INTERNATIONAL
HELLENIC
UNIVERSITY

Cybersecurity and the Internet of Things

Evgenia Skouteli

SID: 3307200018

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

APRIL 2023

THESSALONIKI – GREECE

INTERNATIONAL HELLENIC UNIVERSITY

Cybersecurity and the Internet of Things

Evgenia Skouteli

SID: 3307200018

Supervisor:		Prof. Stavros Stavrinides
Supervising Members:	Committee	Prof. Konstantinos Rantos
		Prof. Dimitrios Baltatzis

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

APRIL 2023

THESSALONIKI – GREECE

Abstract

The Internet of Things (IoT) is rapidly gaining popularity and is poised to transform our perception of physical objects by transforming them into intelligent virtual objects. The ultimate objective of IoT is to integrate all aspects of our world into a unified infrastructure, which will not only enable us to manage our environment but also keep track of their status. However, the widespread adoption of IoT devices and services has also led to a rise in cyber threats and attacks. Although these attacks are not novel to the realm of IoT, their integration into our daily lives and societies has made it essential to give importance to cybersecurity measures. Consequently, there is a greater attempt to comprehend the hazards and assaults that imperil IoT infrastructure, and this citation focuses on exploring IoT cyber defense mechanisms.

It is crucial to secure IoT, as cyber-attacks can have severe consequences for governments, businesses, and individuals. Cybersecurity weaknesses in some countries, advances in cybercriminal technology, and the potential for cybercrime to infiltrate services and other business operations are all contributing factors to these attacks. To minimize these risks, effective and easily accessible antivirus and anti-malware tools must be employed.

Skouteli Evgenia

07/04/2023

Contents

Table of Figures

1 Introduction

As technology progresses, the Internet of Things (IoT) is becoming a potential innovation that can create a global computing network where every person and object can connect to the internet. The concept of IoT is continually developing and offers infinite possibilities for exploration and advancement. The development of technology has the ability to transform the current condition of the internet and incorporate it into a revised form. The quantity of devices using online services is rising constantly, and establishing wireless connections between all these devices can provide us with a vast amount of information easily accessible.

Large corporations are the primary motivation for the progress of the Internet of Things (IoT) due to the benefits they can reap from being able to track objects throughout the supply chains they participate in. The skill to program and monitor objects has enabled companies to enhance their efficiency, streamline procedures, minimize errors, hinder theft-related activities, and implement sophisticated and adaptable organizational systems through IoT. This technological transformation is viewed as the upcoming phase of computing and communication, relies on continuous technical advancements in areas such as wireless sensors and nanotechnology [1]. As part of this system, objects are labeled for identification, automation, monitoring, and control purposes.

While the idea of facilitating communication among smart devices is seen as groundbreaking, the individual technologies that constitute the Internet of Things are not novel to us. IoT involves merging data from various devices onto a virtual platform that utilizes the current internet framework. The concept of IoT can be dated back to 1982, when a coke vending machine was linked to the internet and could report on its inventory and the temperature of its beverages [2]. In 1991, Mark Weiser [3] introduced a modern idea of IoT through ubiquitous computing. In the same year, Bill Joy mentioned Device-to-Device communication in his internet taxonomy, and Kevin Ashton coined the term "Internet of Things" in 1999 to describe a system of interconnected devices [4].

The core idea of IoT is to enable self-directed transmission of valuable data among distinct, embedded physical devices by utilizing cutting-edge technologies like RFID and

WSNs. These devices are detected by sensors, and the data is then analyzed to make decisions, leading to automated actions [2].

The development of IoT technology has created numerous opportunities, including the potential for smart cities, advancements in education, e-commerce and banking, healthcare, and improved entertainment and protection for individuals. However, with the widespread use of connected devices comes the increased need for strong security measures. As more and more devices become connected and potential attackers continue to increase, the tools available to attackers are becoming more advanced and dangerous, resulting in both the number and complexity of attacks. In the 1990s, the term "Cyberspace" gained popularity as digital communication, networking, and internet usage increased rapidly. This term encompasses the various new concepts and phenomena that emerged during this time, though there is no clear definition for it. Generally, Cyberspace refers to the largest unregulated and uncontrollable sector that arises from the interconnection of information systems in human history. It is a unique realm that is created by people who oppose traditional physical areas, and their attacks are becoming more advanced and challenging to overcome. As a result, predicting the types of threats that may arise in the next few years is challenging, but it is certain that they will be more dangerous than the current ones. Additionally, old sources of threats will weaken while new sources will arise to take their place. Therefore, effective cybersecurity is becoming increasingly complex, and it is essential to use endpoint solutions such as virus detection software, IDS systems, IPS, patching, and encryption to combat these threats [5].

To achieve the complete potential of IoT, it is crucial that it is adequately protected against these threats and vulnerabilities. With devices always connected to the network, there is a risk of open attacks, and industrial IoT-clouds are particularly vulnerable to malware and pirated software. Malicious attacks on IoT networks are becoming more frequent and can compromise the privacy and security of devices, computer systems, and smartphones. It is crucial to ensure security measures are in place to prevent physical harm, unauthorized entry, theft, or loss and to safeguard that information about the object is kept confidential and accurate, making it readily accessible when required.

2 Background of IoT and its potential benefits

IoT is a term used to depict the linkage between physical objects and devices with the internet, allowing them to gather and share data with other systems and devices. This concept offers notable advantages, such as improved automation, efficiency, and convenience in various industries, including healthcare, transportation, energy, and agriculture. Nevertheless, IoT comes with considerable obstacles that must be dealt with to ensure trustworthy and secure operation of IoT systems.

2.1 IoT background

The Internet of Things, also referred to as IoT, is based on the connection between physical world and the world of internet. [6]. The IoT concept has been around for several years but has gained significant momentum in recent times. We first heard this term in 1999 from Kevin Ashton, which was MIT Executive Director of Auto - ID Labs. Although Kevin Ashton invented the phrase ‘’Internet of Things’’, the definition evolved over the years. The IoT technology has rapidly increased in the technology industry and undoubtedly it is a fundamental component of the upcoming internet. The term "IoT" is employed to describe the growing network of objects and devices that have internet connectivity and can exchange information with one another. It refers to a network of tangible devices that are equipped with software, sensors and internet connectivity, enabling them to amass and share data. The devices can be anything from home appliances, vehicles, industrial equipment, to wearable devices, among others. The collected data can be analyzed to gain insights into the behavior of the devices, the environment, and the people using them. We can call the Internet of Things an internet revolution, which is able to generate innovative intelligent ecosystems that enhance urban areas, transportation, healthcare, agriculture, energy, and other domains by incorporating intelligent features. The concept driving IoT is to facilitate universal connectivity among things, people, and networks, regardless of location or network type, to enable seamless interaction (Figure 1) [7].

The basic idea of this technological breakthrough is the variety of interconnected devices, things or objects, animals, or people such as Radio-Frequency IDentification (RFID) tags, mobile, phones, actuators, sensors, etc. which, through unique identifiers and IoT data protocols can be exchange information between the network, even without an internet connection or requiring human-to-human or human-to-computer interaction [8].

The devices within the network have the capability to communicate with each other, allowing for the remote access of sensor data and control of the physical world from a distance. The devices collect information and data about how they are used and the environment in which they operate with their sensors. Sensors constantly share information about these devices operational status and collect it on the Internet of Things platform. The data is processed there, and the results are shared with the other connected devices for a more pleasant user experience, automated processes, and improved operations.

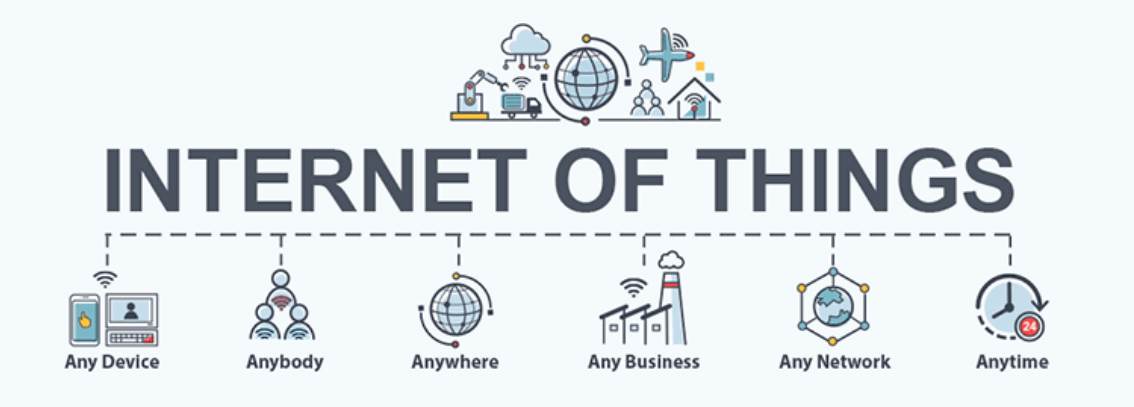

Figure 1. Internet Of Things

2.2 Overview of IoT technologies and architectures

The Internet of Things (IoT) encompasses a range of components and systems that work together to enable its functionality. These can be broadly categorized into three groups: devices, networks, and cloud platforms. IoT devices are physical objects equipped with sensors, actuators, and communication modules that collect and transmit

data. These can include various items such as appliances, wearables, and industrial equipment. Sensors collect environmental data like temperature and pressure, which is processed by a microcontroller to make decisions, and then executed by actuators. IoT networks facilitate communication between devices and cloud platforms, and they can be wired or wireless, using different protocols such as Wi-Fi, Bluetooth, ZigBee, and Z-Wave [88]. IoT networks can be categorized as personal area networks (PANs), local area networks (LANs), and wide area networks (WANs), with varying ranges and communication purposes. Cloud platforms are the central hub of IoT systems, storing and processing the collected data. Cloud platforms can offer services such as data analytics and machine learning to process and interpret the data collected by IoT devices. There are three types of cloud platforms: public, private, and hybrid. Public cloud platforms are accessible to anyone over the internet, while private cloud platforms are operated by individual organizations, and hybrid cloud platforms are a mix of both. While IoT technologies have the potential to collect and analyze large amounts of data, there are significant cybersecurity challenges associated with their complexity and interconnectedness. These challenges must be addressed to ensure the security and privacy of IoT data [9].

In the development of the Internet of Things (IoT), several pioneering technologies are being utilized, such as nanotechnology, sensor networks, smart technology, and RFID. One of the foundational elements and crucial networking components for establishing the IoT is RFID.Another type of data collection technology used in the IoT is the wireless sensor network (WSN). Wireless sensor network (WSN) technology using self-organization capabilities enables wireless communication between multiple nodes. It can also use multi-hopping features. A common Wireless sensor network (WSN) system consists of a hub that enables wireless access to the wired network and decentralized nodes equipped with sensors for detecting various physical events like pressure, light, and heat. The purpose of the network design is to assist in working together so that it can gather data from the environment, and to process the sensor data while also performing tasks such as collecting, measuring, combining, and transmitting applications [9].

2.2.1 An Overview of IoT Technologies

Initially, the concept of the Internet of Things (IoT) was introduced by individuals in the RFID industry. Their idea was to browse an internet address or database entry that corresponds to a particular RFID or Near Field Communication (NFC) technology, to obtain information about a tagged object. According to the study titled "Research and application on the smart home based on component technologies and Internet of Things" [95], several essential technologies that facilitate the functioning of IoT include RFID, sensors, embedded intelligence, and nanotechnology. Out of these, RFID is considered the fundamental technology that forms the networking core for building IoT.

IoT utilizes numerous tagging technologies such as RFID, NFC and 2D barcode to bring physical objects into the cyber world. These objects can then be identified and accessed through the internet. IoT is a ubiquitous network that is based on the omnipresent hardware resources of the internet and is integrated with sensor technology and radio frequency technology. It represents a new wave of the IT industry, which combines computing fields, communication networks, and global roaming technology. Along with advanced technologies, IoT encompasses numerous supporting technologies such as information collection, remote communication, and remote information transmission, intelligent analysis of measurement information, and controlling technology [91].

Radio Frequency Identification (RFID) is a wireless communication system that transmits the identification of a person or an object in the form of a serial number using radio waves [10]. Its initial use was in Britain during World War II to distinguish Friend or Foe and was later developed at MIT's Auto-ID Center in 1999. In the context of the Internet of Things (IoT), RFID technology is critical in identifying objects in our surroundings in a cost-effective way [11]. The technology is divided into three categories that differ in how power is supplied to the tags: Active RFID, Passive RFID, and Semi-Passive RFID. The main components of RFID are tags, readers, antennas, access controllers, software, and servers. RFID is dependable, efficient, secure, cost-effective, and precise, and has a broad range of wireless applications, including distribution, tracking, patient monitoring, military applications, and more [12] [91].

Internet Protocol (IP), which was developed in the 1970s, is the primary protocol used for networking on the internet. It is responsible for transferring datagrams across network boundaries and is a key component of the Internet protocol suite. There are

currently two versions of IP in use, IPv4 and IPv6, each with their own way of defining IP addresses. The term "IP address" usually refers to the addresses used in IPv4 due to its widespread use. IPv4 has five classes of IP ranges, and can support 4.3 billion addresses, with this ability IPv4 is becoming increasingly inadequate. IPv6, on the other hand, can support a much larger number of addresses, estimated at 85,000 trillion, making it the protocol of choice for the 21st century [13][91].

The EPC, or Electronic Product Code, is an alphanumeric code that is stored on an RFID tag and contains either 64 or 98 bits. Its purpose is to enhance the conventional EPC barcode system by enabling storage of additional information such as product specifications, manufacturer information, unique serial number of the product, and type of EPC.The AutoID Centre at MIT developed EPC in 1999. The standardization of EPC technology is overseen by the EPCglobal Organization, which created the EPCglobal Network to facilitate the sharing of RFID information. The EPCglobal Network has four components: Object Naming Service (ONS), EPC Discovery Service (EPCDS), EPC Information Services (EPCIS), and EPC Security Services (EPCSS) [16] [91].

