Challenges for the ioa era. In 2018 9th IFIP *International Conference on New Technologies, Mobility and Security* (NTMS) (pp. 1-5). IEEE.

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.

Malina, L., Hajny, J., Fujdiak, R., and Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, 102, 83–95.

Maloney, M., Reilly, E., Siegel, M., & Falco, G. (2019). Cyber physical IoT device management using a lightweight agent. In *2019 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. 1009-1014). IEEE.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy, 2*(2), 155-184.

Meagher, L. (2018). Cybersecurity and Safety Concerns of Future Automated Vehicle Software (Doctoral dissertation, Utica College).

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018). Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT. In *2018 ieee international conference on pervasive computing and communications workshops* (percom workshops) (pp. 197-202). IEEE.

Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., ... & Baird, M. (2016). Distributed ledger technology in payments, clearing, and settlement.

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, 1, 1-13.

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.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, 12(5), 491-505.

Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems*, 100, 325-343.

Mukherjee, B., Wang, S., Lu, W., Neupane, R. L., Dunn, D., Ren, Y., ... & Calyam, P. (2018). Flexible IoT security middleware for end-to-end cloud–fog communication. *Future Generation Computer Systems*, *87*, 688-703.

Nappi, M., Ricciardi, S., & Tistarelli, M. (2016). Deceiving faces: when plastic surgery challenges face recognition. *Image and Vision Computing*, 54, 71-82.

Naumovski, T., & Taneski, N. (2019). Social engineering in the context of cyber security. In *10 th International scientific conference The great power influence on the security of small states* (Vol. 1, pp. 282-292). Univerzitet" Sv Kliment Ohridski" Bitola-Fakultet za bezbednost-Skopje.

Neuman, C., & Steiner, J. (1988). Authentication of unknown entities on an insecure network of untrusted workstations. In *Proceedings of the Usenix Workshop on Workstation Security* (Vol. 8, pp. 10-11).

Ng, J. (2019). Rethinking the cybersecurity of consumer Internet of Things (IoT): how to incentivise companies to produce cyber-secure consumer IoT products. Içinde Information Security Group-Royal Holloway University of London.

Nguyen, K. T., Laurent, M., and Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17–31.

O'Gorman, T. (2017). A Primer on IoT Security Risks. Pridobljeno iz Available at :https://securityintelligence. com/a-primer-on-iot-security-risks/(accessed 15 May, 2017).

O'Hara, P. M. (2019). *Internet of Things Risks in the Energy and Healthcare and Public Health Sectors of US Critical Infrastructure* (Doctoral dissertation, Utica College).

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.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited connections: a study of vulnerable devices on the internet of things (IoT). In *2014 IEEE joint intelligence and security informatics conference* (pp. 232-235). IEEE.

Pecchia, L., Piaggio, D., Maccaro, A., Formisano, C., & Iadanza, E. (2020). The inadequacy of regulatory frameworks in time of crisis and in low-resource settings: personal protective equipment and COVID-19. *Health and Technology*, 10(6), 1375-1383.

Perković, T., Damjanović, S., Šolić, P., Patrono, L., & Rodrigues, J. J. (2020). Meeting challenges in iot: Sensing, energy efficiency, and the implementation. In *Fourth International Congress on Information and Communication Technology* (pp. 419-430). Springer, Singapore.

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.

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.

Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters.*

Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1761-1804.

Rana, B., Singh, Y., & Singh, P. K. (2021). A systematic survey on internet of things: Energy efficiency and interoperability perspective. Transactions on Emerging Telecommunications Technologies, 32(8), e4166.

Rashid, B., & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of network and computer applications*, 60, 192-219.

Razzak, F. (2012). Spamming the Internet of Things: A possibility and its probable solution, *Procedia Computer Science*, 658–665.

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6), 383.

Rehman, S. U., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and privacy issues in IoT. *International journal of communication networks and information security*, 8(3), 147.

Renuka Venkata Ramani, C. (2016). Two-way Firewall for Internet of Things.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, 44(9), 51-58.

Roman, R., Rios, R., Onieva, J. A., & Lopez, J. (2018). Immune system for the Internet of Things using edge technologies. *IEEE Internet of Things Journal*, 6(3), 4774-4781.

Roman, R., Zhou, J., and Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, 57(10), 2266–2279.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117-2135.

