**JOSEPH CHAT AYUBA**

**BU/22C/PGS/7636**

**BAZE UNIVERSITY**

**TOPIC: VULNERABILITIES IN INTERNET OF THINGS (IoT): A CYBER-SECURITY GUIDE**

**CHAPTER ONE**

**INTRODUCTION**

* 1. **Background to the Study**

The emergence of the Internet of Things (IoT) represents a notable advancement within the realm of communication technology. According to Leloglu (2017), the term "Internet of Things" refers to the interconnections of computing devices that are embedded in physical objects, enabling the collection and exchange of data. There exists a vast multitude of wirelessly connected devices, numbering in the billions. Distributed, grid, and vehicular networks represent a subset of the diverse range of devices, infrastructure, and applications that stand to gain advantages from the implementation of the Internet of Things. The Internet of Things (IoT) employs a combination of sensors, processors, and communication hardware to acquire data from the physical environment. Subsequently, these data are subjected to various operations (Dean & Agyeman, 2018). The Internet of Things (IoT) refers to a comprehensive and continuously expanding network of interconnected computing devices that possess the ability to perceive and react to their physical environment. Numerous enterprises often fail to recognize the extent of their utilization of Internet of Things (IoT) devices, thereby remaining unaware of the potential cybersecurity and privacy risks associated with such devices.

The phrase "Internet of Things" (IoT) is employed to denote the interconnected network of devices capable of autonomously collecting and exchanging data, as well as performing tasks, owing to their embedded software, processing capabilities, sensors, network connectivity, and other technological components. IoT devices utilize wireless protocols such as Bluetooth and Wi-Fi for inter-device communication. The aforementioned protocols facilitate the exchange of data between devices and their integration with diverse cloud platforms for the purposes of data storage and processing (Yadav & Vishwakarma, 2018). The emergence of the Internet of Things (IoT) has brought about the aspiration to achieve the highest level of automation in the computing era. The term "Internet of Things" (IoT) pertains to a network comprising interconnected wireless devices capable of autonomously exchanging data without requiring human intervention. In the context of the Internet of Things (IoT), peripheral devices establish connections with a central hub, which may be hosted in a cloud environment. Subsequently, these devices are programmed and accessed through the hub, aligning with the specific requirements of the user. The principal objective of the Internet of Things (IoT) is to enhance the efficiency and effectiveness of frequently utilized devices. The concept of the Internet of Things (IoT) was initially introduced and coined by Kevin Ashton in 1999. The proliferation of the Internet of Things (IoT) is steadily increasing as an increasing number of machines, sensors, and cameras are interconnected with the internet (Gupta, 2019).

The Internet of Things (IoT) has emerged as one of the most cutting-edge technologies currently available, according to recent research by Radanliev, De Roure, Maple, Nurse, Nicolescu, and Ani (2019). The Internet of Things (IoT) refers to a network of physical devices that are interconnected and capable of communicating with each other via the Internet. This term refers to computers that are capable of sensing, collecting, and transmitting information while being connected to the internet. The Internet of Things (IoT) has a wide range of applications, one of which is the remote management of appliances (Choudhary, Umamaheswari, & Kumawat, 2021). The Internet of Things (IoT) enables the connectivity of various objects to the internet. The Internet of Things (IoT) is poised to have a profound impact on our societal norms and daily routines. Currently, the industry is experiencing significant growth and success. According to analysts, there is a projected acceleration in the growth of Internet of Things (IoT) products and services in the foreseeable future. The term "Internet of Things" (IoT) pertains to a collection of interconnected devices that have the ability to exchange and receive data over a network autonomously, without the need for human involvement. Given the widespread adoption of the Internet of Things (IoT), it is imperative that connected devices provide adequate security measures. In the present era, the imperative to develop a secure device has become increasingly paramount due to the substantial amount of personal data that is stored in digital form. The primary focus in any system is the protection of data due to the increased susceptibility of internet-enabled devices to hacking (Choudhary, Umamaheswari, & Kumawat, 2021).

The complex nature and wide range of technology and data that IoT systems use present security challenges (Lee, 2020). The expeditious resolution of security issues on the Internet of Things is imperative. In an Internet of Things (IoT) environment, ensuring the security of data and services necessitates the incorporation of fundamental features such as confidentiality, accuracy, completeness, authentication, access control, availability, and privacy. In the realm of cybersecurity, the Internet of Things (IoT) possesses distinctive idiosyncrasies and limitations. Consequently, there is a continuous emergence of novel attacks and threats pertaining to the Internet of Things (IoT) on a daily basis (Kandasamy, Srinivas, Achuthan, & Rangan, 2020). Hence, it is imperative that we acquire a comprehensive comprehension of the hazards presented by this technology and formulate strategies to mitigate them. It is imperative to possess a comprehensive understanding of the diverse manifestations of attacks and the corresponding strategies employed to mitigate them. The frequency and severity of cybersecurity attacks targeting Internet of Things (IoT) systems are on the rise, leading to a multitude of challenges for both individuals and businesses.

Vulnerabilities refer to inherent weaknesses present in a system or its design that can be manipulated by an unauthorized individual to illicitly obtain access to information, compromise the system's integrity, or initiate a denial-of-service attack (Skarmeta, 2015). The IoT infrastructure presents numerous potential vulnerabilities that can be exploited by hackers. According to Kizza (2013), vulnerabilities can exist within the hardware, software, policies, procedures, and user components of a system. The proliferation of Internet of Things (IoT) technologies, such as smart grids, patient monitoring systems, the industry, environmental monitoring, smart manufacturing, and smart logistics, has resulted in a rise in cyber attacks. The complexity of ensuring security in the Internet of Things (IoT) arises from the dynamic and ever-changing nature of device connections, the diverse range of actors involved in IoT systems, and the limited availability of resources (Pahlevanzadeh, Koleini, & Fadilah, 2021).

Premised on the foregoing, this study seeks to investigate vulnerabilities in internet of things (IOT) using cyber-security as a guide. In ensuring this, the study will examine major vulnerabilities associated with internet of things, investigate ways through which IOT vulnerabilities has affected the safety of vital information resources and data of institutions in the Nigerian b indnkingustry; and investigate cyber-security strategies adopted by educational firms to address vulnerabilities associated with internet of things.

* 1. **Statement of Problem**

There are several factors that contribute to the heightened susceptibility of Internet of Things (IoT) applications to security vulnerabilities in comparison to traditional computer systems. Firstly, it is important to note that there is a diverse array of Internet of Things (IoT) devices, platforms, communication channels, and protocols available for selection. Furthermore, it should be noted that Internet of Things (IoT) systems are not primarily intended for online interaction. Instead, their main purpose is to establish connections between different physical networks through the utilization of interconnected "things." Furthermore, due to the mobility of users and devices, Internet of Things (IoT) systems exhibit a perpetual state of evolution and possess limited delineations. Ensuring the security of the Internet of Things (IoT) against potential cyber threats poses significant challenges. To begin, it is imperative for Internet of Things (IoT) devices to possess the capability to accommodate an extensive range of protocols, standards, and operating environments. Administrators will encounter heightened challenges in safeguarding these entities from potential assailants (Restuccia, D'Oro, & Melodla, 2018). Furthermore, it should be noted that not all Internet of Things (IoT) devices will derive equal advantages from a uniform security solution. Consequently, there is no universally effective solution for safeguarding the Internet of Things.

According to Restuccia, D'Oro, and Melodla (2018), the implementation of security countermeasures on IoT devices poses a significant challenge due to the reliance on computationally intensive algorithms and protocols with high overhead. Wireless security attacks, such as eavesdropping, denial of service, spoofing, message injection, and jamming, pose significant concerns for the Internet of Things (IoT) due to its distributed nature and heavy reliance on wireless data transmission. Consequently, this study aims to investigate vulnerabilities in internet of things (IOT) using cyber-security as a guide.