Barcodes are a method of encoding letters and numbers through various widths of bars and spaces. While the name "barcode" accurately describes the method, it is not crucial to understanding it [14]. There exist different ways to input data. Quick Response (QR) codes are a type of matrix barcode that were originally created in Japan for use in the automotive industry. They have become widely used due to their high storage capacity and quick readability compared to traditional barcodes. Barcodes come in three different types: alphanumeric, numeric, and 2D. They are intended to be read by machines, often with the aid of laser scanners, but they can also be read using cameras [91].

Wireless Fidelity (Wi-Fi) is a wireless technology that enables communication between devices through radio waves. Vic Hayes is commonly known as the "father" of Wi-Fi, although the technology's precursor was developed by NCR Corporation in the Netherlands in 1991. The first wireless products were marketed as WaveLAN, with data transmission speeds of 1-2 Mbps. Today, Wi-Fi is nearly omnipresent, delivering fast Wireless Local Area Network (WLAN) connectivity to millions of homes, offices, and public spaces like airports, cafes, and hotels. Wi-Fi is integrated into a wide variety of devices, including notebooks, handhelds, and consumer electronics [15]. The technology supports various IEEE 802.11 standards, including dual-band, 802.11a, 802.11b,

802.11g, and 802.11n. In some cities, Wireless access points have transformed entire areas into Wi-Fi hotspots [91].

Bluetooth is a low-cost radio technology that allows wireless communication among devices such items as computers, cameras, and printers within a range of 10 to 100 meters without the need for cables. The maximum speed of communication for Bluetooth is less than 1 Mbps, and it uses IEEE 802.15.1 standard. The project "Bluetooth" was initiated by Ericson Mobile Communication in 1994 to create Personal Area Networks (PAN). A Piconet refers to a cluster of Bluetooth-enabled devices that share a single communication channel. This cluster can support the transfer of various types of data such as text, pictures, videos, and audio, and can host between 2 to 8 devices simultaneously. The responsibility of standardizing and developing Bluetooth technology lies with the Bluetooth Special Interest Group, comprising more than 1000 companies such as Cisco, HP, Intel, IBM, Aruba, and Toshiba [61] [91].

ZigBee is a wireless protocol used for sensor networks, which was developed by the ZigBee Alliance in 2001 to improve its features. The protocol's key features include cost-effectiveness, low data rate, short transmission range, scalability, reliability, and adaptable protocol design. Based on the IEEE 802.15.4 standard, ZigBee is a low-power wireless network protocol [16]. It can operate in a variety of topologies, including star, cluster tree, and mesh topologies, and can cover a distance of up to 100 meters with a bandwidth of 250 kbps. ZigBee has various applications in industries like home automation, digital agriculture, industrial management, healthcare surveillance, and energy grids [61] [91].

Near Field Communication (NFC) is a wireless technology operating at a frequency of 13.56 MHz, which typically functions at a range of 4 cm. It simplifies transactions, digital content exchange, and connection of electronic devices by enabling intuitive initialization of wireless networks. While NFC is similar to Bluetooth and 802.11 in terms of its wireless capabilities, its range is limited to approximately 10 cm. NFC technology is complementary to these other technologies, and it has the added advantage of functioning in dirty environments without requiring a direct line of sight. Originally, it was created by the companies Philips and Sony, and it has a data transfer speed of around 424 kbps. The amount of power used when reading data through NFC is less than 15 milliamperes [91].

An actuator is a device that transforms energy into movement, driving mechanical systems. The energy source can be hydraulic fluid, electric current, or some other power source. Actuators are devices that are capable of generating movement in the form of linear, rotary, or oscillatory motion. They can cover short distances, usually limited to a maximum of 30 feet, and commonly communicate at speeds of less than 1 Mbps. Actuators are frequently used in industrial and manufacturing environments. The three main types of actuators are electrical, hydraulic, and pneumatic. Electrical actuators include AC and DC motors, stepper motors, and solenoids. Hydraulic actuators use hydraulic fluid, while pneumatic actuators use compressed air. Although all three types are commonly used, electric actuators are the most popular due to their versatility. Hydraulic and pneumatic systems offer increased force and torque from smaller motors [91].

A wireless sensor network (WSN) comprises a collection of independent devices that are distributed across an area and use sensors to cooperatively observe and monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion, or pollutants. The network consists of numerous motes that communicate with one another and transmit data between nodes. WSNs are a critical component of the Internet of Things (IoT) ecosystem. Due to the burden of managing a large number of sensors, the sensor nodes may not possess a global ID. WSNs have a variety of applications, including military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire, and flood detection [17]. For instance, in healthcare, sensors placed on a patient's body monitor the response to medication to enable physicians to assess the medicine's impact [91].

Artificial Intelligence (AI) refers to digital environments capable of detecting and reacting to human presence. In an ambient intelligence context, devices collaborate to assist people in accomplishing their daily tasks in an easy and natural way by utilizing information and intelligence concealed in networked devices. Ambient intelligence is identified by the following features:

- Embedded: A plethora of networked devices are assimilated into the environment.
- Context-Aware: These devices can recognize the user and the context of the situation.
- Personalized: They can be customized to cater to the user's needs.
- Adaptive: They can alter their responses according to the user's behavior.

- Anticipatory: They can predict the user's preferences without any conscious input [61] [91].

2.2.2 An Overview of IoT Architecture: Understanding the Layers

Not all IoT applications or technologies adopt a universal architecture. Instead, every individual technology has its own distinct framework and asserts its superiority. The IoT can be challenging due to its heterogeneity and ability to address and deliver data on a large scale. In order to generate intelligent results with security measures and provide data in line with user expectations, IoT architecture must involve devices, networks, and applications that integrate and connect things. The IoT architecture comprises several layers of technologies, protocols, and standards that enable various scenarios to implement IoT with scalability, diversity, and interoperability [88].

At present, a tendency exists in reviewing the architecture of the Internet of Things (IoT) based on either the OSI layer or the TCP/IP layer, which includes 3-layer, 4-layer, and 5-layer architectures. The most commonly used IoT architecture layer model is the three-layer model comprising of the perception layer, network layer, and application layer. This model is widely adopted and used in various IoT applications and devices. However, other models such as the four-layer and five-layer models are also used in some specific applications and industries. The selection of the architecture layer model is determined by the specific requirements and needs of the IoT application or device [88].

2.2.3 Three Layer Architecture

This proposed IoT architecture is very basic but still serves the fundamental purpose of IoT. It was first suggested in the initial phases of the development of IoT and

consists of three layers, namely the perception, network, and application layers, as illustrated in the Figure 2 [18].

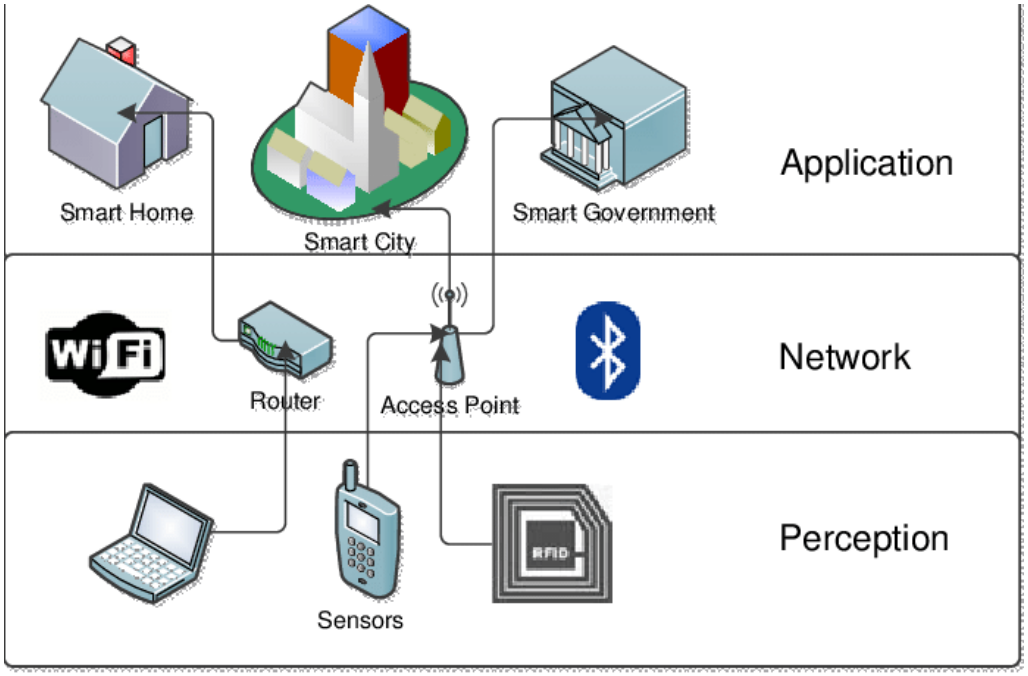

Figure 2. Three-layer IoT architecture

Physical and perception layer: The physical layer of the IoT system has several tasks, including interconnecting devices, identifying devices, and discovering services. The interconnected devices can vary in their types including Arduino, Raspberry Pi, or Zigbee. Nonetheless, for a device to be considered as part of the IoT system, it is required to have communication technology that permits to establish a connection with the internet either directly or indirectly, such as an Arduino with an Ethernet connection. Additionally, every device must possess a distinct identifier, such as a Universally Unique Identifier (UUID), that enables it to connect to the network [19]. The physical layer's technology is influenced by energy and computing power, and hostile environments can damage sensor devices, directly affecting the system's performance. The difficulty faced by this particular layer is protecting against malicious attacks that can interfere with data collection and identification technology. The physical layer is the lowest layer in the IoT architecture, consisting of physical devices or "things" connected to the network, including sensors, actuators, and other physical objects capable of sensing or manipulating the environment. The layer's primary responsibility is collecting data from

the environment and transmitting it to the upper layers of the architecture. To ensure reliable, scalable, and secure communication between devices and the network layer, the physical layer must be appropriately designed [19] [88].

The perception layer, often referred to as the sensor layer, functions like human senses such as eyes, ears, and nose. Its primary responsibility is to identify objects and collect data from them. Different categories of sensors including RFID, 2-D barcode, and other sensors are attached to objects to collect information, depending on the application's requirement. The collected data may be related to location, environmental changes, motion, vibration, and so on. However, these sensors are often targeted by attackers who try to replace them with their own, making them vulnerable to a majority of security threats [20][21].

Network Layer: The Network Layer is responsible for enabling communication between the physical and application layers of the IoT system, as well as facilitating communication between different IoT devices. This layer comprises communication protocols, routers, and gateways that allow devices to connect to the IoT network and exchange data securely and reliably. Edge computing devices may also be included in this layer to process data closer to the source, reducing latency and improving network speed and efficiency. The Network Layer is responsible for ensuring communication and connectivity between all devices in the IoT system using multiple communication protocols, such as MQTT 3.1 and Constrained Application Protocol (CoAP) are used to transmit information collected from the physical layer through communication infrastructures like the internet or mobile network to specific information processing systems or external networks. Physical devices utilize wireless sensors that are small in size, have limited computing power, and consume low energy. The received sensor data is wirelessly transmitted to the end-user, which can be a human or a device after processing.

However, the Network Layer is vulnerable to diverse types of assaults that can affect the collaboration among devices and the exchange of data, thus jeopardizing the reliability and safety of the network. Thus, it is crucial to enforce robust security measures to safeguard the network from attacks and ensure seamless communication and connectivity between IoT devices [22].

Application Layer: The Application Layer is responsible for processing and analyzing data collected from the physical layer of the IoT system. This layer comprises

software applications and platforms that offer data storage, analytics, and visualization functionalities, designed to process vast amounts of data and provide valuable insights for informed decision-making. Additionally, cloud-based platforms can provide machine learning and artificial intelligence services for data analysis. The Application Layer is also known as the Service Layer because it ensures that connected devices receive the same type of service.

The Application Layer is responsible for receiving data from sensors and actuators in a readable format. It is often referred to as the Service layer. This data can be used to provide various services and perform operations. The collected data is stored in a database to enable connections with other applications, such as Smart Home, eHealth, Smart Transportation, and Smart Objects. However, security is a significant concern for the Application Layer, as attackers often target the IoT system's software to access sensitive data and perform malicious operations. Therefore, robust security measures must be implemented to safeguard sensitive data and prevent unauthorized access [22] [88].

2.2.4 Four Layer Architecture

In this section, the four-layer architecture of IoT is adopted and discussed in detail in relation to the development of applications. The initial IoT architecture with only three layers was deemed inadequate to meet the evolving needs of IoT. Therefore, a new architecture with four layers was introduced by researchers to address this limitation. Although the new architecture retains the same three layers as the previous one, it adds an extra layer called the support layer, which is responsible for enhancing security against attacks. The Figure 3 [23] illustrates this layered architecture, along with recommended security measures to protect against intruders. The three layers perform the function similarly to the architecture mentioned earlier, while the support layer adds additional security functionality.