Sadeghi, A.-R., Wachsmann, C., and Waidner, M. (2015). Security and privacy challenges in industrial internet of things, *Proceedings of the 52nd Annual Design Automation Conferenc*e on – DAC ’15, 1–6.

Saeed, I. A., Selamat, A., & Abuagoub, A. M. (2013). A survey on malware and malware detection systems. *International Journal of Computer Applications*, 67(16).

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, 1375-1384.

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).

San, C. (2018). Faxploit: New Check Point Research Reveals How Criminals Can Target Company & Private Fax Machines to Take Over Networks and Spread Malware. Available online: https://www.checkpoint.com/press/2018/faxploit-new-check-point-research-reveals-criminals-can-target-company-private-fax-machines-take-networks-spread-malware/ (accessed on 16 September 2021).

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, 12(17), 7002.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, 4(2), 118-137.

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, *83*, 326-337.

Shahzad, M., & Singh, M. P. (2017). Continuous authentication and authorization for the internet of things. *IEEE Internet Computing*, 21(2), 86-90.

Shepard, K., Wing, B., Miles, C., & Blackburn, D. (2006). Iris Recognition-National Science and Technology Council (NSTC)–Committee on Technology–Committee on Homeland and National Security–Subcommittee on Biometrics (EUA), last updated 31 march 2006.

Shi, Q., Dong, B., He, T., Sun, Z., Zhu, J., Zhang, Z., & Lee, C. (2020). Progress in wearable electronics/photonics—Moving toward the era of artificial intelligence and internet of things. *InfoMat*, *2*(6), 1131-1162.

Shone, N., Dobbins, C., Hurst, W., & Shi, Q. (2015). Digital memories based mobile user authentication for IoT. In 2015 *IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* (pp. 1796-1802). IEEE.

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, *179*, 107345.

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.

Sicari, S., Rizzardi, A., Grieco, L. A., Piro, G., & Coen-Porisini, A. (2017). A policy enforcement framework for Internet of Things applications in the smart health. Smart Health, 3, 39-74.

Singh Lallie, H., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *arXiv* e-prints, arXiv-2006.

Snoeren, A. C., & Balakrishnan, H. (2000). An end-to-end approach to host mobility. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 155-166).

Sompolinsky, Y., & Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 507-527). Springer, Berlin, Heidelberg.

Srinivasan, C. R., Rajesh, B., Saikalyan, P., Premsagar, K., & Yadav, E. S. (2019). A review on the different types of Internet of Things (IoT). *Journal of Advanced Research in Dynamical and Control Systems*, 11(1), 154-158.

Steinberg, J., & Speed, T. (2005). SSL VPN: Understanding, evaluating, and planning secure, web-based remote access. *Packet Publishing Ltd*.

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.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Stuurman, K., & Kamara, I. (2016). IoT Standardization-The Approach in the Field of Data Protection as a Model for Ensuring Compliance of IoT Applications. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshop*s (FiCloudW) (pp. 336-341). IEEE.

Suchitra, C., & Vandana, C. P. (2016). Internet of things and security issues. *International Journal of Computer Science and Mobile Computing*, 5(1), 133-139.

Suo, H., Wan, J., Zou, C., and Liu, J. (2012). Security in the Internet of Things: A Review. *International Conference on Computer Science and Electronics Engineering*, IEEE, 648–651.

Surya, L. (2016). Security challenges and strategies for the IoT in cloud computing. *International Journal of Innovations in Engineering Research and Technolog*y ISSN, 2394-3696.

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems*, *108*, 909-920.

Thilakarathne, N. N. (2020). Security and privacy issues in iot environment. *International Journal of Engineering and Management Research*, 10.

Torres, N., Pinto, P., & Lopes, S. I. (2021). Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem. *Applied Sciences*, 11(7), 3176.

Tu, Y. J., & Piramuthu, S. (2007). RFID distance bounding protocols. In *First International EURASIP Workshop on RFID Technology* (pp. 67-68).

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.

Verma, R. S., Chandavarkar, B. R., & Nazareth, P. (2019). Mitigation of hard-coded credentials related attacks using QR code and secured web service for IoT. In *2019 10th International Conference on Computing, Communication and Networking Technologies* (ICCCNT) (pp. 1-5). IEEE.

Visoottiviseth, V., Sakarin, P., Thongwilai, J., & Choobanjong, T. (2020). Signature-based and Behavior-based Attack Detection with Machine Learning for Home IoT Devices. In *2020 IEEE Region 10 Conference (TENCON)* (pp. 829-834). IEEE.