* 1. **Research Questions**

The following questions are stated to guide the study

1. What are the major vulnerabilities associated with internet of things (IOT) in websites of an educational institution?
2. In what way(s) has IOT vulnerabilities affected the safety of vital information resources and data of educational institution?
3. What are the cyber-security strategies adopted by educational institutions to checkmate or address vulnerabilities associated with internet of things of educational institution?
4. How effective are cyber-security strategies adopted by educational institutions to address vulnerabilities associated with internet of things of educational institution?

* 1. **Aim and Objective of the Study**

The main objective of this research is to investigate vulnerabilities in internet of things (IOT) using cyber security as a guide. Specifically, the objectives of the study are as follows

1. To examine major vulnerabilities associated with internet of things (IOT) in the educational sector.
2. To investigate ways through which IOT vulnerabilities has affected the safety of vital information resources and data of institutions in the educational sector.
3. To investigate cyber-security strategies adopted by educational firms to address vulnerabilities associated with internet of things.
   1. **Research Hypothesis**

The following hypothesis are stated

H01: Vulnerabilities associated with IOT has significantly affected safety of information in the educational sector.

H02: Cyber-security strategies adopted by educational institutions to address vulnerabilities associated with IOT in the educational sector.

* 1. **Significance of the Study**

The results of this study are expected to contribute to a better understanding of the characteristics and extent of the risks presented by both institutional and espionage-related actors. In order to ascertain the invulnerability of the security solution against malicious attacks, it is imperative to initially identify the potential threats to the system as well as the inherent vulnerabilities within the system. This research is centered on the examination of cyber-security risks and issues within the context of the Internet of Things (IoT). The primary objectives of this study are twofold: (1) to identify and analyze the diverse threats and vulnerabilities that emerge in the IoT domain, thereby pinpointing the associated risks and issues; and (2) to compile the countermeasures and solutions proposed by scholars and authorities to address these risks and issues. These countermeasures encompass both technical approaches and the implementation of security policies. The outcome of this research is expected to be of relevance to educational institutions, governments and IoT developers as it will aid in coming up with cyber-security strategies to address vulnerabilities associated with IOT.

* 1. **Scope of the Study**

This study focused on investigating the vulnerabilities in Internet of Things (IOT) using cyber-security as a guide. The research will focus on websites of educational institutions in Nigeria due to numerous trend of attacks on information facilities and resources of these institutions. For the purpose of this study, an educational institution BAZE University, Nigeria will be focused upon.

* 1. **Limitation of study**

The limitations expected to be encountered in this research is easy accessibility to the educational organization preferred for this study. However, the researcher will explore all options in ensuring that the objectives stated by this study are achieved.

**1.9 Organization of the Study**

The present study will be structured into five distinct chapters. The first chapter of this thesis will provide an introduction to the topic and present the statement of the problem. The document also delineated the study's aims, research inquiries, significance, and structure. Chapter two will present the review of related literature, while chapter three will discuss the methodology of the study. Chapter four will focus on the presentation, analysis, and discussion of data. Chapter five of this research paper will provide a comprehensive overview of the key findings and outcomes derived from the study. Additionally, it will present a concise summary of the research, followed by a well-supported conclusion. Finally, this chapter will offer valuable recommendations based on the research findings, which can serve as practical guidelines for future endeavors in this field.

**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Conceptual Review**

**2.1.1 Internet of Things (IOTs)**

The Internet of Things (IoT) is a system that consists of interconnected computing devices, individuals, connected objects, sophisticated machinery, data, and information. The components possess distinct identification and can transmit information over a network autonomously without requiring human involvement (Prakash et al., 2020). The Internet of Things (IoT) refers to the integration of internet connectivity, computational capabilities, electronic components, applications, power sources, sensors, actuators, and control systems into physical devices. These components enable devices to communicate, generate, collect, exchange, and consume data with minimal human intervention. Rajmohan et al. (2020) presented a concise definition of an IoT system as a network of entities that participate in the exchange of information and interact with the physical world through the processes of sensing, information processing, and actuation.

The Internet of Things (IoT), as defined by ENISA (2017), is a system of interconnected sensors and actuators that form a cyber-physical ecosystem and enable decision-making. The Internet of Things (IoT) is now an essential technology in modern society, with significant implications for cybersecurity. The prevalence of IoT devices is extensive, as they are interconnected and often lacking in essential security measures, making them vulnerable to various cyber threats. Opponents possess the capacity to exploit these vulnerabilities with the aim of obtaining sensitive data, launching distributed denial-of-service (DDoS) attacks, and potentially gaining control over critical infrastructure (Mazumdar, Roy, Nag, & Singh, 2022). A colossal cyberattack on Internet of Things (IoT) networks could lead to severe consequences, including the disruption of crucial services and the infliction of substantial economic damage.

The Internet of Things (IoT) is a complex network comprising interconnected devices and individuals collaborating to monitor and exchange information about their usage and environmental conditions. The system consists of intelligent devices that are equipped with embedded systems, which include central processing units (CPUs), sensors, and connectivity hardware. These devices gather, transmit, and react to information acquired from their environment within the Internet of Things (IoT) ecosystem. IoT devices establish communication with an IoT gateway or another edge device to facilitate the exchange of sensor data between them (Akhtar & Feng, 2022). The data can be either sent to the cloud for analysis or processed locally. These devices periodically exchange information and react accordingly. Generally, Internet of Things (IoT) devices function autonomously without necessitating human intervention. The Internet of Things (IoT) is a rapidly expanding field that poses unique challenges in terms of device compatibility, protection of data privacy, and security (Kareem, Aborisade, Onashoga, Sutikno, and Olayiwola, 2023).

The Internet of Things (IoT) improves individuals' efficiency in both their personal and professional lives while also giving them greater control and power over their own lives. Businesses rely extensively on the Internet of Things (IoT) because it offers technological devices that facilitate the automation of corporate environments. Organisations can optimise processes and reduce labour costs by utilising IoT technology to obtain real-time and precise information about the operations of various systems. Furthermore, the Internet of Things (IoT) provides a transparent perspective on business transactions, reduces costs associated with manufacturing and shipping, and enhances the efficiency of services. These applications provide practical and useful information to corporate users through user interfaces (Zeng et al., 2022).

**2.1.2 Internet of Things (IOTs) Vulnerabilities**

The term "vulnerability" refers to a flaw in a systemic asset that a person can exploit for their own benefit. A backdoor is a covert method used to gain unauthorized access to a location or system, typically without the knowledge or consent of the owner. This activity can be more precisely described as an act of trespass or encroachment on assets, which involves gaining access to the victim's systems, including hardware, software, and established procedures (ENISA, 2017). If vulnerabilities were completely absent, systems would be impervious to harm, and there would be no necessity for security measures. In the present digital environment, characterized by the widespread use of smart devices and the growing frequency of interactions between individuals and objects, a new domain has arisen for cybercriminals to take advantage of.

Cybercriminals are diligently and actively seeking vulnerabilities in products and procedures that manufacturers or developers may have inadvertently neglected. The presence of these vulnerabilities facilitates convenient entry to the product, enabling cybercriminals to acquire complete authority not only over the product itself but also over the entire hosting ecosystem (Prakash & Saini, 2020). When examining these vulnerabilities, it is essential to take into account the interconnectivity of the Internet of Things (IoT). This suggests that the different parts of the Internet of Things (IoT) should not be considered separately but rather as a cohesive whole made up of different components. Researchers have conducted numerous studies to ascertain the fundamental causes of exploiting Internet of Things (IoT) systems and rectify the shortcomings of IoT design (Wheelus & Zhu, 2020). The main weakness identified through analysis is the existence of a remarkably large attack surface.

With billions of devices worldwide, malicious users have a vast array of targets to test their hacking abilities. This enhances their likelihood of discovering numerous security vulnerabilities and attaining unauthorized entry to these devices (Stergiou, Plageras, Psannis, & Gupta, 2019). Moreover, the substantial abundance of these "objects" disseminated worldwide renders them exceedingly enticing objectives. This attribute enhances the probability of creating extensive multinational armies composed of zombie device soldiers, which can be readily employed to execute further assaults (Stergiou, Psannis, Kim, & Gupta, 2018). Furthermore, the extensive integration of the Internet of Things (IoT) into critical infrastructures offers further motivation for potential attacks. These infrastructures, such as power grids, water supply networks, defense systems, airports, and others, possess considerable importance in our society. Any effective assault on these systems can significantly affect economies and the operational capacities of adversary parties during periods of warfare (NSFOCUS, Inc., 2019).