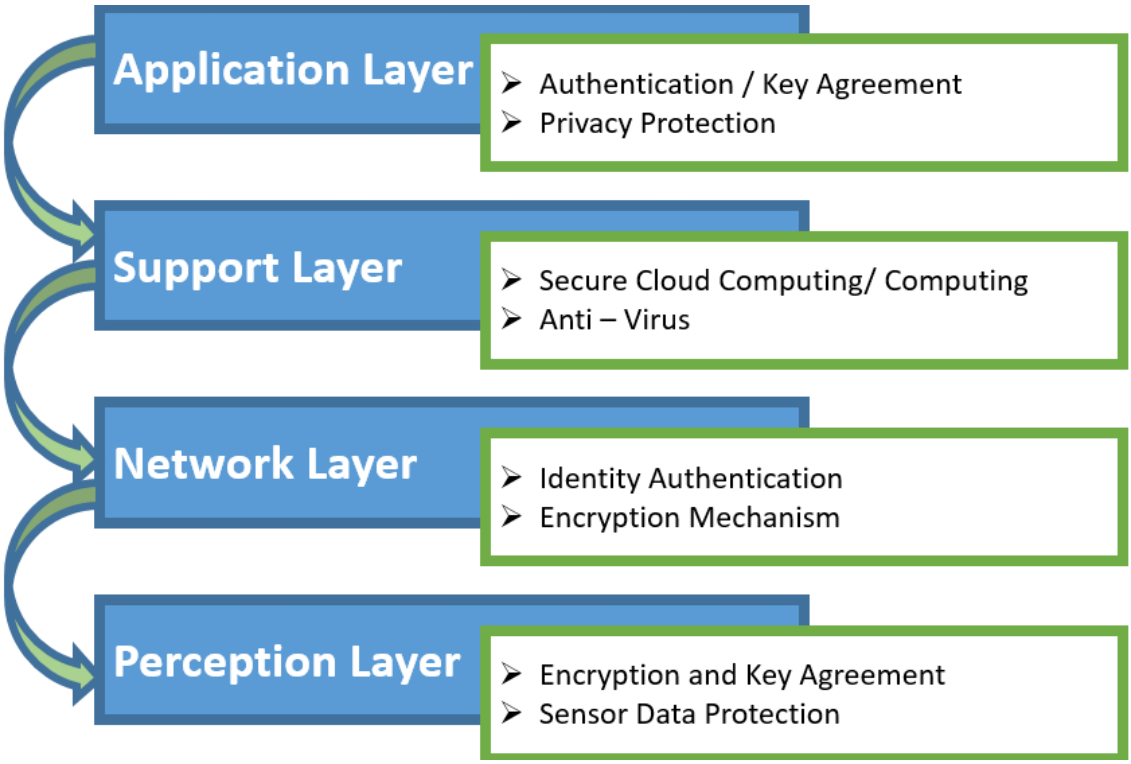

Figure 3. Four-layer IoT architecture

Support Layer: The support layer obtains data from the perception layer and is in charge of verifying that information is authentic and protected from threats before it is transmitted to the network layer. The support layer is primarily responsible for two key functions: Authentication and Security [24].

Authentication: The support layer verifies the authenticity of users and information using pre-shared secrets, keys, and passwords. This helps to prevent unauthorized access and ensure that the information being transmitted is from authentic sources [24].

Security: The support layer provides additional security mechanisms to protect against various types of attacks that can affect IoT systems, such as Denial of Service (DoS) attacks, malicious insider attacks, and unauthorized access. It acts as a buffer between the perception and network layers, ensuring that any threats or attacks are intercepted and dealt with before they can affect the system [24].

The support layer also facilitates communication between the perception and network layers, using either wireless or wired mediums, and provides additional functionality to enhance the overall security of the IoT system. It is also responsible for

managing device discovery and managing device configuration, as well as providing interoperability between different IoT devices and platforms. The support layer can also enable data aggregation and distribution, and can provide data processing capabilities, such as filtering and data analytics. Additionally, the support layer can enable remote device management and control, allowing for over-the-air updates and maintenance of IoT devices [24].

2.2.5 Five Layer Architecture

The Four-Layer IoT Architecture was an important development in IoT, but it faced issues related to security and storage. As a solution, researchers proposed the Five-Layer IoT Architecture, Figure 4 [25], which adds an extra layer for service/application support. This new architecture includes three layers from the previous architectures: the physical/perception layer, network layer, and application layer, and introduces two additional layers, the processing or middleware layer and business layer. This new architecture has the potential to meet the evolving requirements of IoT and to provide greater security for IoT applications. Each layer has specific functions, and there are security threats that can affect each layer, which should be addressed for the system's security [26].

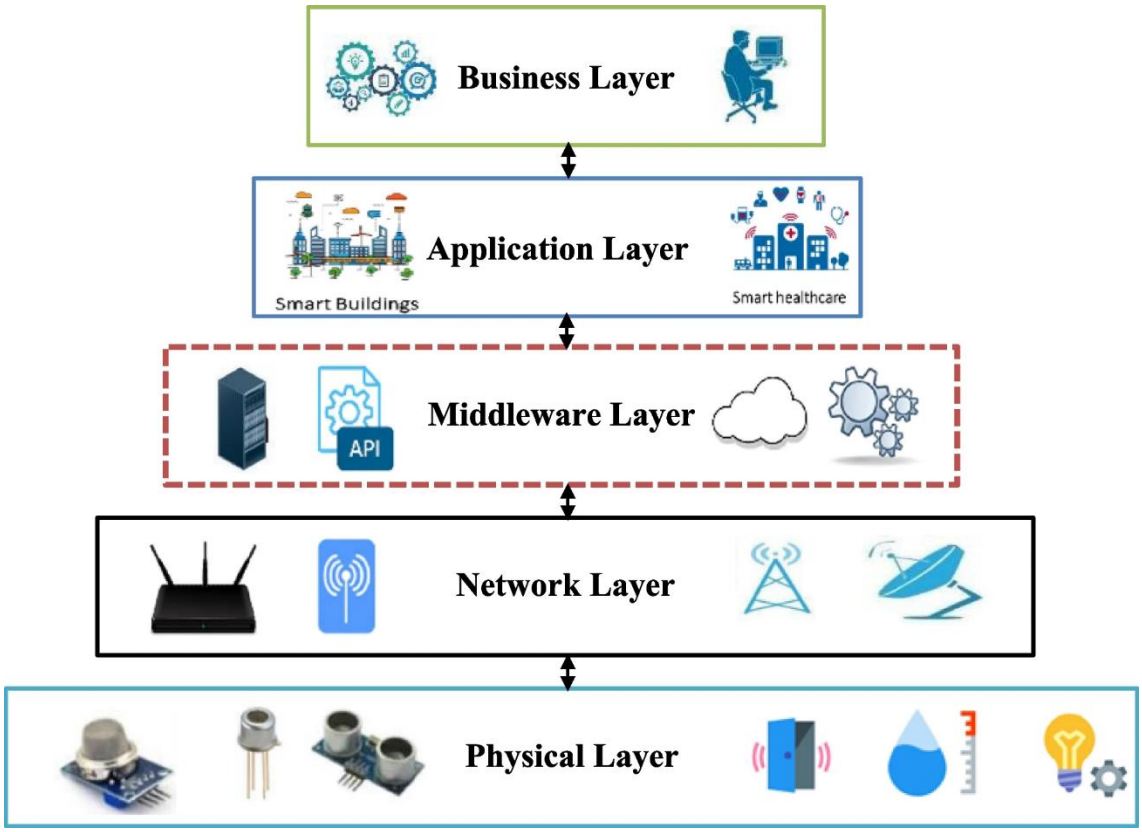

Figure 4. Five-layer IoT architecture

Processing Layer: The processing layer commonly referred to as a middleware layer. This layer plays a critical role in IoT by bridging the gap between physical devices and the applications that use their data. Its main tasks involve acquiring data from the network layer, connecting the system to the cloud and database, and managing data processing and storage. As cloud computing and IoT continue to develop, the middleware layer has the potential to provide improved computing and storage efficiencies, and it can reduce latency by processing data closer to the source. The middleware layer also provides APIs that allow the application layer to access and use the data collected by the physical layer. However, the security of the middleware layer is vulnerable to various attacks, such as eavesdropping, fraudulent packet injection, and unauthorized conversations [9]. It's crucial to consider the security of the database and cloud, as any issues can impact the quality of service in the application layer. Therefore, designing a secure and reliable communication between the physical layer, network layer, and application layer in an IoT system is essential for the middleware layer. In summary, the middleware layer is responsible for managing the flow of data among the various layers

of an IoT system and has a significant impact on ensuring the overall security and efficiency of the system [27].

Business Layer: In IoT architecture, the Business Layer is the highest layer, which interacts with users and external systems. It is responsible for providing business logic and decision-making capabilities based on the data collected from the lower layers. The Business Layer determines how the information gathered from the lower layers will be used to drive business outcomes and generate value. The Business Layer is particularly important for organizations that are leveraging IoT data to optimize their operations or create new revenue streams. It enables the organization to create new business models, improve customer experiences, and make data-driven decisions [63] [93].

From a security perspective, the Business Layer is also an important target for attackers, as it is where valuable business data and intellectual property reside. Therefore, security measures such as access controls, encryption, and authentication must be in place to protect the Business Layer from unauthorized access, tampering, or theft [28] [93].

Overall, the three layers of IoT architecture work together to enable the seamless flow of data between physical devices and software applications. By designing each layer to be secure, scalable, and efficient, developers can build more effective and innovative IoT systems that meet the needs of businesses and consumers alike.

2.3 IoT benefits

The possible advantages of IoT are enormous, and it could fundamentally transform numerous sectors. One of the most significant benefits is the creation of a more connected and intelligent world. IoT devices can be incorporated into diverse environments, such as homes, factories, and public spaces, to collect data that can be analyzed and used to make more informed decisions. Many new prospects may be anticipated not just for businesses and marketers, but also for society in general [6]. The integration of many smart devices in the field of learning, health and remote monitoring makes the impact of IoT on people's daily lives noticeable [29].

It is extremely useful in the average consumer's daily life, medical care, commerce, and even the manufacturing process. Consumers benefit most clearly from the Internet of Things in the area of "smart" homes. This includes automating everyday objects like furniture, electronics, and automobiles. In the health sector, an IoT application known as the Internet of Medical Things collects and analyses data for research purposes. In addition, many people have begun to use wearable devices to track their physical activity, sleep, and other habits. Transportation services are then provided with a network that establishes interaction relationships between vehicles and traffic, resulting in intelligent traffic control, intelligent parking, intelligent fleet and logistics management, and other benefits.

Corporate leaders will benefit from cognitive IoT technologies because they will have a greater knowledge of what is going on in the world. Injecting intelligence into systems and processes enables businesses to enhance consumer delight, encounter new business opportunities, and foresee potential risks or threats in order to address them more effectively. In industrial production and commerce, IoT provides data collection sensors that are integrated into machines or warehouses to alert about potential problems or control inventory. As a result, work is completed more efficiently, and costs are reduced. Consequently, IoT has also having a significant impact on the world of industry, specifically in the field of automation, intelligent industrial manufacturing, smart transportation, smart logistics and much more [29].

IoT technology can be utilized in households to monitor and manage temperature, lighting, and security systems, providing a more comfortable, safe, and energy-efficient living environment. For instance, smart thermostats can adapt to user preferences, and smart lighting systems can automatically turn off when an area is unoccupied.

Similarly, in the manufacturing sector, IoT devices can track equipment performance and recognize potential issues, allowing for preventive maintenance, reducing downtime and improving productivity. These devices can also monitor inventory levels and supply chains, improving operational efficiency and cost savings.

Moreover, healthcare can benefit from IoT technology as devices can remotely track patients' health, minimize in-person visits, and detect potential health concerns early. Wearable devices can record vital signs, while implantable devices can observe glucose levels and other health indicators, enhancing patient outcomes while reducing healthcare costs. Additionally, IoT sensors can enhance safety and security in smart cities,

adjusting traffic signals based on traffic flow, decreasing congestion, and improving safety [30].

In the energy industry, IoT devices can monitor power grids and predict potential outages, reducing the risk of power failures and enabling more efficient repairs.

The Internet of Things (IoT) has immense potential to revolutionize several industries, including healthcare, manufacturing, and transportation as mentioned above.

2.4 Security in IoT

However, like any novel technology, it comes with its share of challenges and risk. It faces three major issues in particular: collecting data, transmitting data, and securing data. Hence cybersecurity and data privacy issues. To address the data collection problem, various sensors have been developed and adapted for use in IoT devices. Additionally, several protocols have been created to facilitate the transfer of collected data and enable IoT devices to connect to existing networks.

Nevertheless, the issue of data security has not received adequate attention, resulting in various security concerns such as authentication and authorization. Securing data in IoT devices and services is an essential concern that requires attention. Not only users, but authorized objects can also access the data, making it necessary to address access control and authorization mechanisms, along with authentication and identity management (IdM) mechanisms [87]. To ensure the authorized access to services, IoT devices must be capable of validating whether the entity, like a human or object, is permitted to use the service, identification process assists in deciding. Regulating access to resources by permitting or prohibiting methods employing various criteria is part of access control. Authorization and access control play an essential role in establishing a secure connection among multiple devices and services [31].

Authentication and identity management are additional important elements to take into account while addressing the confidentiality of data. In the context of IoT, it is crucial to address the issue of authenticating several users, devices, and objects or things in a secure manner. The main challenge is to identify a secure approach for managing the

identity of these entities. Weaknesses in authentication may result in various types of attacks, such as replay, Denning-Sacco, denial of service, and password guessing attacks. Unfortunately, authenticating IoT devices across different protocols presents a significant challenge, as these protocols need to consider the limitations of IoT devices such as energy consumption, small memory size, and low processing capability [32][33].

Privacy is a significant matter in the realm of IoT due to its ubiquitous nature, where individuals, objects, or devices are interconnected, and information is shared and exchanged over the internet. Protecting user privacy is a delicate topic in numerous research articles, and privacy concerns related to data gathering, sharing, management, and security are ongoing research challenges.

In a dynamic IoT environment where many entities interact, trust is of utmost importance in establishing secure communication. Trust can be categorized into two dimensions: the reliability of an IoT system relies on both the trustworthiness of the entities involved and the trust that users have in the system. Trust in an IoT device is determined by various hardware and software components, such as sensors, memory, processor, applications, operating systems, drivers, and power source. To establish trust in a dynamic and collaborative IoT environment, it is essential to have an effective mechanism for defining trust [34].

It is crucial to address these concerns and mitigate risks while maximizing the potential benefits of the IoT as it grows and develops.