Vittori, P. (2019). Ultimate password: is voice the best biometric to beat hackers? *Biometric Technology Today*, 2019(9), 8-10.

Wang, H., Zhang, Z., & Taleb, T. (2018). Special issue on security and privacy of IoT. *World Wide Web*, 21(1), 1-6.

Weber, R. H. (2009). Internet of things–Need for a new legal environment? *Computer law & security review*, *25*(6), 522-527.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, 26(1), 23-30.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In *Security in pervasive computing* (pp. 201-212). Springer, Berlin, Heidelberg.

Wu, Y., Bao, W. S., Cao, S., Chen, F., Chen, M. C., Chen, X., ... & Pan, J. W. (2021). Strong quantum computational advantage using a superconducting quantum processor. *arXiv preprint* arXiv:2106.14734.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. In *2016 21st Asia and South Pacific Design Automation Conference* (ASP-DAC) (pp. 519-524). IEEE.

Xiong, J., Ma, R., Chen, L., Tian, Y., Li, Q., Liu, X., & Yao, Z. (2019). A personalized privacy protection framework for mobile crowdsensing in IIoT. *IEEE Transactions on Industrial Informatics*, 16(6), 4231-4241.

Yang, A., Zhuang, Y., & Wong, D. S. (2012). An efficient single-slow-phase mutually authenticated RFID distance bounding protocol with tag privacy. In *International Conference on Information and Communications Security* (pp. 285-292). Springer, Berlin, Heidelberg.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250-1258.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 129, 444-458.

Yeh, T. C., Wang, Y. J., Kuo, T. C., & Wang, S. S. (2010). Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert systems with applications*, *37*(12), 7678-7683.

Yin, C., Xi, J., Sun, R., & Wang, J. (2017). Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8), 3628-3636.

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices, *Proceedings of the 14th ACM Workshop on Hot Topics in Networks – HotNets-XIV*, ACM Press, 1–7.

Yu, Y., Guo, L., Liu, S., Zheng, J., & Wang, H. (2020). Privacy protection scheme based on CP-ABE in crowdsourcing-IoT for smart ocean. *IEEE Internet of Things Journal*, 7(10), 10061-10071.

Zaidi, S., Atiquzzaman, M., & Calafate, C. T. (2020). Internet of Flying Things (IoFT): A survey. *Computer Communications*.

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.

Zeng, K., & Li, Z. (2020). Best Practices in Cybersecurity for Utilities: Secure Remote Access.

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).

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).

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 230-234). IEEE.

Zheng, L., Zhang, H., Han, W., Zhou, X., He, J., Zhang, Z., ... & Wang, J. (2011). Technologies, applications, and governance in the internet of things. *Internet of things-Global technological and societal trends. From smart environments and spaces to green ICT*.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375.

Zhong, R. Y., & Ge, W. (2018). Internet of things enabled manufacturing: a review. International *Journal of Agile Systems and Management*, 11(2), 126-154.

Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010). Iot gateway: Bridgingwireless sensor networks into internet of things. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (pp. 347-352). IEEE.

Abiodun Esther Omolara 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.

Abdullah Alabdulatif is Assistant Professor of Computer Department, College of Sciences and Arts, Qassim University. He graduated from Qassim university, Saudi Arabia in 2004. received a bachelor of computer Science degree. Then entered Newcastle University, UK and received a master of computer security and resilience degree in 2009 and PhD in information security from Nottingham Trent University in 2014. He has a number of research papers in referred international journals and conferences. He is interesting research in Academic & Research includes Wireless security, IoT security, Blockchain Security.

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.

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.

Abdulatif Alabdulatif is an Assistant Professor in the College of Computer, Qassim University, Saudi Arabia. He received the Ph.D. degree in Computer Science from RMIT University, Australia. He received his M.Sc. degree in Computer Science from the same university. His research interests include applied cryptography, cloud computing, and data mining.

His research interests include artificial intelligence, machine learning, information retrieval, VOIP, and wireless networks.

Wafa' Hamdan Alshoura received her BSc degree from Al- Zaytoonah University, Jordan in 2012 and MSc degree in Computer Science from Al-Zaytoonah University in 2017. She is currently a PhD student in the School of Computer Sciences, University Sains Malaysia. Her research interests include digital watermarking and hash function.

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.