The Internet of Things (IoT) is an intricate ecosystem comprising a wide range of components, including individuals, devices, gateways, services, and networks. These elements exhibit distinct designs, functionalities, and implementations in the environment and are deployed within the interconnected ecosystem. The wide range of differences in IoT hardware and software presents significant challenges, causing severe problems that adversely affect the entire IoT landscape (Millar, 2021). Embedded systems make "things" highly prevalent and widespread. These systems are autonomous and standalone devices that are directly linked to the cloud via the internet. These devices are often found in demanding environments, which exacerbates the accumulation of significant problems that need to be addressed. Unlike traditional hardware equipment, which is usually located in secure data centers with strong physical security measures such as firewalls, segregated access, and guards, many IoT devices are deployed in remote and exposed locations (Millar, 2021).

The absence of tamper-resistant packaging in these devices makes them vulnerable to physical tampering by attackers, as their physical security is weak (ENISA, 2021). Furthermore, these devices are meticulously crafted with a distinct objective in mind and precisely engineered to execute specific tasks with optimal efficiency. In order to maximize efficiency, IoT devices are designed with minimal complexity. Moreover, manufacturers primarily focus on ensuring that these products are affordable for consumers while also maximizing their own profitability during the production process. Consequently, these "things" frequently possess multiple restrictions in their hardware and software constituents (James, 2019).

The energy supply of most Internet of Things products is not derived from the power grid. Rather, they are frequently made to be portable electronics that run on internal batteries (Abdalla & Varol, 2020). In order to overcome this problem, low-power components like CPUs and peripherals with slower clock rates must be used to offset the limited power supply. Processing power levels that are inadequate to support computationally demanding algorithms for cryptographic services are the result of this limitation. Moreover, memory is one area in which the hardware of "things" is limited. These devices cannot run multiple software programs, such as cryptographic algorithms, that need a large amount of free volatile memory due to their limited memory capacity. They can therefore only carry out their primary duties and refrain from using other software features (Malche, Maheshwary, & Kumar, 2020).

To elaborate on the notion of "memory," it is critical to recognize the dearth of sufficient non-volatile memory, or storage. No matter what storage choices are offered for these entry-level gadgets, it is always a serious issue that needs to be considered. This is due to the fact that their storage capacity is insufficient to match the large-scale local data storage capabilities of conventional information systems. When these devices' storage capacities cannot be increased in any way—by adding new memory or swapping out the old one—the problem gets more and more problematic. The gadgets become outdated as a result (Sharma & Pippal, 2020). There are many different kinds of software vulnerabilities that require attention. These problems stem from flaws in the process of developing software as well as in following the right protocols. The operating system itself is the main drawback when it comes to IoT devices. These operating systems are made to be simple and light to fit the devices' constrained hardware capabilities. But as a result, there are noticeably fewer security elements and features. It's also critical to recognize that the system lacks sufficient security configurability, which limits it to preset security settings and, in the end, makes it unable to adequately defend against new threats (Ahmed, Islam, Ashraf, Chowdhury, & Rahman, 2020).

Many defects can be found in IoT systems when they are examined, particularly in the software limitations' design. Due to the IoT market's explosive growth and intense pressure to release products quickly, extensive software design methodologies and beta testing are frequently neglected. Poorly written applications are therefore being used, which makes it more difficult to implement security and privacy by design procedures. In the end, this results in products having software vulnerabilities (Srivastava & Prakash, 2020). Despite unsafe programming, missing updates and security patches are the main cause of serious vulnerabilities in IoT devices, which anyone can exploit. Even the least experienced person with a basic understanding of programming languages, network security, and system penetration techniques can easily exploit these well-known vulnerabilities, which act as backdoors for the global security community. Anyone can easily gain access to the system by following the published guidelines for taking advantage of outdated software (Victorian Government Directory, 2020).

The operating system that is presently being used or the web interfaces of the devices that act as the interactive frontend for users are examples of common paradigms. From the manufacturers' perspective, patching and updating IoT devices is a challenging and intricate process. Even in the event that updates and patches are produced, it is difficult because of the products' insufficient default updating mechanisms, the variety of products with notable code differences, and the costly operations necessary for these updating processes (ENISA, 2019). Endpoints within the Internet of Things ecosystem depend on other services in the event of compromised software. The mobile frontends, which are always linked to the intelligent "things," provide access to the aforementioned services. The Internet of Things (IoT) as a whole has a serious security flaw because of these end-user applications. Because they have complete access to the device—something that has always been granted in the past—they give attackers a weak point of entry. Furthermore, the fronted application may be viewed as a single point of failure if numerous "things" with full access rights are linked to this unsecure mobile interface. HKCERT (2020).

A serious vulnerability exists when a lot of devices are hosted in an IoT ecosystem and an attacker manages to obtain unauthorized access to the insecure cloud services interface. Malicious actors may be able to take full control of the Internet of Things (IoT) network in addition to stealing individual devices through unauthorized access to cloud services. The serious consequences worsen when the information collected by the "things" is combined into this hacked cloud service, where it becomes available to unauthorized users (Stergiou, Bompoli, & Psannis, 2023). There is another possible weakness in IoT ecosystems that is highlighted, and it has to do with privacy issues. Unfortunately, a lot of organizations collect too much data, and even when that extra data is required for specific reasons, it is still not sufficiently protected against data breaches or leaks. In addition to the limitations imposed by software and hardware, it is crucial to acknowledge that network-based constraints can also function as major vulnerabilities (Sharma & Pippal, 2020).

For the Internet of Things (IoT) to work and provide its extra benefits, all entities need to be connected to the IoT ecosystem and to each other. Although connectivity is necessary, there are a number of risks associated with it because networks are vulnerable. The security of the network link directly relates to the degree of security in the data flow between devices. The system as a whole could be compromised if the link is compromised. Data compromise is more likely when there is no encryption or integrity verification in place during communication between IoT nodes. This is due to the fact that the data is sent in a human-readable format and that no safeguards are in place to identify any unauthorized changes. Inadequate authorization or authentication for intermediate network devices as well as end nodes increases the risk (Abdullah, Kaur, & Biswas, 2018). Compared to wired installations, which usually have physical security measures in place to protect the network medium, such as the use of wired connections, wireless communications are more susceptible to cyberattacks. Ray and Bagwari (2020) have highlighted that vulnerabilities in IoT devices are not restricted to software and hardware implementation but also extend to procedures.

**2.1.3 Internet of Things Devices and Services**

IoT devices are tangible entities that facilitate the integration of an entity into the digital domain (De, Barnaghi, Bauer, & Meissner, 2011). A smart object refers to a wide range of interconnected items, including household appliances, medical devices, automobiles, structures, factories, and other objects equipped with sensors and embedded computers. These objects collect data about their environment. An Internet of Things (IoT) device possesses the capability to establish communication with other IoT devices and information and communication technology (ICT) systems. These devices employ diverse communication protocols, including cellular networks (3G or LTE), WLAN, wireless, or other technologies (Taneja, 2013). The categorization of IoT devices is based on various criteria, such as their dimensions (small or standard), mobility (mobile or stationary), power supply (external or internal), connectivity (intermittent or constant), automation (automated or non-automated), nature (logical or physical entities), and whether they possess IP capabilities or not. The key characteristics of IoT devices encompass their capability for actuation and/or sensing, the capacity to regulate power and energy consumption, integration with the physical environment, intermittent connectivity, and mobility (Koien & Oleshchuk, 2013).