2.4.1 Vulnerabilities

Organizations are increasingly recognizing the significance of information and technology in every aspect of their operations, especially in driving innovation and achieving a competitive edge. However, the current information landscape poses various security risks to corporate information and technology services, such as prolonged disruptions in internet access and email, as well as data breaches [89].

The term "vulnerabilities" denotes flaws or shortcomings in the design or system that can enable unauthorized access to data, execution of commands, or denial-of-service

attacks by intruders. IoT systems can have vulnerabilities in various areas, such as hardware, software, policies, procedures, and even the users themselves.

The system hardware and software are the two primary constituents of IoT systems, and both of them frequently contain design faults. Due to hardware compatibility and interoperability issues, hardware vulnerabilities are challenging to detect and repair, and resolving them necessitates a significant amount of effort. Operating systems, application software, control software, communication protocols, and device drivers can all contain software vulnerabilities. Software design flaws can arise from a variety of factors, including human factors and software complexity. Technical vulnerabilities usually arise due to human weaknesses, such as inadequate planning, poor communication between developers and users, skills, knowledge, insufficient resources and a lack of system management and control [35].

2.4.2 Threats and Attacks

A threat refers to an activity or event that takes advantage of the vulnerabilities in a system, leading to adverse impacts [36]. Such threats may arise from two primary sources, namely humans and nature [37][38]. Natural calamities like earthquakes, hurricanes, floods, and fires may cause extensive damage to computer systems, and preventing them is difficult. To protect systems from natural hazards, contingency plans such as backup and disaster recovery plans are effective. Conversely, human threats occur when individuals or organizations attempt to cause damage and interfere with the functioning of a system. These can be malicious threats that may originate from insiders with authorized access or outsiders trying to cause damage [39][40]. The human threats can be classified into various types.

To categorize threats that exploit system vulnerabilities, there are two types: unstructured threats and structured threats. Unstructured threats are mostly caused by inexperienced individuals who utilize readily available hacking tools. Conversely, structured threats are carried out by individuals who have comprehensive knowledge of system vulnerabilities and are capable of developing and exploiting codes and scripts. Advanced Persistent Threats (APT) [41] is an instance of a structured threat that targets

business and government organizations, like manufacturing, financial industries, and national defense, with the goal of stealing valuable information [42].

The term "attacks" refers to the actions taken by attackers to exploit system vulnerabilities using different techniques and tools, resulting in harming or disrupting the normal operation of the system. Attackers usually launch these attacks to achieve a sense of contentment or compensation. The level of effort that an attacker puts into an attack is known as the "attack cost," [43] which is influenced by their expertise, resources, and motivation. Attackers, who pose a threat to the digital realm [44] may include hackers, cybercriminals, or even government agencies [35]. Attack methods can manifest in various ways, such as active network attacks that eavesdrop on unencrypted data to extract sensitive information, passive attacks that decrypt weakly encrypted data to acquire authentication details, close-range attacks, insider abuse, and more.

Cyber-attacks refer to a range of methods and tools that attackers use to harm or disrupt a system. These attacks come in various forms, such as physical attacks on IoT devices in outdoor environments, reconnaissance attacks that involve unauthorized discovery of systems and vulnerabilities, denial-of-service attacks that make network resources unavailable to users, and access attacks that allow unauthorized access to networks or devices. Attacks on privacy exploit remote access mechanisms through data mining, cyber espionage, eavesdropping, and tracking [45].

Password-based attacks involve attempts to duplicate valid user passwords using brute force or dictionary attacks.

Cybercriminals seek to gain materialistic benefits by exploiting users and data, which includes stealing intellectual property, identities, brands, and committing fraud.

Destructive attacks can cause large-scale disruption and destruction of life and property, including terrorism and revenge attacks.

SCADA attacks are carried out by shutting down the system using denial-of-service or by taking control of it using Trojans or viruses, such as the Stuxnet attack on an Iranian nuclear facility in Natanz in 2008 [45].

2.4.3 The main objectives for Security and Privacy

To address these risks, an organization must establish a comprehensive framework for implementing a security plan that enables creation, establishment, evaluation, and enhancement of the program. The plan should align with the organization's overall strategic plans and trace its content to these higher-level sources.

Despite most organizations employing baseline security measures such as antivirus software, firewalls, and intrusion detection systems, security incidents continue to rise. Research has shown that security risks increase due to internal and external threats, and organizations have been subjected to targeted attacks. In this environment, businesses must use strategies to direct their security efforts and make the most of their limited resources [2].

However, a single system may not be sufficient, and several security measures to protect information should be employed to guarantee that security measures are efficient and security policies are upheld. Although most literature focuses on security controls and their implementation to prevent security attacks, several security strategies, including detection, deterrence, and deception, have been conceptualized. However, there has been limited investigation into the security approaches employed by organizations to mitigate diverse security threats and the implementation methods used. Previously, security managers ignored business security risks, and plans were implemented ad hoc rather than as part of a planned and systematic approach to risk management [46].

In order to achieve successful implementation of effective security measures for Internet of Things (IoT) devices, it is imperative to have a clear understanding of the primary security goals (Figure 5)[47]. These goals can be defined as the fundamental objectives that need to be accomplished to ensure that IoT systems are secured against cyber threats and vulnerabilities. By identifying and prioritizing these security goals, organizations can develop and implement a comprehensive IoT security strategy that addresses the specific security challenges and risks associated with IoT devices. Therefore, it is critical to recognize and comprehend these primary security goals to establish a strong and reliable security framework for IoT devices [31].

Ensuring confidentiality is a critical security feature when it comes to protecting Internet of Things (IoT) devices, as it helps to safeguard sensitive information from unauthorized access or disclosure. While there may be some scenarios where

confidentiality is not a mandatory requirement, such as when data is presented publicly, it is still an essential consideration in many cases where confidential information should not be viewed or retrieved by unauthorized individuals [48]. This is particularly true in cases where highly sensitive data, such as patient information, private business data, military data, security credentials, and secret keys, are involved [18]. To prevent unauthorized entities from accessing this information, it is necessary to implement robust security measures that can effectively conceal and safeguard the data from potential cyber threats or breaches. By prioritizing confidentiality as a key security goal in IoT device security, organizations can develop a comprehensive security strategy that addresses the unique security challenges and risks associated with IoT devices, ensuring that sensitive data is protected and secure [60].

Maintaining integrity is an essential security feature for ensuring that Internet of Things (IoT) devices provide reliable and trustworthy services to users. In most cases, integrity is a mandatory security property that must be implemented to safeguard the accuracy and consistency of data, as different systems in IoT have varying integrity requirements depending on their specific functions and purposes. For example, a remote patient monitoring system must have high integrity checking capabilities to detect and correct any random errors that may occur due to the sensitive nature of the information being transmitted [48]. Loss or manipulation of data in such systems can potentially result in loss of human lives, which makes maintaining integrity even more critical. Additionally, communication-related issues can also lead to loss or manipulation of data, further emphasizing the importance of implementing robust integrity measures in IoT device security. By prioritizing integrity as a key security goal, organizations can develop a comprehensive security strategy that effectively safeguards IoT devices against potential cyber threats or breaches that could compromise the integrity of data, ensuring the reliability and accuracy of the services provided [31].

The ubiquitous connectivity of the Internet of Things (IoT) has significantly increased the complexity of authentication processes due to the diverse communication scenarios that can occur between different entities. These scenarios include device-to-device communication (M2M), human-to-device communication, and even human-to-human communication. Due to the varied authentication requirements across different systems, there is a need for different authentication solutions that cater to specific needs. An instance of this can be seen in the authentication mechanisms employed by banks for

their cardholders or banking systems which need to be robust and strong to ensure maximum security [49]. In contrast, authentication solutions for international systems, such as ePassports, must be globally recognized and accepted. At the same time, there is a need for local authentication solutions to cater to specific local contexts and requirements. The property of authorization ensures that only authorized entities (those that have been authenticated) are allowed to perform certain operations within the network. This ensures that only legitimate users can access the network and perform operations, preventing potential security breaches or unauthorized access to sensitive information. By prioritizing both authentication and authorization as key security goals in IoT device security, organizations can develop a comprehensive security strategy that effectively addresses the diverse authentication requirements and ensures the security and reliability of the IoT network [48].

Security goals	Definition
Confidentiality	Only authorized objects or users can get access to the data
Integrity	Data completeness and accuracy is preserved
Non-repudiation	The IoT system can validate the occurrence of any event
Availability	Ensuring the accessibility of an IoT system and its services
Privacy	The presence of privacy rules or policies
Auditability	Monitoring of the IoT object activity
Accountability	End users can take charge of their actions
Trustworthiness	Reliability on IoT object identity

Figure 5. Security Goals in IoT

In the context of Internet of Things (IoT) devices, availability is a crucial security feature that ensures users can access services whenever they need them. To achieve this, different hardware and software components of IoT devices must be designed to be resistant and capable of providing services despite the presence of malevolent entities or unfavorable circumstances. Different systems may have varying availability requirements, depending on their specific functions and purposes [50]. For instance, fire monitoring or healthcare monitoring systems require high availability to ensure that critical services are always available when needed. On the other hand, roadside pollution sensors may not require such high availability levels. By prioritizing availability as a key security goal in IoT device security, organizations can develop a comprehensive security strategy that ensures the reliability and availability of services provided by IoT devices. This will help to mitigate potential cyber threats or attacks that could compromise the availability of critical services, ensuring that users can access services whenever they need them [60].

In the context of secure network development, accountability plays a crucial role in ensuring redundancy and responsibility for specific actions, duties, and planning related to implementing network security policies. While accountability alone cannot prevent attacks, it adds an additional layer of security and ensures that other security techniques are functioning as intended. In fact, core security features such as integrity and confidentiality may be rendered ineffective without proper accountability measures in place. Furthermore, in the event of a repudiation incident, an accountability process can be utilized to trace an entity's actions and determine who was responsible for the incident. This can provide valuable insights into what happened and help identify potential weaknesses in the security system. Overall, by prioritizing accountability as a key security goal in IoT device security, organizations can develop a comprehensive security strategy that ensures that all security measures are implemented correctly and that potential security breaches are detected and addressed quickly [51],[52].

Auditing is the process of methodical assessment and examination of the security measures implemented on a device or service to measure its conformity to established security criteria. Given the prevalence of bugs and vulnerabilities in most systems, security auditing is crucial in identifying any exploitable weaknesses that could potentially compromise data security. In the context of IoT, the need for security auditing varies depending on the application and the value of the data being processed. For

instance, IoT applications that handle sensitive data such as healthcare information or financial transactions would require more extensive security auditing measures compared to applications that process less sensitive information. By conducting regular security audits, organizations can proactively identify and address any security vulnerabilities or weaknesses, which can help prevent potential security breaches and safeguard the integrity and confidentiality of the data being processed [31].

Non-repudiation is a security feature that ensures an evidence that a user or device cannot deny an action they have taken. Although non-repudiation is not generally regarded as a crucial security property in most IoT systems, it may have relevance in certain contexts, such as payment systems, where it is necessary to prevent users or providers from denying a payment action. In such scenarios, non-repudiation can be useful in establishing accountability and ensuring that all parties involved in the transaction accept responsibility for their actions [31].

Privacy refers to the entitlement of an individual or entity to control its interactions with the environment and decide to what degree it is willing to disclose information about itself to others. In IoT, privacy goals are of utmost importance and include various aspects.

The first is privacy in devices, which involves physical and communication privacy. In situations where a device is stolen or lost, confidential data can be exposed, making it crucial to have protection against side-channel attacks [31].

The second goal of privacy is ensuring privacy during communication, which relies on the availability, reliability, and integrity of devices. To avoid data privacy from being exposed during communication, it is important for IoT devices to transmit data solely when necessary.

The third goal is privacy in storage, which requires the consideration of the potential amount of data that needs to be stored in devices. Regulations should be extended to safeguard user data after the end-of-device life, such as deletion of the device data in the event of theft, loss, or non-use [53].

The fourth privacy goal is privacy in processing, which is dependent on the integrity of devices and communication. Data should not be disclosed to or retained from third parties without the knowledge of the data owner.

The fifth goal is identity privacy, which means that the discovery of a device's identity should only be permitted for authorized individuals or devices.

The sixth privacy goal is location privacy, which means that the location of pertinent devices should be revealed solely to authorized individuals or devices.

All of these privacy goals must be considered and met in order to ensure a secure and private IoT ecosystem [53].

2.4.4 IoT and Its Resulting Cyber Threats: An Overview

The term IoT or Internet of Things pertains to a network of interconnected devices that can communicate with each other and the internet. IoT devices can be vulnerable to cyber threats, which can pose significant security risks to individuals and organizations. Among the cybersecurity risks that can arise from IoT are:

Malware: Hackers can create and distribute malware specifically designed to target IoT devices, such as viruses, worms, and Trojan horses, which can spread to other devices on the network and cause damage [54] [55].

Botnets: IoT devices can be infected with malware and used to form botnets, which can be controlled remotely and used to launch large-scale attacks, such as Distributed Denial of Service (DDoS) attacks [55] [57].

Data breaches: IoT devices often collect and store sensitive data, such as personal information and financial data. If these devices are not properly secured, they can be vulnerable to data breaches, which can result in identity theft and financial loss [58].

Physical attacks: IoT devices can also be targeted for physical attacks, such as hacking into medical devices or critical infrastructure, which can result in serious harm or even loss of life [56].

Remote access: IoT devices can be accessed remotely, which means that hackers can gain access to the network and the devices themselves from anywhere in the world [59].

Overall, IoT devices are susceptible to various types of cybersecurity threats, and it is essential to implement protective measures against them. This includes establishing strong passwords, keeping the software up to date, and utilizing encryption techniques to secure confidential data.

2.4.5 IoT's Contribution to the Surge of Cyber Threats

The expansion of the Internet of Things (IoT) has resulted in a surge of cyber threats, primarily due to various factors. Initially, the sheer number of connected devices has provided cybercriminals with a larger attack surface to target, increasing the likelihood of exploiting vulnerabilities. Furthermore, many IoT devices are not equipped with sufficient security measures, which makes them vulnerable to cyber-attacks. (Figure 6)[60].

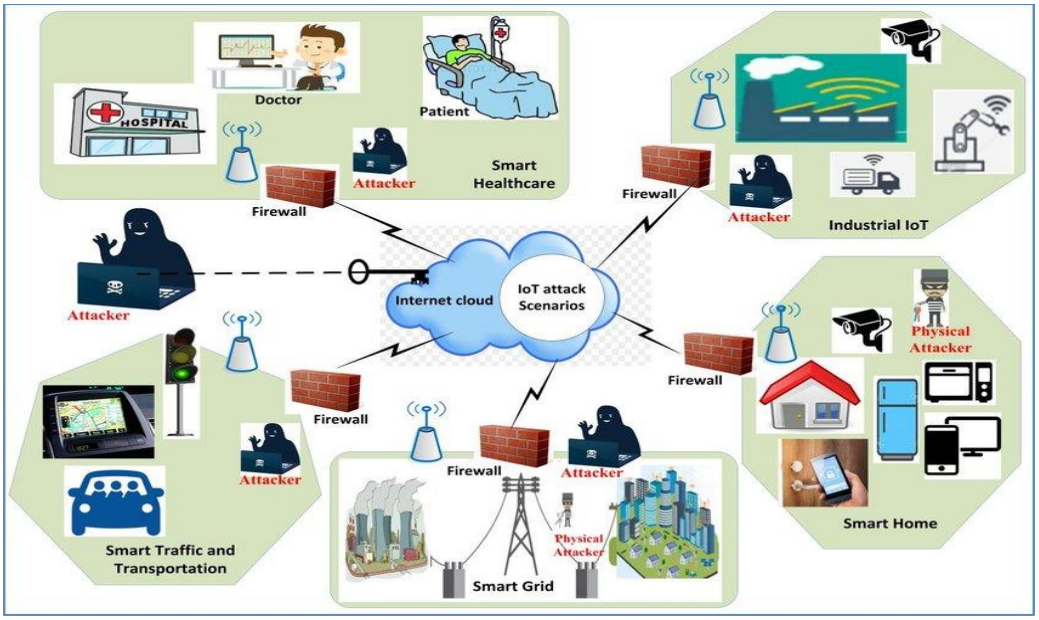

Figure 6. Various Application Areas and Their IoT Security Attack Scenarios

Additionally, the sensitive data collected and transmitted by IoT devices creates new avenues for data breaches and theft. Finally, the intricate nature of IoT networks makes it challenging to identify and counter cyber threats, enabling attackers to evade detection for extended periods. Altogether, these factors contribute to the escalation of cyber threats that stem from the use of IoT devices. The following are some of the factors that have led to the increase in cyber threats due to IoT:

Increased Attack Surface: The proliferation of connected devices has amplified the attack surface for cybercriminals, providing more opportunities for them to exploit vulnerabilities and access sensitive information.

Weak Security Measures: Many IoT devices are developed without adequate security measures, making them more susceptible to cyber-attacks. Some devices may lack fundamental security features such as robust passwords or encryption, further enhancing their vulnerability to hacking [62].

Data Collection and Transmission: IoT devices often gather and transfer sensitive data such as financial or personal information. Inadequately secured IoT devices may expose this data to cybercriminals, leading to identity theft, financial loss, and other forms of cybercrime. The vast amount of data collected and transmitted by IoT devices can lead to privacy concerns. In the wrong hands, this data can be used maliciously [61] [62].

Complex Network Architecture: IoT networks are typically complex, with numerous devices and systems communicating with each other. This complexity can make it difficult to identify and counter cyber threats, providing attackers with opportunities to evade detection for extended periods.

Human Error: Non-experts typically manage and configure many IoT devices, leading to configuration errors and other oversights that can compromise security. Additionally, some IoT devices may be unconfigured, leaving them susceptible to attacks.

Third-Party Integrations: Many IoT devices depend on third-party services and applications to function properly, which can introduce new security risks as third-party providers may have varying security standards compared to the device manufacturer [62].

Legacy Devices: Older IoT devices may not have been developed with security in mind and may not be compatible with modern security measures, posing a significant threat to the overall security of the IoT network.

Distributed Denial of Service (DDoS) Attacks: IoT devices have been utilized in massive DDoS attacks, which involve using a network of compromised devices to overwhelm a target with traffic. Preventing these attacks can be difficult, as they frequently originate from numerous sources [63].

Absence of Security Updates: IoT devices may not receive regular security updates, making them more susceptible to new cyber threats over time [62].

Physical Security Risks: IoT devices pose physical security risks, especially in critical infrastructure such as power grids and water treatment plants. They can be exploited to cause physical damage or disrupt operations.

Supply Chain Vulnerabilities: The complexity of IoT devices' supply chain can expose vulnerabilities if any of the vendors have weak security measures.

Lack of Awareness: Many people are unaware of the security risks associated with IoT devices, leading to poor security practices such as weak passwords, or failing to update software [62].

In general, the adoption of IoT has brought about various security challenges that must be tackled. To minimize these risks, it is crucial to apply security measures that match the particular requirements of each IoT system or device. This involves carrying out frequent security evaluations, setting up strong password protocols, and incorporating security techniques like encryption and two-factor authentication.

3 Cyberthreats

A cyberthreat is any activity or potential harm that is intended to target computer systems, networks, or internet-connected devices, including unauthorized system access, confidential data theft, malware infection, and critical infrastructure disruption. Cyberthreats can originate from different sources, such as criminal groups, nation-states, hacktivists, and individual hackers, and can be delivered through multiple ways, such as phishing, social engineering, email, or exploiting software or hardware vulnerabilities. As technology advances, cyberthreats are becoming increasingly complex and challenging to detect and defend. Therefore, it is crucial for individuals and organizations to take proactive measures to safeguard their digital assets and sensitive information against potential cyberattacks [66].

In today's digital world, cyberthreats have become an increasingly significant concern as technology becomes increasingly prevalent, both individuals and businesses are increasingly dependent on it for storing sensitive information and carrying out transactions. Cyberthreats can take various forms, such as malware, phishing, DoS attacks, MitM attacks, APTs, botnets, password attacks, and insider threats, and are designed to exploit system vulnerabilities and specific types of data (Figure 7) [67]. Cyberattacks motivated from financial gain to political or ideological objectives. The impact of cyberattacks can be devastating, resulting in financial losses, reputational damage, physical harm, and disruption of critical infrastructure, such as power grids and transportation systems. Prevention and mitigation of cyberthreats requires a multi-layered approach that includes technical measures, employee training and awareness programs, regular updates, and patches to software and systems. To effectively address cyberthreats, ongoing attention and investment are necessary. By staying informed about the latest threats and implementing proactive measures, individuals and organizations can reduce their risk and protect their systems and data.

Figure 7. Cyberthreats

3.1 Review of cyberthreats

Malware is a harmful software designed to exploit computer systems, networks, and devices. It encompasses a range of programs and applications that can infiltrate and compromise systems. Malware can take different forms, such as viruses, Trojans, worms, ransomware [68] and spyware, which can cause harm, steal data, or encrypt files. Malware can spread through various means, including email attachments, infected software downloads, malicious websites, or social engineering tactics. Once installed, it can be used to steal data, disrupt operations, or gain unauthorized access to sensitive systems or networks. Protection against malware requires a multi-layered approach, which involves implementing security software, regularly updating software and systems, and training users to recognize and avoid potential threats. It is also essential to back up critical data regularly in case of a malware attack [46].

Phishing is a type of social engineering attack that tricks individuals into revealing sensitive information, such as passwords or credit card numbers, through fraudulent communication methods such as email or text messages. Phishing attacks involve several steps that scammers use to trick people into divulging their sensitive information. The first step is to send a fraudulent message, such as an email or text, pretending to be a trustworthy organization like a bank or social media platform. These messages often

contain links to fake websites or malicious attachments that can steal personal data or infect the victim's device. If the victim clicks on the link or opens the attachment, they may be taken to a phony login page or unintentionally download malware that gives the attacker control of their system. Phishing attacks are a serious threat that can lead to identity theft, financial losses, and damage to one's reputation. Cybercriminals are using more sophisticated methods, such as targeted phishing (spear-phishing), texting (smishing), or voice calls (vishing), to deceive people [69]. To prevent falling prey to phishing attacks, one must take technical measures and be aware of the risks. Some best practices for avoiding phishing scams are to avoid clicking on links or opening attachments from unknown sources, verify the sender and website address, use two-factor authentication, keep software and security tools updated, and educate oneself on how to identify and report potential phishing attacks.

Denial-of-Service (DoS) attacks are attempts to make a website or network unavailable to its intended users by overwhelming it with traffic or other requests. To disrupt or prevent access to a website, network, or service, cybercriminals may execute Denial-of-Service (DoS) attacks, which involve flooding the targeted system with traffic so that it cannot respond to legitimate requests. There are various types of DoS attacks, such as flood attacks that send a large number of requests to a server, amplification attacks that exploit vulnerabilities to amplify the attack size, and Distributed Denial-of-Service (DDoS) attacks that use multiple devices to send traffic to a system. The impact of a DoS attack can be temporary inconvenience or severe financial loss if the targeted system is crucial to an organization's operation. Preventing DoS attacks involves implementing security measures like firewalls and monitoring network traffic, using intrusion detection and prevention systems, distributing server resources across multiple data centers, educating users on recognizing and reporting potential attacks, and using specialized services like DDoS protection provided by internet service providers or cloud services [46].

Man-in-the-Middle (MitM) attacks involve intercepting communication between two parties to steal information or inject malicious code. Man-in-the-Middle (MitM) attacks are a type of cyberattack that allow a hacker to intercept and modify communication between two parties, such as a user and a website. The attacker exploits weaknesses in the communication channel to redirect traffic to a different destination, while the user and the website are unaware of the interception. Common MitM attacks

include session hijacking, DNS spoofing, SSL stripping, and Wi-Fi eavesdropping. These attacks can lead to serious consequences, including stolen credentials, financial loss, or data breaches. To prevent MitM attacks, it is important to use SSL/TLS encryption, verify SSL certificates, avoid public Wi-Fi networks, monitor network traffic, and educate users on recognizing and reporting potential attacks [88].

Advanced Persistent Threats (APTs) are long-term targeted attacks that aim to compromise networks or devices to gain access to sensitive information or systems. Advanced Persistent Threats (APTs) refer to a type of cyber-attack that uses sophisticated and targeted techniques to gain unauthorized access to sensitive information over an extended period, often with the aim of stealing valuable data or intellectual property. These attacks are designed to remain undetected and involve a series of steps that include gathering information about the target organization, creating malware or other tools to exploit vulnerabilities, delivering the malware or tools, exploiting the target organization's systems, evading detection, and establishing a foothold in the target organization's systems to continue stealing data. APTs are often carried out by well-resourced attackers such as nation-state actors or criminal groups and can result in severe consequences such as stolen intellectual property, financial loss, and reputational damage. To protect against APTs, organizations should regularly update their software and security tools, implement multi-factor authentication and strong password policies, conduct security assessments, implement network segmentation, and access controls, and educate employees on how to recognize and report potential APTs [46].

Botnets refer to networks of infected computers that can be controlled remotely to carry out malicious activities such as spamming or launching Distributed Denial-of-Service (DDoS) attacks. Botnets are networks of compromised computers controlled remotely by cybercriminals to carry out malicious activities, such as DDoS attacks, spam campaigns, stealing data, or cryptocurrency mining. Cybercriminals infect a large number of computers with malware using social engineering tactics like phishing emails or infected downloads. Once infected, the malware connects the compromised computer to a central command and control server, allowing the attacker to remotely control the botnet. Botnet attacks can cause significant financial loss, data breaches, or reputational damage. Organizations can prevent botnet attacks by updating software and security tools regularly, using anti-malware software and firewalls, educating employees on how to

recognize and avoid phishing emails and infected downloads, implementing network segmentation, and monitoring network traffic [55].

Password attacks involve guessing or cracking passwords to gain unauthorized access to systems or accounts. To gain unauthorized access to a user's account or system, cybercriminals use password attacks, which involve guessing or stealing the user's password. Some common types of password attacks are brute force attacks, dictionary attacks, phishing attacks, and keylogging. If successful, password attacks can have severe consequences, such as stealing sensitive data or causing other damage. To protect against password attacks, individuals and organizations should implement security measures, such as using strong and unique passwords, implementing multi-factor authentication, regularly changing passwords, avoiding password reuse, educating employees and users about phishing attacks, and monitoring network activity and user behavior for signs of suspicious activity or unauthorized access [92].

Insider threats involve individuals within an organization intentionally or unintentionally causing harm to systems or data. Insider threats refer to the cybersecurity risks posed by authorized individuals who have access to an organization's systems, data, or resources, and can cause harm to the organization either intentionally or unintentionally. Insiders can be employees, contractors, or business partners. Malicious insiders intend to harm the organization by stealing sensitive data, installing malware, or sabotaging systems, whereas accidental insiders inadvertently cause damage by misconfiguring systems, clicking on phishing links, or unintentionally disclosing sensitive information. Compromised insiders have had their credentials or access stolen or compromised, enabling attackers to gain unauthorized access. Insider threats can have severe impacts, such as financial loss, data breaches, or reputational damage. To protect against insider threats, organizations should implement access controls, monitoring systems, and security awareness training programs for employees. Additionally, conducting background checks and screening procedures during the hiring process, monitoring network activity and user behavior for signs of suspicious activity or unauthorized access, and implementing incident response and data backup plans are effective measures against insider threats [92].