Certain services must exhibit a combination of rapidity and dependability while also providing reliable safeguards for security and privacy. On the other hand, there could be other services that lack these characteristics (Gluhak & Krco, 2011). Certain devices are equipped with physical safeguards, whereas others operate without supervision. Devices in IoT environments must be protected against any possible threats that could jeopardize their functionality. The majority of Internet of Things (IoT) devices are vulnerable to both external and internal attacks due to their inherent characteristics (Anwar, Zainal, Abdullah, & Iqbal, 2020). Implementing and utilizing a strong security mechanism in IoT is challenging due to constraints in computational capabilities, memory capacity, and battery power. An IoT service, as defined by Thomas et al. (2012), is a transaction that takes place between two entities: the service provider and the service consumer. A designated function is accountable for facilitating interaction with the tangible realm. This can be accomplished by assessing the condition of entities or by instigating actions that will result in a modification of the entities. A service provides a well-defined and standardized interface that offers all the essential functionalities for interacting with entities and their associated processes. Services facilitate the utilization of a device's capabilities by interacting with the resources it offers (De, Barnaghi, Bauer, & Meissner, 2011).

**2.1.4 Threats in Internet of Things (IOTs) Security**

Vulnerabilities pertain to weaknesses or imperfections in a system's security, while threats are actions or procedures that raise the probability of an unfavorable incident occurring. According to Ayed, Taveras, and Younes (2020), these procedures entail the exploitation of vulnerabilities, which are defined as flaws in the system that leave it open to malevolent acts by a hostile actor. The possible effects of IoT deployments on security, privacy, and general physical safety are the main issues and dangers. Attacks on Internet of Things (IoT) devices can have far-reaching effects because even one compromised device can lead to larger attacks and be used to target vital infrastructure. The extensive usage of IoT in a variety of settings and activities makes this especially worrisome (Anwar, Zainal, Abdullah, & Iqbal, 2020).

**Brute force attack:** The attacker employs a straightforward method in this type of attack, aiming to gain unauthorized access to the system, either through the frontend or backend of a node. The attacker achieves this by systematically trying all possible combinations of credentials. Initially, the process involves inputting the commonly used or default credentials, as users often choose easily guessable passwords or neglect to modify the default ones (Wheelus & Zhu, 2020).

**Calibration Parameters Tampering attack**: The adversary in this attack manipulates the configuration parameters of sensors and actuators to intentionally misalign their calibration. This results in falsified measurements from the sensors and altered interactions of the actuators with their environment (Wustrich, Pahl & Liebald, 2020).

**Cryptanalysis attack:** It refers to acts of aggression resulting from human actions, such as theft, bomb attacks, vandalism, and so on, can render IoT devices unavailable due to their destruction or sabotage. In many instances, this can also result in various malfunctions within the entire IoT ecosystem. For example, if the sabotage targets IoT sensors, it may lead to incomplete measurements. The attacker in these instances does not need any prior knowledge of the IoT system in order to carry out their malicious actions (Bhagyashri Bhandari & Jareena, 2020).

**DoS / DDoS attack:** Distributed Denial of Service, or DDoS, is a kind of attack that developed from DoS attacks. A DDoS attack uses multiple sources, as the term "Distributed" implies, whereas a DoS attack only uses one source. The goal of DoS and DDoS attacks is to take over the resources of a system or infrastructure. A denial-of-service (DoS) attack occurs when a single origin overloads the system, resulting in a crash or rendering it inaccessible to authorized users. A DDoS attack involves several origins cooperating to accomplish a common goal. These attacks overwhelm the system or network by sending more false or fictitious requests than it can handle, thereby exceeding its capacity for normal traffic. This results in a halt or crashed state of the system or network, as it is unable to process valid requests from authorized users (Ayed, Taveras & Younes, 2020).

**Network Disruption:** Unintentional or intentional communication failures will cause the Internet of Things network to collapse and prevent it from serving its intended purpose. This threat, which originates from outside the network from things like failing power supplies and deteriorating wires, has the potential to do a great deal of damage, from high to critical. The evaluation considers both the duration of the recovery period and the significance of the network segment. (ENISA, 2017).

**Node tampering**: The attackers have the ability to physically capture the node, which can be either an end device or an intermediate device like a gateway, regardless of whether it is visible in the surroundings. This threat has the potential to generate additional threats and could serve as the origin of attacks on the entire Internet of Things (IoT) ecosystem, or the disclosure of sensitive information (ENISA, 2017).

**Replay Attack:** The goal of this attack, which affects both the software and hardware components, is to methodically find flaws and vulnerabilities in order to take advantage of them and possibly spark additional attacks. Reverse engineering, put simply, is the process of understanding a system's internal workings by studying it backwards, starting from the output of the system (ENISA, 2017).

**Reverse Engineering:** The adversary intercepts a genuine transmission, stores it, and then resends it to demonstrate that they are the legitimate node. By posing as a real sender, this is done with the goal of deceitfully influencing the target's response. It is not necessary to have deep knowledge of network mapping to execute this kind of attack. It is sufficient to just record and play back the message that was captured (ENISA, 2017).

**Sinkhole Attack:** This attack makes use of the routing protocol in use and is a classic form of network targeting. By sending bogus routing information, the compromised node entices neighboring nodes, greatly increasing network traffic. According to the routing protocol, it achieves this by offering an alluring link that promises incredibly low latency. Like water flowing into a sinkhole, all network packets are routed through the compromised node, where their data is intercepted and used to determine how to handle them (ENISA, 2017).

**2.2 Internet of Things (IOTs) Vulnerabilities**

Identifying the system assets, or parts, that make up the Internet of Things (IoT), is essential before addressing security threats. Understanding the asset inventory—which includes all Internet of Things (IoT) devices, components, and services—is essential. An economic resource that is owned by an entity and has value is referred to as an asset. According to Vermesan et al. (2011), the main parts of an Internet of things system are its hardware, which includes things like machinery and buildings, as well as its software, services, and data.

**2.2.1 Vulnerability**

According to Bertino et al. (2010), vulnerabilities are innate flaws or weaknesses in a system or its design that an unauthorized person can use to execute commands, obtain unauthorized access to data, or launch denial-of-service attacks that disrupt the system's availability. There are weaknesses in a number of IoT system components. In particular, vulnerabilities may appear in the software or hardware of the system, in the rules and guidelines that are used by the system, or even in the users of the system (Kizza, 2013). The two main parts of an Internet of Things system are its software and hardware, both of which often have design flaws. Finding hardware vulnerabilities is difficult, and even when one is found, resolving them can be equally difficult because of problems with hardware compatibility, interoperability, and the substantial work necessary to address them.

Vulnerabilities in software can be found in operating systems, application programs, and control programs like device drivers and communication protocols. There are several reasons why software design flaws occur, including human factors and software complexity. Human fallibility frequently leads to technical vulnerabilities. Not understanding the requirements can lead to a number of problems, such as starting the project without a plan, poor developer-user communication, a lack of resources, expertise, and knowledge, and the incapacity to manage and control the system (Kizza, 2013).

**2.2.2 Exposure**

An exposure refers to a flaw or error in the configuration of a system that enables an attacker to carry out activities aimed at gathering information. One of the most difficult problems in the field of Internet of Things (IoT) is ensuring the ability to withstand physical attacks. In the majority of Internet of Things (IoT) applications, devices are often left unattended and are susceptible to being placed in easily accessible locations for potential attackers. The aforementioned scenario increases the potential for an assailant to seize the device, extract cryptographic secrets, manipulate their programming, or substitute them with a malicious device under the attacker's command (Padmavathi & Shanmugapriya, 2009).

**2.2.3 Threats and Attack**

An action that takes advantage of weaknesses in a system and has unfavorable effects is considered a threat (Brauch, 2011). According to Rainer and Cegielski (2010), threats can originate from two primary sources: humans and nature. There is a chance that natural disasters like earthquakes, tropical storms, floods, and fires will seriously damage computer systems. It is impossible to totally prevent natural disasters from occurring, but there are certain precautions that can be taken. Plans for disaster recovery, which include backup and contingency plans, are the best ways to protect systems from natural disasters. Human threats are defined as risks posed by individuals, such as deliberate threats that come from both internal and external sources and are intended to cause harm or disruption to a system (Baybutt, 2002). The advent of the Internet of Things (IoT) has resulted in a notable surge in the quantity of widely used devices, raising concerns about security that affect the broader population. Unfortunately, a new set of security flaws is introduced by the Internet of Things (IoT). The vulnerability of the newest generation of computers, smartphones, and other devices to malware and possible attacks is becoming more widely acknowledged (Li & Lai, 2011).