Physical attacks involve physically damaging or stealing computer equipment or stealing data using physical means, such as stealing or tampering with storage devices. Physical attacks are a form of cybersecurity threat that involves gaining physical access

to an organization's systems, devices, or infrastructure. These types of attacks can be carried out by both insiders and outsiders and can lead to the theft, damage, or disruption of crucial assets. There are several common types of physical attacks, including the theft of physical devices, unauthorized access to facilities, destruction, or damage of infrastructure, and tampering with devices. The consequences of physical attacks can be severe, resulting in significant financial loss, data breaches, or harm to the organization's reputation. To protect against physical attacks, organizations should implement a range of security measures, including physical security measures such as access controls, surveillance cameras, and alarm systems, encryption of data on devices, and remote wiping capabilities to prevent theft or loss of devices, conducting regular physical security audits, implementing security awareness training programs for employees, and monitoring network activity and user behavior for signs of suspicious activity or unauthorized access [92].

3.2 Potential Threats to Various Layers of IoT

IoT is an ever-growing network of interconnected devices that provide exceptional levels of convenience and efficiency. Despite its benefits, as the IoT expands, it becomes more exposed to potential risks. These risks could take place at different levels of the IoT, including the physical, network, application, and data layers (Figure 8) [70]. Physical tampering or damage to devices is a possible threat at the physical layer, while unauthorized access or denial of service can occur in the network layer. The application layer is prone to injection attacks, and the data layer is vulnerable to data interception or manipulation. Therefore, individuals and organizations must recognize the potential hazards to the various layers of the IoT and implement suitable measures to safeguard against them.

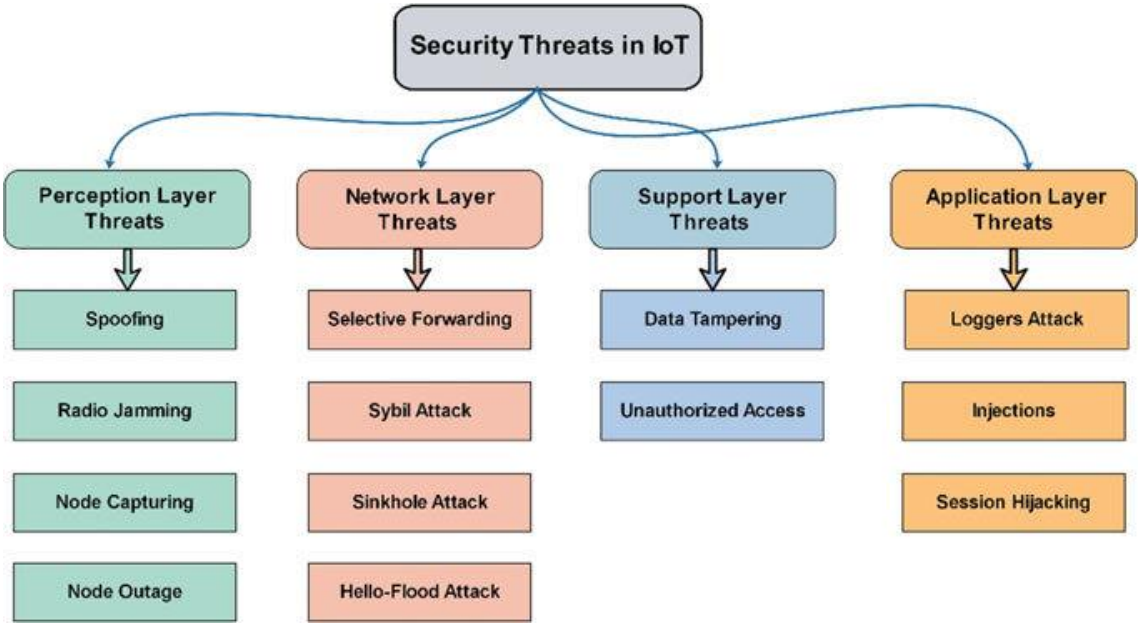

Figure 8. Categorizing malicious attacks according to the levels of IoT.

3.2.1 Perception Layer Threats

Wireless technologies such as GPS devices, sensors, and RFID readers that utilize intelligence embedded technologies are vulnerable to security threats. The primary threats are outlined below:

One type of attack is *spoofing*, where the attacker into the sensor network is sending a fraudulent broadcast message deceiving it into believing that it is legitimate and originating from the source of origin. This kind of situation can lead to the attacker obtaining complete control of the specific system, making it vulnerable to attack [71].

Another type of attack is *radio* or *signal jamming*, which is a type of denial-of-service (DoS) attack that conceives the channel of communication among the nodes, obstructing them from exchanging data with one another. [72].

Device-tampering or *node-capturing* is another attack where the attacker physically seizes the sensor node and substitutes it with a harmful node, allowing them to gain complete control of the captured node and harming the network [73].

A *path-based attack* is a type of DoS attack, in which an attacker overwhelms the multi-hop end-to-end communication path by flooding it with spurious packets that are

either replayed or injected. This type of attack can overpower sensor nodes located far away, leading to decreased system availability, and draining the batteries of nodes.

The *node outage attack* can halt the operational capability of the network elements either logically or physically. Collect, read and enable operation node services are obstructed from this attack, which results in stopping the proper functioning of the network components [73].

Eavesdropping is also a possible attack where the wireless characteristics of RFID systems enable the attacker to intercept and obtain confidential information, such as data being transmitted between tags and readers or passwords, resulting in a compromised system.

3.2.2 Network Layer Threats

Next-generation networks, or the network layer, is susceptible to a range of different types of security risks. These threats are discussed below:

Selective Forwarding: Is an attack, where malicious nodes selectively drop certain messages to prevent them from propagating. The attacker can forward remaining traffic to conceal their actions. There are several types of selective forwarding attacks, such as those that target a specific node or multiple nodes. These attacks can lead to denial-of-service (DoS) attacks [74].

Sybil Attack: This is a form of attack in which a single malicious node takes on multiple identities, presenting multiple identities to other nodes in the network, thereby reducing the effectiveness of fault-tolerant schemes [75].

Sinkhole Attack (Blackhole): This type of attack leads to increased competition for resources among nearby nodes, resulting in congestion and increased energy consumption. This attack can also make the sensor network may become susceptible to other forms of DoS attacks [76].

Wormhole: This type of denial-of-service (DoS) attack is a technique that involves moving data packets from their original location within a network by transmitting small portions of data over a connection with low latency.

Man-in-the-Middle Attack: This type of attack involves unauthorized interception of private communications between two parties, allowing the attacker to monitor or manipulate them [62].

Hello-flood Attack: Is a type of attack that floods a communication channel with a large number of unnecessary messages, resulting in high traffic and congestion in the channel [72].

Acknowledgment Flooding: This attack disrupts routing algorithms in sensor-based systems by transmitting inaccurate data to neighboring nodes through the use of acknowledgments.

3.2.3 Support Layer Threats

The support layer is primarily focused on data storage technologies and is susceptible to various threats that are outlined below:

Data Tampering: This attack occurs when an individual with access to the system intentionally modifies data for personal or third-party commercial benefits [77].

DoS Attack: Similar to attacks in previous layers, The support layer of IoT system can be susceptible to DoS attacks, which can cause service unavailability and system shutdown.

Unauthorized Access: It is relatively simple for attackers to gain unauthorized access to the system, deny access to IoT services, or delete sensitive data, causing severe damage to the system. As a result, gaining access without authorization can have severe consequences for the system [78].

3.2.4 Application Layer Threats

The application layer of IoT includes customized services based on users' needs, such as interfaces for controlling devices. The services provided by this layer are the target of various types of threats, which include:

Sniffer/Loggers: In this type of attack, attackers may use programs such as sniffer/logger to intercept and gather confidential information from network traffic, including email content and passwords.

Injection: Attackers can insert code into the application, causing problems like data loss and corruption [79].

Session Hijacking: Attackers exploit vulnerabilities in the authentication and session management processes to masquerade as legitimate users and gain unauthorized access to their sensitive information [79].

DDoS (Distributed Denial of Service): Similar to traditional DoS attacks but executed by multiple attackers at once.

Social Engineering: A serious threat in which attackers manipulate users into providing sensitive information via chat or other means.

3.2.5 Business Layer Threats

The business layer is a layer in the IoT architecture that is accountable for managing the business logic of an IoT system. It provides an interface among the application layer and the data processing layer. The business layer is where the actual value of an IoT system is derived, as it determines how data collected from the perception and transport layers is processed and used to create value for the organization. However, the layer that deals with business operations is also susceptible to various security risks. Some of these threats to the business layer in IoT include [93]:

Data tampering: Attackers may try to manipulate data in the business layer to interrupt normal functions or obtain unauthorized entry to confidential data.

Unauthorized access: Hackers may attempt to illicitly obtain access to the business layer to steal or cause damage to the IoT system.

Malware attacks: Malware can be used to infect devices connected to the business layer, allowing attackers to gain access and control over the system.

Denial of service (DoS) attacks: The main goal of these attacks is to disrupt the availability of the IoT system, making it difficult or impossible for users to access it.

Social engineering: Attackers can resort to social engineering techniques to deceive users into revealing their login credentials or other confidential data, which can be misused to gain unauthorized entry into the business layer [93].

To prevent these risks, it's crucial to apply robust security measures, like access control, encryption, and intrusion detection systems at the business layer. Staying aware of the latest security threats and vulnerabilities, and periodically reviewing and revising security policies and protocols is also crucial [87] [93].

3.3 Defending Against Cyberthreats with IoT

Although IoT can help enhance cybersecurity, it is not a complete solution to prevent the increase of cyber threats. To secure IoT devices, appropriate techniques to ensure security, such as encoding, two-factor authentication, and regular security assessments must be implemented. IoT devices can also be used to gather data and analyze patterns to detect and respond to cyber threats. However, since cybercriminals continually develop new attack methods, it's important to understand that IoT alone cannot entirely eliminate cyber threats.

In order to comprehensively address cybersecurity, a multi-faceted approach is necessary. This approach includes securing not only IoT devices, but also network infrastructure, policies and procedures, and user education and awareness.

The Internet of Things (IoT) can significantly aid in defending against cyber threats in various ways. One such way is by using IoT devices to monitor networks and detect potential security breaches. IoT sensors can detect abnormal network activity, which can then alert security personnel to investigate further and address the issues before they escalate [63].

Moreover, IoT can improve access control and authentication by implementing advanced security measures such as biometric identification and multi-factor authentication. This can aid in thwarting unauthorized access to confidential information and systems, thereby increasing overall security [90].

In addition, IoT devices have the capability to gather and scrutinize vast amounts of data for the purpose of detecting potential security risks. By utilizing machine learning algorithms to recognize suspicious patterns of activity, security personnel can be notified promptly, enabling them to take swift action if necessary [90].

Another way IoT can aid in defending against cyber threats is by implementing security measures such as encryption and firewalls at the device level. This helps prevent unauthorized access to sensitive information by encrypting data both at rest and in transit [93].

IoT can also improve cybersecurity in other ways, such as by providing improved visibility into network activity and allowing for real-time monitoring of potential threats [90].

Additionally, IoT devices can automate security processes like software updates and patches, ensuring that all devices in the network are running the latest security software and are less vulnerable to attack [59].

Centralized management of IoT devices also allows for greater control over security policies and configurations, minimizing the risk of cyber attacks. IoT devices can provide valuable data that can be used for advanced analytics and threat detection, helping organizations identify potential threats and take proactive measures to prevent them [63].

While IoT can be useful in enhancing security measures, it's essential to note that it cannot completely eliminate the risk of cyber attacks. A comprehensive and multi-layered security approach is necessary to effectively defend against cyber threats. To effectively protect against cyber-attacks, IoT security measures must be implemented alongside other security measures.

4 The importance of cybersecurity for IoT

The rapid expansion of the Internet of Things (IoT) has brought numerous benefits and opportunities for both individuals and businesses. Nevertheless, the increased connectivity and interactivity among devices and systems have resulted in a rise in potential security risks and threats. Consequently, cybersecurity has become a crucial factor in maintaining the safety and trustworthiness of IoT systems.

One of the major challenges in securing IoT devices is the vast number of devices with varying capabilities and vulnerabilities. These devices can range from simple sensors and actuators to complex machines and systems. The large quantity of devices and the fact that they are often deployed in remote and uncontrolled environments makes it challenging to manage and secure them [92].

Another challenge in securing IoT devices is their limited processing power and memory. Many IoT devices are designed to be low-power and low-cost, which means they may not be able to handle advanced security measures such as encryption and authentication. This makes them susceptible to attacks that exploit their weak security protocols [92].

The significance of cybersecurity for IoT cannot be overstated, as IoT devices are increasingly being used in critical applications such as healthcare, transportation, and energy management. Any security breach in these systems can have severe outcomes that may result in loss of life, damage to property, and disruption of essential services. Therefore, it is crucial to guarantee that IoT devices are designed and implemented with security as a top priority [92].

One solution to securing IoT devices is to use a layered security architecture, which involves implementing multiple layers of security measures like firewalls, intrusion detection systems, encryption, and access control. This approach can help to mitigate the risks of attacks and limit the damage caused by security breaches [90].

Another approach to securing IoT devices is to utilize machine learning and artificial intelligence (AI) technologies, which can aid in detecting and preventing attacks by analyzing patterns in the data generated by IoT devices. For example, machine learning

algorithms can identify anomalies in network traffic or usage patterns that may indicate a security breach. This can enable proactive measures to be taken to prevent or mitigate the impact of a potential attack [63].

To sum up, the significance of cybersecurity for IoT cannot be underestimated. The increasing use of IoT devices in critical applications means that any security breach can have serious consequences. Therefore, it is crucial to ensure that IoT devices are designed and implemented with security as a top priority, utilizing a layered security architecture, machine learning and AI technologies, and other advanced security measures. By adopting a thorough and preemptive strategy towards cybersecurity, we can ensure the safety and integrity of IoT systems and harness the full potential of this transformative technology.

4.1 Cyberdefense mechanisms for the IoT

Cyberdefense mechanisms for IoT can include various technologies and practices to address cybersecurity threats. One such mechanism is network segmentation, access control, authentication measures, encryption, firewalls, regular software updates and patches. It's important to note that while these mechanisms can improve IoT security, a comprehensive and multi-layered approach to cybersecurity is necessary to effectively defend against cyber threats. The following is an extensive compilation of cyber defense mechanisms designed to protect IoT.

Network segmentation involves dividing a network into smaller subnetworks, each with its own security policies and access controls. This helps to limit the spread of a security breach to other parts of the network. For example, IoT devices can be segmented by location, function, or other criteria to create smaller, more manageable subnetworks. Each subnetwork can have its own access controls and security policies, ensuring that a breach in one part of the network does not compromise the entire network.

Access control mechanisms can be implemented to restrict access to IoT devices and ensure that only authorized users or devices are granted access. Access control policies can be implemented at the network, device, and application levels. For example, access control lists can be used to define which devices are allowed to communicate with

each other, while role-based access control can be used to define the privileges of different users [64].

Encryption and authentication are critical cyberdefense mechanisms for the IoT. Encryption involves the use of cryptographic algorithms to secure data transmission between IoT devices and servers. The data is encrypted in transit and decrypted upon receipt, ensuring that it cannot be intercepted or modified by hackers. Common encryption techniques used in IoT systems include Advanced Encryption Standard (AES) and Transport Layer Security (TLS). Authentication, on the other hand, is the process of verifying the identity of a user or device. Digital certificates and secure protocols such as Public Key Infrastructure (PKI) can be used to authenticate IoT devices and ensure that only authorized users or devices are granted access to the network. Authentication can also be used to prevent unauthorized access to IoT devices, by requiring a valid username and password or other authentication factors [64].

Firewalls are an effective way to defend against cyber-attacks on IoT devices and networks. Essentially, a firewall is a system that controls both incoming and outgoing traffic on a network, using a predetermined set of security rules. This system can be put into place through hardware, software, or a combination of the two. The firewall can act as a line of defense to keep unauthorized individuals or programs from gaining access to the IoT network, and thereby prevent data breaches. By only allowing authorized traffic through and blocking unauthorized traffic, firewalls can stop threats like malware or hackers from taking control of IoT devices. Additionally, firewalls can enforce access control policies, allowing only authorized devices or users to connect to the network. This can be implemented at various levels of the network, such as at the network perimeter, device level, or both. For instance, network perimeter firewalls can protect the entire IoT network from external threats, while device-level firewalls can safeguard individual devices from internal threats. Moreover, firewalls can be configured to offer other security features including intrusion detection and prevention, deep packet inspection, and virtual private network (VPN) connectivity. Intrusion detection and prevention can detect and block suspicious traffic or activity on the network, while deep packet inspection can scan the content of data packets for any signs of danger. VPN connectivity, on the other hand, can offer a secure and encrypted connection between IoT devices and the network, ensuring that data is transmitted securely [93].

Regular firmware and software updates can address known vulnerabilities and security issues in IoT devices. These updates can be implemented through Over-The-Air (OTA) updates or through manual updates. OTA updates can be particularly useful for IoT devices that are deployed in remote or inaccessible locations. Firmware and software updates should be performed regularly and promptly to ensure that known vulnerabilities are addressed as soon as possible [62].

Advanced Analytics and Threat Detection: Implementing advanced analytics and threat detection mechanisms can help identify and respond to potential security threats before they can cause damage. This mechanism involves analyzing data from IoT devices to identify patterns and anomalies that could indicate a potential attack [63].

Threat detection and response mechanisms can be implemented to identify and react to security risks immediately. This can include the use of intrusion detection and prevention systems, as well as automated response mechanisms. Intrusion detection systems can detect unusual activity on the network, while intrusion prevention systems can block suspicious traffic or activity. Automated response mechanisms can be used to take immediate action in response to security breaches, such as isolating compromised devices or shutting down affected systems [63].

Physical security measures can prevent unauthorized access to IoT devices. These measures can be particularly important in cases where IoT devices are deployed in public spaces or industrial settings. Tamper-resistant seals can be used to protect IoT devices from physical tampering, while secure enclosures can be used to protect IoT devices from unauthorized access. Physical security measures can also include monitoring and surveillance, to identify and react to security breaches immediately [64].

Security Information and Event Management (SIEM): SIEM solutions can help gather and examine data from multiple origins to detect possible security risks. This mechanism can help organizations identify and respond to security incidents in real-time.

Incident Response Plans: Organizations can respond promptly and efficiently to cyberattacks by having a prepared incident response plan. This mechanism involves creating a plan for detecting, investigating, and responding to potential security incidents [90].

Blockchain technology can be used to secure IoT devices and networks through the use of decentralized ledgers and smart contracts. Blockchain technology provides an immutable and tamper-proof ledger of transactions, ensuring that data cannot be modified

or deleted without permission. This can provide an added layer of security and transparency to IoT transactions, ensuring that data is secure and can be trusted. Smart contracts can be used to define the terms and conditions of IoT transactions, ensuring that all parties involved are aware of their obligations [65].

In summary, the cyberdefense mechanisms for IoT include authentication and access control, encryption, network segmentation, firewalls, firmware and software updates, and security assessments and penetration testing. These mechanisms can be used in combination to create a layered approach to security and help protect IoT devices and networks from cyber threats. and responsibilities.

4.2 Securing the Internet of Things: A Layer-by-Layer Approach to IoT Security

The security of IoT is addressed through multiple layers of security solutions, each of which addresses specific security concerns. These layers include the application layer, the support layer, the network layer, and the perception layer. Each layer employs various security mechanisms such as encryption, firewalls, [93] and intrusion detection systems to ensure the security and integrity of IoT devices and their data. By implementing these security solutions, IoT systems can protect against various threats such as DDoS attacks, unauthorized access, and tampering with data, among others.

4.2.1 Ensuring Secure Communication in the Perception Layer of IoT

Securing the perception layer in IoT has been a concern for a long time. The different devices in this layer, such as sensors, RFID readers, and GPS, require efficient security measures to protect against cyber-attacks. In fact, poor physical security has been identified as one of the top 10 IoT vulnerabilities by OWASP [96]. Therefore, a physical identity and access management policy should be defined to ensure that only authorized personnel have access to sensitive data generated by physical objects. Similarly,

authentication and authorization requirements must also be satisfied to secure IoT data [80].

Data collection is another critical issue in the perception layer, which can be examined under two headings: multimedia data collection and image data collection. Multimedia data collection can be secured using techniques such as multimedia compression, steganography, watermarking, encryption, time session, and intellectual property. On the other hand, image data collection can be secured using image compression and CRC [62].

Cryptographic processing is another key task in securing sensor data in IoT. This involves operations like encryption and decryption, key and hash generation, and sign and verify hashes to ensure data privacy. Risk assessment is also essential to determine the potential threat and risks associated with an IoT system. Organizations like NIST, ISO, and IEC have developed guidelines for conducting risk assessment to determine the suitable measures for minimizing or removing risks in the process of risk mitigation [81],[82],[83].

In conclusion, securing the perception layer in IoT is crucial to prevent unauthorized access and data breaches. By implementing physical and logical security measures, organizations can protect themselves against cyber-attacks and ensure secure communication in the perception layer.

4.2.2 Enhancing Security in the Network Layer

The network layer of IoT can be divided into two sub-layers, wireless and wired, both of which require proper security measures to ensure the safety of the system. The wireless sub-layer can be secured by developing authentication and key management protocols, such as SSL/TLS and IPsec, which provide authentication, confidentiality, and integrity for each layer. Private Pre-Shared Key (PPSK) can also be used to define the access domain for each type of device connected to the network, ensuring unique keys are provided for each device [84].

For the wired sub-layer, firewalls and Intrusion Prevention System (IPS) can be applied to prevent unauthorized access, detect anomalies, and block malicious traffic. Network segmentation can be used to divide the network into smaller segments,

controlling access to each based on predefined rules, while intrusion detection and prevention can be used to monitor network traffic for suspicious activity and prevent attacks in real-time [93].

To further enhance security in the network layer, it's crucial to implement secure communication protocols like TLS or SSL to encrypt data transmission and prevent unauthorized interception. It's also essential to disable default and guest passwords in network devices like routers and gateways and implement strong password policies that involve periodic changes [93].

In conclusion, securing the network layer is vital in the overall security of IoT systems. A combination of security measures and techniques, including multi-layered security, should be implemented to mitigate the risk of attacks and ensure the confidentiality, integrity, and availability of IoT systems.

4.2.3 Ensuring Security in IoT's Support Layer

To ensure security in the support layer of IoT, organizations need to implement a range of security measures and best practices. One approach is to use strong authentication and access control mechanisms to limit access to IoT devices and systems. This can include the use of multi-factor authentication, strong passwords, and access control policies that restrict access to specific users or devices [85].

Another important measure is to implement secure communication protocols and encryption mechanisms to protect data transmission and prevent unauthorized interception. This can involve the use of SSL/TLS protocols, which can encrypt data at the transport layer, as well as IP security protocols (IPSec) that can provide confidentiality, authenticity, and integrity at the network layer [87].

In addition to these measures, organizations need to regularly update and patch IoT devices and systems to address vulnerabilities and protect against emerging threats. This can include implementing automatic updates and regular security audits to identify and remediate vulnerabilities.

Another key factor is to ensure that IoT devices are deployed in secure environments and that physical security measures are in place to prevent unauthorized access. This can include the use of secure storage facilities, locked cabinets, and access control mechanisms to prevent unauthorized access to IoT devices and systems [87].

Overall, ensuring security in the support layer of IoT requires a holistic approach that addresses a range of security concerns and best practices. By implementing strong authentication and access control mechanisms [87], using secure communication protocols and encryption mechanisms, updating and patching IoT devices and systems, and deploying IoT devices in secure environments, organizations can mitigate the risk of security threats and protect their IoT systems and data.

4.2.4 Protecting Applications: Strategies for Application Layer Security

Securing IoT applications at the application layer is a crucial aspect of protecting IoT devices and systems from cyber-attacks. The application layer is responsible for the actual processing of data and commands between IoT devices, as well as between devices and cloud-based servers.

One key approach to securing the IoT application layer is the use of secure communication protocols such as HTTPS, MQTT, or CoAP. These protocols employ encryption and authentication mechanisms to ensure that data transmitted between devices and servers is secure and not tampered with. Additionally, access control mechanisms can be employed to limit the data that each device can access and send, as well as to ensure that only authorized devices are communicating with each other [87] [88].

Another important strategy for securing IoT applications at the application layer is the use of secure software development practices. This includes writing secure code, conducting thorough testing and validation, and ensuring that software updates are implemented in a secure manner. The use of secure coding standards can help to mitigate potential security vulnerabilities in IoT applications [59].

In addition to these technical measures, organizations can also implement security policies and procedures to ensure that IoT devices and applications are being used in a secure manner. This includes training employees on how to identify and respond to potential security threats, conducting regular security assessments and audits, and implementing incident response plans in case of a security breach [92].

Logging and auditing mechanisms should be in place to monitor access and detect suspicious activity. This includes logging user and device activity, as well as network traffic and system events [31].

Authentication and Authorization process verify the identity of users or devices and determine what actions they are authorized to perform. Strong authentication and authorization mechanisms should be in place to prevent unauthorized access [86].

Encryption is employed to safeguard information while it is being transmitted and at rest by converting it into a form that is unreadable without the correct decryption key. End-to-end encryption is especially important in IoT systems, where data may be transmitted through multiple devices and networks [94].

Overall, securing IoT applications at the application layer is a multifaceted task that requires a combination of technical measures, secure software development practices, and organizational policies and procedures. By taking a comprehensive approach to IoT security, organizations can help to ensure the safety and reliability of their IoT devices and systems.

4.2.5 Securing the Business Layer in IoT Architecture: Best Practices and Strategies

Securing the business layer in IoT architecture is crucial to ensure the safe and efficient functioning of IoT systems. Below are some measures that can be taken to secure the business layer from threats:

Secure authentication: Implement strong and secure authentication methods to ensure that only authorized users can access the business layer. This can be achieved through the use of multi-factor authentication, such as passwords, biometric verification, and smart cards [93].

Secure Communication Protocols: To secure communication protocols in the business layer, it's important to use secure communication protocols such as TLS (Transport Layer Security) and SSL (Secure Sockets Layer) to ensure secure data transmission. Also, ensure that the device only communicates with trusted sources and has a secure authentication process [87] [93].

Encryption: Implement end-to-end encryption to protect data transmission between the business layer and other layers. Data stored in the business layer should be encrypted to prevent unauthorized access. This can be accomplished by utilizing AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) which is some of the various encryption algorithms [62].

Strong Access Control: Access control is critical for securing the business layer. Devices should have a strong authentication process, such as two-factor authentication, and only allow authorized users to access the data. Additionally, access control should be regularly reviewed and updated to ensure it remains secure [49].

Regular Software Updates: Software updates should be regularly applied to devices to patch vulnerabilities and ensure they remain secure. This includes both the operating system and any applications running on the device [62].

Security testing: Intrusion detection and prevention systems (IDPS) should be implemented to monitor and detect any unauthorized access attempts. This can include firewalls, intrusion detection software, and antivirus software. Additionally, regular audits and vulnerability assessments should be conducted to identify and address any weaknesses in the system [93].

Data backup: Regularly backup data from the business layer to ensure that critical information is not lost in the event of a security breach or system failure.

Disaster recovery plan: Develop a disaster recovery plan to ensure that the business layer can quickly recover in the event of a security breach or system failure [59].

Physical Security Measures: Physical security measures such as access control to the location where the devices are stored, video surveillance, and security personnel should be implemented to prevent unauthorized physical access to the devices [59].