Attacks are purposeful actions meant to damage a system or interfere with its regular operations by exploiting weaknesses using various methods and instruments. Attackers launch attacks with the goal of achieving targets, either for their own satisfaction or financial gain. Attack cost is the measurement of the effort needed by an attacker, accounting for their ability, resources, and drive (Bertino, 2010). Those who represent a serious risk to the digital sphere are known as adversarial actors (Schneier, 2011). They might be proficient hackers, participate in illegal activity, or even work for the government (Kizza, 2013). An attack can take many different forms. These include close-quarters attacks, insider exploitation, passive attacks, and active network attacks, which monitor unencrypted traffic to find sensitive information. Passive attacks, on the other hand, monitor unprotected network communications to decrypt weakly encrypted traffic and obtain authentication information (Bertino, 2010).

**2.3 Primary Security and Privacy Goals in Cyber-Security**

**Confidentiality:** Ensuring confidentiality is an essential element of security in the Internet of Things (IoT). Nevertheless, there are specific circumstances in which it may not be mandatory, especially when the data is readily available to the public (Lopez, et.al 2009). However, it is crucial that confidential information remains undisclosed and unread by unauthorized individuals in most situations and circumstances. Confidential information, such as patient records, proprietary business data, classified military information, security credentials, and secret encryption keys, must be protected from unauthorized access.

**Integrity:** Integrity is a crucial security attribute that is indispensable for guaranteeing the dependability of services offered to IoT users in the majority of situations. Internet of Things (IoT) systems display a wide range of integrity requirements (Jung, et.al 2001). For instance, a remote patient monitoring system will utilize strong integrity checks to reduce the impact of random errors, which have the potential to undermine the accuracy of the information. Communication can potentially lead to loss of human lives due to data loss or manipulation (Schneier, 2011).

**Authentication and Authorization:** The extensive connectivity of the Internet of Things (IoT) amplifies the problem of authentication because of the unique features of IoT environments, where communication can take place between devices (M2M), humans and devices, and/or humans and humans. Different systems necessitate unique solutions due to varying authentication requirements. Some solutions require robustness, such as the authentication of bank cards or bank systems. Nevertheless, most of these documents will require a global perspective, like the e-Passport, while others will only be relevant at a regional level (Schneier, 2011). The authorization property limits certain operations within the network to exclusively authenticated entities, thereby excluding unauthorized entities.

**2.4 Classification of Possible Intruders**

The presence of a Dolev-Yao (DY) intruder is typically assumed (Cervesato, 2001). An intruder, acting as the network, has the ability to intercept any and all messages transmitted between IoT devices and hubs. The DY intruder possesses exceptional capabilities, although some of these capabilities may be considered somewhat unrealistic. Therefore, the level of safety will significantly increase if our IoT infrastructure is specifically designed to be highly resistant to unauthorized access. The DY intruder, unlike regular intruders, does not possess the ability to physically compromise a system. Therefore, the demand for tamperproof devices is also high. The objective is inherently unachievable, but ensuring physical tamper resistance remains a highly significant aim. Alongside tamper detection capabilities (tamper evident), it can serve as a satisfactory initial defense. In literature, intruders are categorized into two primary types: internal and external. Internal intruders refer to individuals who have been granted privileges or authorized access to a system, either through having an account on a server or physical access to the network (Duncan, 2012). External intruders refer to individuals who are not part of the network domain. Intruders, regardless of their origin, can be classified into various categories and may include individual assailants as well as intelligence agencies operating on behalf of a nation. The extent of an intrusion's impact is contingent upon the objectives that are sought to be accomplished. An individual assailant may have limited goals, whereas espionage agencies may have more extensive motivations (Sheldon, 2012).

**Individuals**

Single hackers are lone experts who only concentrate on breaking into systems with weak security (Sheldon, 2012). They lack the resources and knowledge that professional hacking teams, organizations, or spy agencies have. Attacks carried out by lone hackers usually target smaller and less diverse entities, meaning that their impact is not as great as that of organized groups. Individual attackers typically use social engineering techniques to obtain basic system information, such as the address, password, port information, and so forth. Hackers typically target public and social media platforms in an attempt to trick gullible users. Moreover, there are common and well-known vulnerabilities in the operating systems of laptops, desktop computers, and mobile phones that can be utilized by lone attackers. Banks and other financial institutions are frequently the focus of lone hackers because of their susceptibility to hacking. These organizations deal with financial transactions that hackers might take advantage of by altering the data to their benefit. There is a long history of credit card information theft committed by lone hackers. The growth of online shopping has made it easier to use credit card information that has been stolen to make purchases of goods and services (Sheldon, 2012).

To take advantage of a system, individual hackers use a variety of tools, including worms, viruses, and sniffers. They plan their assaults according to the equipment that is available, the internet's accessibility, the network environment, and the system security level. Insiders are one particular type of hacker (Duncan, 2012).Insiders are people who have been given permission to act against a system by abusing their privileges or knowledge. Insiders have the ability to provide vital information to outside attackers (third parties) in order to take advantage of weaknesses that could allow an attack. The individuals are aware of the weaknesses in the system and have a thorough comprehension of how it operates. Insiders may be driven by greed, retaliation, or self-interest. People can tolerate risk in different degrees, ranging from negligible to substantial, depending on their degree of motivation (Rudner, 2013).

**Organized groups**

Criminal organizations are increasingly becoming acquainted with current communication methods and Internet of Things (IoT) technology. Furthermore, as these groups gain proficiency in technological applications, they can develop a heightened awareness of the potential benefits provided by the infrastructure for directing information across various networks. The motivations of these groups vary significantly, with their typical targets encompassing specific organizations for the purpose of seeking revenge, stealing trade secrets, engaging in economic espionage, and targeting the national information infrastructure. They also engage in the sale of personal information, including financial data, to other illicit groups, terrorists, and even governmental entities. They possess significant capabilities in terms of financial funding, expertise, and resources. Criminal organizations possess varying levels of proficiency in terms of methods and techniques, ranging from moderate to high, contingent upon their specific objectives. The individuals possess exceptional expertise in developing botnets, malicious software, and denial-of-service attack techniques (Wilson, 2008).

Organized criminals are highly probable to possess financial resources, enabling them to recruit proficient hackers if needed, or acquire user-friendly attack tools from the clandestine market to target any systems (Nicholson, 2012). These types of criminals have a higher threshold for risk compared to individual hackers and are willing to invest in attacks that yield profitable outcomes. Cyber terrorism refers to a type of cyber-attack that specifically targets military systems, banks, and specific facilities like satellites and telecommunication systems that are part of the national information infrastructure. These attacks are motivated by religious and political interests (Archer, 2014). Terrorist organizations rely on the internet to disseminate propaganda, solicit funds, acquire intelligence, and communicate with collaborators across the globe. Another prevalent group of criminal organization entails hacktivists. Hacktivists are collectives of skilled hackers who participate in activities such as denial-of-service attacks, fraudulent actions, and/or identity theft. Furthermore, certain factions such as the Syrian Electronic Army (SEA), Iranian Cyber Army, and Chinese cyber-warfare units possess political agendas (Archer, 2014).

**Intelligence Agency**

Intelligence agencies from various nations exhibit unwavering determination in their endeavors to investigate the military systems of other nations for specific objectives, such as industrial espionage, as well as political and military espionage. In order to achieve their goals, the agencies necessitate a substantial quantity of specialists, a wide range of infrastructure including research and development organizations that offer technologies and methodologies (such as hardware, software, and facilities), as well as adequate financial and human resources. These agencies possess well-structured systems and advanced resources to achieve their objectives of intrusion. These agencies pose the greatest risk to networks and require strict surveillance and monitoring methods to protect against threats to the information systems that are crucial for any country and military organization (Ball, 2011).

The Internet of Things (IoT) has experienced significant and swift growth in recent times. Its capacity to provide diverse services has positioned it as the most rapidly expanding technology. This growth has had a profound influence on both social life and business environments (Andreev & Koucheryavy, 2012). The Internet of Things (IoT) has slowly become a part of every aspect of modern human life, including education, healthcare, and business. It involves the storage of sensitive information about individuals and companies, financial data transactions, product development, and marketing. The widespread proliferation of interconnected devices in the Internet of Things (IoT) has resulted in a significant need for strong security measures to address the increasing demand from millions, or even billions, of connected devices and services globally (Kumar & Patel, 2014). The frequency of threats is escalating on a daily basis, with attacks becoming more numerous and intricate. The number of potential attackers and the size of networks are increasing, and the tools available to potential attackers are also becoming more advanced, efficient, and effective (Kizza, 2013). In order for the Internet of Things (IoT) to reach its maximum potential, it is crucial to safeguard it against potential threats and vulnerabilities (Taneja, 2013).

**2.3 Empirical Review**

**2.3.1 Security in IoT Devices and Services**

**Malware and Malicious Code Injection Attacks:** Malware and the injection of malicious code present significant cybersecurity threats, particularly aimed at Internet of Things (IoT) devices and systems. During these attacks, assailants inject malicious code into Internet of Things (IoT) devices or networks with the aim of undermining their functionality, stealing confidential information, or gaining unauthorized access. Malware attacks on IoT infrastructure involve the distribution of malicious code, including viruses, worms, ransomware, or botnets, which exploit vulnerabilities in IoT systems. These attacks often target web applications or communication protocols used by Internet of Things (IoT) devices (Xiao et al., 2014). These attacks enable unauthorized individuals to gain access to IoT devices, granting them the ability to manipulate device functionality and compromise the integrity of data. Adversaries possess the capability to surreptitiously acquire sensitive information, such as passwords and login credentials, that are stored on Internet of Things (IoT) devices, resulting in breaches of privacy. Malicious actors can impede the functioning of IoT devices and networks by introducing them to malicious code, leading to disruptions in services. Malicious actors can also infect devices with malicious software and exploit them to launch further attacks (Gubbi, 2013).

Stuxnet serves as a prime example of a targeted and malevolent software assault directed specifically at industrial control systems. Stuxnet capitalized on weaknesses in the software utilized to manage centrifuges in Iranian nuclear facilities, resulting in tangible harm to the equipment (Zorzi, 2010). To effectively reduce the risk of such attacks, it is crucial to implement regular security updates and patches, employ strong authentication methods, and utilize secure communication protocols (Hongsong, et.al 2011). Moreover, intrusion detection and prevention systems can assist in promptly identifying such attacks by carefully examining network traffic for recognizable patterns that indicate these attacks (Zorzi, 2010).

**False Data Injection (FDI) Attack:** This attack involves the deliberate manipulation of data collected or transmitted by IoT devices, leading to the generation of incorrect outcomes or the initiation of unintended actions. False Data Injection (FDI) attacks often exploit vulnerabilities in the communication protocols used by Internet of Things (IoT) devices for transmitting data, such as insufficient encryption and lack of authentication (Lopez, et.al, 2009). False Data Injection (FDI) attacks can lead to compromised data integrity, as the attackers manipulate or alter the data collected and processed by Internet of Things (IoT) devices. This can result in erroneous decision-making, which can have substantial consequences in critical sectors such as healthcare, energy, and transportation systems. False Data Injection (FDI) attacks can occur when an individual with malicious intent deliberately introduces falsified sensor data into an industrial control system, leading to the disruption of equipment functionality. The injection of false data into IoT devices can lead to privacy infringements, enabling unauthorized individuals to access sensitive information and monitor personal activities (Roman, et.al 2013).

**Replay Attack:** This attack entails the intentional selection of IoT devices by intercepting and retransmitting valid data packets, with the objective of gaining unauthorized entry. Attackers begin the process by intercepting data packets, which often contain authentication data, while a legitimate transaction takes place between two devices in the IoT network. Later on, the attacker sends the obtained data back to the system in order to trick the receiving device into thinking that the packets are authentic, thus exploiting the system's vulnerability (Rudner, 2013). Replay attacks have the potential to compromise the integrity of IoT systems by introducing replicated or obsolete data packets, which can result in inaccurate decision-making by the device. Moreover, replay attacks can result in a breach of privacy and disclosure of sensitive data, such as user authentication credentials and device-specific information. This attack can also hinder device performance by causing it to process and respond to unnecessary data packets, depleting resources such as memory and processing power (Kozik & Choras, 2013).

Smart home systems and Industrial IoT devices are vulnerable to replay attacks. A replay attack in smart home systems can exploit the communication between a smart lock and its corresponding mobile application. The attacker is able to intercept and store a legitimate unlocking command, which can then be played back later to gain access to the house. Adversaries may also target the interception of communication between sensors and control systems in industrial Internet of Things (IoT) devices (Kozik & Choras, 2013). In order to mitigate replay attacks, it is possible to include timestamps in the transmitted data packets. This can facilitate the detection and removal of duplicated data packets. The receiving device can later authenticate the timestamps of incoming packets and reject those with timestamps that are not within a predetermined range (Kozik & Choras, 2013). Moreover, the incorporation of a unique sequence number for each transmitted packet acts as a protective measure against replay attacks. The receiving device is designed to exclusively accept sequence numbers that surpass those of previously received packets, thereby effectively rejecting any attempts to replay packets. Furthermore, the implementation of digital signatures and message authentication codes (MAC) can offer additional safeguarding measures against replay attacks. Moreover, Intrusion detection systems can assist in thwarting replay attacks by examining network traffic for repetitive patterns linked to replay attacks, such as repeated authentication attempts or duplicates (Gubbi, et.al, 2013).

**2.4 Challenges of IoT Forensics**

**Lack of Standardization and Heterogeneity:** The lack of consistency and diversity among IoT devices has presented considerable obstacles for forensic investigators in implementing effective techniques during digital investigations that involve IoT devices. The IoT ecosystem encompasses a diverse array of devices, spanning from compact sensors to complex industrial control systems. These devices often utilize different hardware, operating systems, and software applications, leading to differences in data formats and storage systems (Mrdovic, 2021). Moreover, the communication protocols utilized by IoT devices can display significant discrepancies. Some devices may employ commonly accepted protocols, such as Wi-Fi, Bluetooth, or Zigbee, while others may rely on proprietary communication protocols. The wide range of IoT devices and their interconnected networks present a significant challenge for forensic investigators, who need to possess the capacity to understand and analyze the communication patterns among these devices (Wu, 2020).

Moreover, the diverse range of operating systems and software applications utilized by IoT devices is another crucial factor. Some devices use well-known operating systems like Linux or Windows, while others use proprietary systems. Forensic investigators encounter difficulties in selecting appropriate tools for extracting and analyzing data from these devices, as conventional tools may be inadequate in such situations (Stoyanova, et.al, 2020). Moreover, the need for enhanced uniformity and variety in IoT forensics presents significant challenges for forensic investigators. In order to successfully conduct digital investigations involving IoT devices, it is essential for individuals to have a comprehensive understanding of a wide range of tools and methodologies. These factors can lead to increased complexity, longer examination periods, and inaccurate results (Stoyanova, et.al, 2020).

**Limitation of Storage Capacity and Processing Capabilities:** IoT devices often have limited storage capacity and processing capabilities due to their small size and power constraints. IoT forensic investigators may encounter difficulties when collecting and analyzing digital evidence from these devices due to this limitation. Moreover, the data generated by IoT devices is often unstable, indicating that it experiences rapid fluctuations or may have time-sensitive importance. Preemptively obliterating or substituting the data prior to its collection can hinder forensic investigations (Mrdovic, 2021). To exemplify this difficulty, let's examine wearable Internet of Things (IoT) devices such as smartwatches or fitness trackers that generate significant amounts of data and activity logs. However, due to their limited storage and processing capabilities, these devices can only store data temporarily or depend on cloud storage services. This adds complexity to the forensic procedure as investigators must navigate through multiple tiers of data storage and retrieval (Stoyanova, et.al, 2020).

IoT devices have limited storage capacity, which means they can only hold a small amount of data. As a result, the stored information has a short lifespan and is likely to be quickly overwritten or lost. Forensic investigators encounter various difficulties in obtaining evidentiary data because it is rare and only available for a limited time. This leads to a limited understanding of the events being investigated. An additional concern arises due to the fact that specific IoT devices store data in volatile memory, such as RAM, leading to data loss in the event of power failure. Preservation and acquisition of digital evidence pose challenges as investigators must ensure continuous power supply to the device during the forensic procedure to prevent data loss (Yaacoub, et.al, 2022). A further concern arises due to the limited storage capacity of IoT devices, leading to data fragmentation and distribution across multiple locations. The fragmentation presents a challenge for investigators as they need to reconstruct the chronological sequence of events by collecting data from different sources. IoT devices have a restricted storage capacity, which results in a lack of sophisticated logging and monitoring capabilities. Consequently, it becomes difficult to identify malicious activities on these devices (Yaacoub, et.al, 2022).

**Data Location and Identification:** An additional significant challenge in IoT forensics is the considerable amount of data produced by IoT devices, which is distributed across numerous servers and networks. Therefore, forensic investigators may encounter challenges in accurately determining the exact location of the data. This is because the data could be stored on the device, different cloud services, or other devices and servers in the IoT network, which provide additional storage capacity. Forensic investigators encounter difficulties in amalgamating data from various sources and reconstructing the chronological order of events (Yaacoub, et.al, 2022). Another challenge arises from the decentralized nature of IoT forensic data, which increases the probability of data loss or corruption. This, in turn, complicates the forensic process even more. Furthermore, the adoption of cloud technology can bring about added intricacy. Cloud storage systems, typically used for storing and analyzing data generated by IoT devices, can be located in different global regions and overseen by different service providers. This further complicates the legal and jurisdictional proceedings, as forensic investigators may face legal limitations when trying to access data stored in various jurisdictions. Before acquiring the data, it might be imperative for them to navigate complex legal frameworks and secure legal authorizations (Esposito, et.al 2017).

**REFERENCE**

Abdullah A, Kaur H and Biswas R (2018) "Universal Layers of IoT Architecture and Its Security Analysis," in *Advances in Intelligent Systems and Computing* [https://doi.org/10.1007/978 981-13-9330-3\_30].

Abdalla, P. A and Varol C (2020) "Testing IoT Security: The Case Study of an IP Camera," [https://doi.org/10.1109/isdfs49300.2020.9116392].

Ayed, A. B, Taveras P and BenYounes T (2020) "Blockchain and IoT: A Proposed Security Framework," in *17th International Conference on Information* *Technology–New Generations (ITNG 2020)* [https://doi.org/10.1007/978-3-030-43020-7\_17].

Ahmed E, Islam A, Ashraf M, Chowdhury, A. I and Rahman, M. M (2020) "Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider," in *11th ICCCNT 2020*, Kharagpur [https://doi.org/10.1109/icccnt49239.2020.9225283].

Anwar, R. W, Zainal A, Abdullah T and Iqbal S (2020) "Security Threats and Challenges to IoT and its Applications: A Review," in *Fifth* *International Conference on Fog and Mobile Edge Computing (FMEC)*, [https://doi.org/10.1109/fmec49853.2020.9144832].

Archer, E.M (2014) “Crossing the rubicon: Understanding cyber terrorism in the European context,” *The European Legacy*, no. ahead-of-print, pp. 1–16.

Akhtar, M.S.; Feng, T (2022) A Systemic Security and Privacy Review: Attacks and Prevention Mechanisms over IOT Layers. *ICST Trans. Secur. Saf* *8*, e5.

Ball D (2011) “Chinas cyber warfare capabilities,” *Security Challenges*, vol. 7, no. 2, pp. 81–103.

Bertino E, Martino, L.D, Paci F and Squicciarini, A.C (2010) “Web services threats, vulnerabilities, and countermeasures,” in *Security* *for Web Services and Service-Oriented Architectures*. Springer pp. 25–44.

Baybutt P (2002) “Assessing risks from threats to process plants: Threat and vulnerability analysis,” *Process Safety Progress*, vol. 21, no. 4, pp. 269–275

Benazzouz Y, Munilla C, Gunalp O, Gallissot M and Gurgen L (2014) “Sharing user iot devices in the cloud,” in *Internet of Things (WF-IoT),* *2014 IEEE World Forum on*. IEEE, pp. 373 374.

Choudhary, Y., Umamaheswari, B., & Kumawat, V. (2021). A study of threats, vulnerabilities and countermeasures: An iot perspective. *Shanlax International Journal of Arts, Science and Humanity* 2021, 8, 39–45. <https://orca.cardiff.ac.uk/id/eprint/162617/7/electronics-12> 03927.pdf

De S, Barnaghi P, Bauer M and Meissner S (2011) “Service modelling for the internet of things,” in *Computer Science and Information Systems* *(FedCSIS), 2011 Federated Conference on*. IEEE pp. 949–955.

Duncan, A.J, Creese S and Goldsmith M (2012) “Insider attacks in cloud computing,” in *Trust, Security and Privacy in Computing and Communications* *(TrustCom), 2012 IEEE 11th International Conference on*. IEEE, pp. 857–862.

Dean, A. and Agyeman, M.O. (2018) A Study of the Advances in IoT Security. The 2nd International Symposium on Computer Science and Intelligent Control , Vol. 15, 1-5. <https://doi.org/10.1145/3284557.3284560>

Esposito C, Castiglione A, Pop F and Choo K.-K. R. (2017) “Challenges of connecting edge and cloud computing: A security and forensic perspective,” IEEE Cloud Computing, vol. 4, pp. <https://www.researchgate.net/publication/316501480_Challenges_of_> Connecting\_Edge\_and\_Cloud\_Computing\_A\_Security\_and\_Forensic\_Perspective

European Union Agency for Network and Information Security (ENISA) (2017) "Baseline Security Recommendations for IoT (in the context of Critical Information Infrastructures)," EU Publications, Heraklion, Greece [https://op.europa.eu/s/oz0X <https://doi.org/10.2824/03228>].

European Union Agency for Cybersecurity (ENISA) (2019) "Good Practices for Security if IoT: Secure Software Development Lifecycle," EU Publications, Athens, Greece, 2019 [https://op.europa.eu/s/oz0Y -<https://doi.org/10.2824/742784>].

Gupta, A. (2019) The IoT Hacker’s Handbook: A Practical Guide to Hacking the Internet of Things. Apress, Walnut. https://doi.org/10.1007/978-1-4842-4300-8

Gubbi J, Buyya R, Marusic S and Palaniswami M (2013) “Internet of things (iot): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660

Garfinkel, S. L “Digital forensics research: The next 10 years (2010) ” Digital Investigation, vol. 7, pp. S64–S73 The Proceedings of the Tenth Annual DFRWS Conference. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287610000368

Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N and Razafindralambo T (2011) “A survey on facilities for experimental internet of things research,” *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 58–67.

Hongsong C, Zhongchuan F, and Dongyan Z (2011) “Security and trust research in m2m system,” in *Vehicular Electronics and Safety* *(ICVES), 2011 IEEE International Conference on*. IEEE pp. 286–290.

James F (2019) "IoT Cybersecurity based Smart Home Intrusion Prevention System," in *3rd Cyber Security in Networking Conference (CSNet)* [https://doi.org/10.1109/csnet47905.2019.9108938].

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0

Kizza, J.M. (2020). Guide to Computer Network Security. Guide to Computer Network Security.

Kizza, J. M (2013) *Guide to Computer Network Security*. Springer.

Koien, G. M and Oleshchuk, V. A (2013) *Aspects of Personal Privacy in Communications Problems, Technology and Solutions*. River Publishers.

Kozik R and Choras M (2013) “Current cyber security threats and challenges in critical infrastructures protection,” in *Informatics and Applications* *(ICIA), 2013 Second International Conference on*. IEEE, pp. 93–97.

Kumar, J. S and Patel, D.R (2014) “Asurvey on internet of things: Security and privacy issues,” *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20–26 published by Foundation of Computer Science, New York, USA

Køien, G. M (2011) “Reflections on trust in devices: an informal survey of human trust in an internet-of-things context,” *Wireless Personal* *Communications*, vol. 61, no. 3, pp. 495 510

Li F, Lai A and Ddl D (2011) “Evidence of advanced persistent threat:Acase study of malware for political espionage,” in *Malicious and Unwanted* *Software (MALWARE), 2011 6th International Conference on*. IEEE, pp. 102–109.

Lopez J, Roman R and Alcaraz C (2009)“Analysis of security threats, requirements, technologies and standards in wireless sensor networks,” in *Foundations of Security Analysis and Design V.* Springer pp. 289–338.

Leloglu, E. (2017). A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, *05*(01), 121–136. https://doi.org/10.4236/jcc.2017.51010

‌

‌Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University - Computer and Information Sciences*, *31*(4), 541–553. https://doi.org/10.1016/j.jksuci.2018.03.011

Millar S (2021) "IoT Security Challenges and Mitigations: An Introduction," [https://www.researchgate.net/publication/357417180\_IoT\_Security\_Challenges\_and\_M tigations\_An\_Introduction].

Mrdovic S (2021) IoT Forensics. Cham: Springer International Publishing pp. 215–229. [Online]. Available: https://doi.org/10.1007/978-3-030-10591-4\_13

Malche T, Maheshwary P and Kumar R (2020) "Secret Key based Sensor Node Security in the Internet of Things (IoT)," in *Fifth International Conference on Communication and Electronics Systems (ICCES)* [https://doi.org/10.1109/icces48766.2020.9138078].

Miorandi D, Sicari S, De Pellegrini F and Chlamtac I (2012) “Internet of things: Vision, applications and research challenges,” *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516

NSFOCUS Inc., (2019) "Annual IoT Security Report " NSFOCUS Inc., USA, 2020 [https://nsfocusglobal.com/2019-annual-iot-securityreport

Padmavathi, D. G, Shanmugapriya M *et al.*, (2009) “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” *arXiv* *preprint arXiv:0909.0576*

Pahlevanzadeh, B., Koleini, S., & Fadilah, S. (2021). Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions. <https://www.researchgate.net/publication/348309426_Security_in_IoT_Threats_and_Vu> nerabilities\_Layered\_Architecture\_Encryption\_Mechanisms\_Challenges\_and\_Solutions citation/download?\_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9u wicGFnZSI6InB1YmxpY2F0aW9uIn19

Prakash C and Saini,R. K (2020) "A Model on IoT Security Method and Protocols for IoT Security Layers," in *Mobile Radio Communications and 5G Networks* [https://doi.org/10.1007/978 981-15-7130-5\_63].

Restuccia, F., D’Oro, S. and Melodla, T. (2018) Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. IEEE Internet of Things , 1, 1. https://doi.org/10.1109/JIOT.2018.2846040

Rainer, R.K and Cegielski,C. G (2010) *Introduction to information systems: Enabling and transforming business*. JohnWiley & Sons.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1). <https://doi.org/10.1186/s42400-020-00052-8>

Restuccia, F., D’Oro, S., & Melodia, T. (2018). Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet of Things Journal*, *5*(6), 4829–4842. <https://doi.org/10.1109/jiot.2018.2846040>

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481. https://doi.org/10.1080/08850607.2013.780552

Ray, A. K and Bagwari A (2020)"IoT based Smart home : Security Aspects and security architecture," in *9th IEEE International Conference on Communication Systems and Network Technologies* [https://doi.org/10.1109/csnt48778.2020.9115737].

Srivastava S and Prakash S (2020) "An Analysis of Various IoT Security Techniques: A Review," in *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida India [https://doi.org/10.1109/icrito48877.2020.9198027].

Skarmeta, A.F., Hernández-Ramos, J.L., & Bernal Bernabe, J. (2015). A required security and privacy framework for smart objects. 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), 1-7. <https://www.semanticscholar.org/paper/A-required-security-and> privacy-framework-for-smart-Skarmeta-Hern%C3%A1ndez Ramos/2e0811d3e177be5712d202594300de465cf3804f

‌ Schaad, A., & Binder, D. (2020). ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool. *Data and Applications Security and Privacy XXXIV*, 274–285. <https://doi.org/10.1007/978-3-030-49669-2_16>

Stergiou C, Plageras, A.P, Psannis, K. E and Gupta, B. B (2019) "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network," in *Handbook of Computer Networks and Cyber* *Security: Principles and Paradigms, Multimedia Systems and* *Applications*, Springer [https://link.springer.com/chapter/10.1007/978-3-030 22277-2\_21].

Sharma, R. K and Pippal, R. S (2020) "Malicious Attack and Intrusion Prevention in IoT Network using Blockchain based Security Analysis," in *12th* *International Conference on Computational Intelligence and Communication Networks* [https://doi.org/10.1109/cicn49253.2020.9242610].

Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E and Markakis, E.K (2020)“ A survey on the internet of things (iot) forensics: Challenges, approaches, and open issues,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191–1221,

Stergiou C, Psannis, K.E, Kim, B. G and Gupta B (2018) "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems,* vol. 78, no. 3, pp. 964-975 [https://doi.org/10.1016/j.future.2016.11.031].

Stergiou, C.L, Bompoli E and Psannis,K.E (2023) "Security & privacy issues in IoTbased Big Data Cloud systems in a Digital Twin scenario," *MDPI, Applied Sciences,* vol. 13, no. 2, January [https://doi.org/10.3390/app13020758].

Schaad, A.; Binder, D. (2020). Ml-supported identification and prioritization of threats in the ovvl threat modelling tool. In Data and Applications Security and Privacy XXXIV; Singhal, A., Vaidya, J., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 274 285.

Thoma M, Meyer S, Sperner K, Meissner S and Braun T (2012) “On iotservices: Survey, classification and enterprise integration,” in *Green* *Computing and Communications (GreenCom), 2012 IEEE International* *Conference on*. IEEE, pp. 257–260.

Taneja M (2013) “An analytics framework to detect compromised iot devices using mobility behavior,” in *ICT Convergence (ICTC) International* *Conference on*. IEEE, 2013, pp. 38 43

Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A, Jubert, I.S, Mazura M, Harrison M and Eisenhauer M *et al.(2011)* “Internet of things strategic research roadmap,” *Internet of Things- Global Technological and Societal Trends*, pp. 9–52.

Victorian Goverment Directory, (2020) "Desktop research," 29 04 2020. [Online]. Available: https://www.vic.gov.au/desktop-research.

Wheelus C and Zhu X (2020) "IoT Network Security: Threats, Risks, and a Data- Driven Defense Framework," pp. 259-285, [https://doi.org/10.3390/iot1020016].

Wu T (2020) “Digital forensic investigation of iot devices: tools and methods,” [Online]. Available: https://ora.ox.ac.uk/objects/uuid: 7e2a4b13-9dfc-4698-884c-26d8c236f074

Wustrich L, Pahl,M.O and Liebald S (2020) "Towards an Extensible IoT Security Taxonomy," [https://doi.org/10.1109/iscc50000.2020.9219584].

Xiao G, Guo J, Xu L and Gong Z (2014) “User interoperability with heterogeneous iot devices through transformation,”

Yaacoub, J.-P. A, Noura, H.N, Salman O, and Chehab A (2022) “Advanced digital forensics and anti-digital forensics for iot systems: Techniques, limitations and recommendations,” Internet of Things, vol. 19, p. 100544,[Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522000464

Yadav, P & Vishwakarma, S (2018). “Application of internet of things and big data towards a smart city,” in 2018 3rd International Conference On Internet of Things: *Smart Innovation and Usages* (IoT-SIU), 2018, pp. 1–5. https://ieeexplore-ieee org.proxy.lnu.se/document/8519920

Zorzi M, Gluhak A, Lange S and Bassi A (2010) “From today’s intranet of things to a future internet of things: a wireless-and mobility-related view,” *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 44–51