By implementing these measures, the business layer in IoT architecture can be secured from threats and ensure the safe and efficient functioning of IoT systems.

5 Conclusions

The technology known as the Internet of Things (IoT) has gained significant popularity due to its ability to interconnect various physical devices to the internet for greater convenience and efficiency in our daily lives. However, the rise of IoT has also attracted the attention of attackers who are continuously searching for vulnerabilities in security, including device and data transport attacks. This poses a serious threat to the security and privacy of IoT devices and networks. Researchers have taken on the task of enhancing the security of IoT devices by exploring different types of security attacks and proposing solutions to make IoT more secure.

The article provides an overview of IoT, its potential benefits in various areas, and the major security issues associated with IoT. It identifies key security challenges, such as confidentiality, privacy, and trust in entities, and emphasizes that addressing these challenges is essential for establishing more secure and widely available IoT devices and services. Various approaches and strategies are proposed for securing IoT devices and networks, including encryption, authentication, access control, network segmentation, firmware and software updates, physical security, threat detection and response, and blockchain technology.

The researchers recommend using digital signatures with lightweight operations for signature and verification to provide enhanced security for IoT devices. They also plan to explore the utilization of various lightweight protocols and cryptographic algorithms that utilize robust encryption and authentication techniques for enhancing security in IoT devices in the future. However, a holistic and integrated approach is required, which takes into account the technical, organizational, and human factors involved in cybersecurity.

In the future, continued innovation and collaboration are expected in the field of cybersecurity and the IoT. This could include the development of new standards and regulations, the use of advanced analytics and machine learning techniques, and the integration of cybersecurity into the design and development of IoT devices and systems. These efforts will be vital in ensuring the security and privacy of IoT devices and networks and safeguarding the valuable data they contain.

6 Bibliography

[1] Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B. Gupta, “An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework”, Future Generation Computer Systems, June 2018.

[2] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, Talha Kamal, “A Review on Internet of Things (IoT)”, International Journal of Computer Applications, March 2015

[3] Mark Weiser, “The computer for the 21st century”, Sci. Amer., 1991.

[4] Kevin Ashton, ”That ’Internet of Things’ Thing”, RFID Journal, June 2009

[5] Johan Sigholm, “Non-State Actors in Cyberspace Operations”, Nov 2016.

[6] Wenjie Gong, “The Internet of Things (IoT): What is the potential of the internet of things (IoT) as a marketing tool?”, July 2016

[7] Mohammad AIYasfo, “Internet of Things”, November 2019, LinkedIn.

[8] Luigi Atzori, Antonio Iera, Giacomo Morabito, “The Internet of Things: A survey”, Computer Networks, October 2010.

[9] Marco Lombardi, Francesco Pascale, Domenico Santaniello, “Internet of Things: A General Overview between Architectures, Protocols and Applications”, Special Issue Wireless IoT Network Protocols, February 2021

[10] Sun, C. “Application of RFID Technology for Logistics on Internet of Things”. [Citation Time(s):1], 2012

[11] Aggarwal, R. and Lal Das, M. “RFID Security in the Context of Internet of Things”, First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56.

[12] Moeinfar, D., Shamsi, H. Nafar, F. “Design and Implementation of a Low-Power Active RFID for Container Tracking @ 2.4 GHz Frequency: Scientific Research”, Scientific Research, 2012.

2012.

[13] Bicknell, IPv6 Internet Broken, Verizon Route Prefix Length Policy, 2009.

[14] Grieco A., Occhipinti, E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. Bollettino de Oculistica, Suppl. 7, 99-111.

[15] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J.P. Makela, R. Pichna, J. Vallstron, “Handoff in hybrid mobile data networks”, IEEE Personal Communications (Volume: 7, Issue: 2), April 2000.

[16] Xian-Yi Chen, Zhi-Gang Jin, “Research on Key Technology and Applications for Internet of Things”, Volume 33, Pages 561-566, 2012.

[17] Th. Arampatzis, J. Lygeros, S. Manesis, “A Survey of Applications of Wireless Sensors and Wireless Sensor Networks”, Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005.

[18] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures”, International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015.

[19] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys & Tutorials, June 2015.

[20] Kozlov, Denis, Veijalainen Jari, Ali Yasir, “Security and privacy threats in IoT architectures”. Conference on Body Area Networks, February, 2012.

[21] Xiaohui Xu, “Study on security problems and key technologies of the Internet of things”. International Conference on Computational and Information Sciences (ICCIS), June 2013.

[22] Mohammed Riyadh ABDMEZIEM, D. Tandjaoui, Imed Romdhani, “Architecting the Internet of Things: State of the Art” ,Springer International Publishing , August 2015

[23] Muhammad Burhan, Rana Asif Rehman, Bilal Khan, Byung-Seo Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey”, Sensors 2018.

[24] Muhammad Burha, Rana Asif Rehman, Bilal Khan, Byung-Seo Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey”, August 2018.

[25] Khaled A. Alaghbari, Mohamad Hanif Md Saad, Aini Hussain & Muhammad Raisul Alam, “Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations”, Journal of Cloud Computing, 2022 .

[26] Pallavi Sethi, Smruti R. Sarang, “Internet of Things: Architectures, Protocols, and Applications”, Journal of Electrical and Computer Engineering, January 2017.

[27] Khan, R., Khan, S. U., Zaheer, R., Khan, S. “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges”, International Conference on Frontiers of Information Technology, 2012.

[28] Stephan Haller, Stamatis Karnouskos & Christoph Schroth “The Internet of Things in an Enterprise Context” , Lecture Notes in Computer Science, 2009 .

[29] F. Li, A. Lai, and D. Ddl, “Evidence of advanced persistent threat: A case study of malware for political espionage,” Malicious and Unwanted Software,International Conference on. IEEE, 2011.

[30] Paul Brous, Marijn Janssen, Paulien Herder, “The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations”, International Journal of Information Management, April 2020.

[31] Mohamed Abomhara, Geir M. Køien, “Cyber Security and the Internet of Things:

Vulnerabilities, Threats, Intruders and Attacks”, Journal of Cyber Security and Mobility, May 2015.

[32] Minahil Rana, Akasha Shafiq, Izwa Altaf, Mamoun Alazab, Khalid Mahmood, Shehzad Ashraf Chaudhry, Yousaf Bin Zikria, “A secure and lightweight authentication scheme for next generation IoT infrastructure,” Computer Communications, vol. 165, pp. 85–96, 2021.

[33] Houshyar Honar Pajooh, Mohammad Rashid. Fakhrul Alam, Serge Demidenko, “Multi-layer blockchain-based security architecture for internet of things,” Sensors, vol. 21, no. 3, 772 pages, 2021.

[34] G. M. Koien and V. A. Oleshchuk,“Aspects of Personal Privacy in Communications-Problems, Technology and Solutions”, River Publishers, 2013.

[35] Joseph Migga Kizza, “Guide to Computer Network Security”, Springer, 2013.

[36] Hans Gunter Brauch, “Concepts of security threats, challenges, vulnerabilities and risks”, Coping with Global Environmental Change, Disasters and Security, Springer, 2011.

[37] Kamal Dahbur, Bassil Mohammad, Ahmad Bisher Tarakji, “A survey of risks, threats and vulnerabilities in cloud computing,” Proceedings of the 2011 International conference on intelligent semantic Web-services and applications, 2011.

[38] R. K. Rainer and C. G. Cegielski, “Introduction to information systems: Enabling and transforming business”. John Wiley & Sons, 2010.

[39] A. J. Duncan, S. Creese, M. Goldsmith, “Insider attacks in cloud computing,” Trust, Security and Privacy in Computing and Communications (TrustCom),International Conference, IEEE, 2012.

[40] P. Baybutt, “Assessing risks from threats to process plants: Threat and vulnerability analysis,” Process Safety Progress, 2002.

[41] C. Tankard, “Advanced persistent threats and how to monitor and deter them,” Network security, 2011.

[42] F. Li, A. Lai, and D. Ddl, “Evidence of advanced persistent threat: A case study of malware for political espionage,” Malicious and Unwanted Software,International Conference on. IEEE, 2011.

[43] E. Bertino, L. D. Martino, F. Paci, A. C. Squicciarini, “Web services threats, vulnerabilities, and countermeasures,” Security for Web Services and Service-Oriented Architectures. Springer, 2010.

[44] B. Schneier, “Secrets and lies:digital security in a networked world”. John Wiley & Sons, 2011

[45] Amir Djenna, Saad Harous, Djamel Eddine Saidouni, “Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure”, Emerging Approaches for Secure and Resilient Cyber-Physical-Social Systems, May 2021.

[46] Jamal Mabrouki, Azidine Guezzaz, Ambrina Kanwa, “Internet of Things Security: Challenges and Key Issues”, September 2021.

[47] Akram Mohammed, “IoT security goals and attacks”, Geneva Business News, December 2020.

[48] Javier Lopez, Rodrigo Roman, and Cristina Alcaraz, “Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network”, 2009.

[49] Tarak Nandy, Mohd Yamani Idna Bin Idris, Rafidah Md Noor, Laiha Mat Kiah, Lau Sian L, “Review on Security of Internet of Things Authentication Mechanism” IEEE Access, October 2019.

[50] Poornima M. Chanal, Mahabaleshwar S. Kakkasageri, “Security and Privacy in IoT: A Survey” , Wireless Personal Communications, 2020.

[51] Rolf H. Weber, “Accountability in the Internet of Things”, Computer Law & Security Review, April 2011.

[52] Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, Jon Crowcroft, “Accountability in the IoT: Systems, Law, and Ways Forward”, July 2018.

[53] Azizi Majid, “Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022)” , Journal of Computer and Communications.

[54] Vinay Gautam, Raj Gaurang Tiwari, Anuj Kumar Jain, Ambuj Agarwal, “Research Pattern of Internet of Things and its Impact on Cyber Security”, International Conference on System Modeling & Advancement in Research Trends (SMART), February 2023

[55] Morteza Safaei Pour, Elias Bou-Harb, Kavita Varma, Nataliia Neshenko, Dimitris A. Pados, Kim-Kwang Raymond Choo “Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns”, Digital Investigation, April 2019.

[56] Ioannis Stellios, Panayiotis Kotzanikolaou, Christos Grigoriadis, “Assessing IoT enabled cyber-physical attack paths against critical systems”, Computers & Security, August 2021.

[57] Manish Snehi, Abhinav Bhandari , “Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks”, Computers & Security, May 2021.

[58] Tanzila Saba, Amjad Rehman Khan, Tariq Sadad, Seng-phil Hong, “Securing the IoT System of Smart City against Cyber Threats Using Deep Learning”, June 2022.

[59] Ömer Aslan, Semih Serkant Aktuğ , Merve Ozkan-Okay, Abdullah Asim Yilmaz, Erdal Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions”, Electronics, March 2023.

[60] Shapla Khanam1, Ismail Bin Ahmedy, Mohd Yamani Idna Idris, Mohamed Hisham Jaward, Aznul Qalid Bin Md Sabri “A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things”, November 2020, IEEE Access.

[61] Kholoud Y. Najmi, Mohammed A. AlZain, Mehedi Masud, N.Z. Jhanjhi, Jehad Al-Amri, Mohammed Baz, “A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability”, April 2021.

[62] Lo’ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, Muhannad Quwaider, “IoT Privacy and Security: Challenges and Solutions”, June 2020.

[63] Nickson M. Karie, Nor Masri Sahri, Paul Haskell-Dowland, “IoT Threat Detection Advances, Challenges and Future Directions”, Workshop on Emerging Technologies for Security in IoT (ETSecIoT), April 2020.

[64] Sita Rani , Aman Kataria, Vishal Sharma, Smarajit Ghosh, Vinod Karar, Kyungroul Lee, Chang Choi, “Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey”, April 2021.

[65] Sushree Bibhuprada B. Priyadarshini, Suraj Kumar Dash, Amrit Sahani, Brojo Kishore Mishra, Mahendra Prasad Nath “An Introduction to Security in Internet of Things (IoT) and Big Data”,

[66] Myriam Dunn Cavelty, “Cyber-threats”, The Routledge Handbook of Security Studies, 2009.

[67] Communications Authority of Kenya, “Cyber Threats on the Rise with Increased Reliance on ICTs in the Mitigation of COVID-19 Pandemic “ , January 2021.

[68] Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy, “Internet of things and ransomware: Evolution, mitigation and prevention”, Egyptian Informatics Journal, March 2022.

[69] Vipin Kumar, Jaideep Srivastava, Aleksandar Lazarevic , “Managing Cyber Threats: Issues, Approaches, and Challenges”.

[70] Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Abdulrahman A. Alshdadi, Gary B. Wills, “Cybercrime and DigitalForensics for IoT”, Principles of Internet of Things (IoT), January 2020.

[71] Aikaterini Mitrokotsa, Melanie R. Rieback , Andrew S. Tanenbaum, “Classifying RFID attacks and defenses”, Information Systems Frontiers , July 2010.

[72] Tuhin Borgohain, Uday Kumar, Sugata Sanyal, “Survey of Security and Privacy Issues of Internet of Things”, January 2015.

[73] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah, Kashif Naseer Qureshi, “Security Issues and Attacks in Wireless Sensor Network”, World Applied Sciences Journal , February 2014.

[74] Preeti Sharma, Monika Saluja, Krishan Kumar Saluja, “A REVIEW OF SELECTIVE FORWARDING ATTACKS IN WIRELESS SENSOR NETWORKS”, International Journal Of Advanced Smart Sensor Network Systems (IJASSN), July 2012.

[75] JongBeom Lim, HeonChang Yu, Joon-Min Gil, “Detecting Sybil Attacks in Cloud Computing Environments Based on Fail-Stop Signature”, Symmetry in Secure Cyber World, March 2017.

[76] Haojun Huang, Hao Yin, Geyong Min, Xu Zhang, Weixing Zhu, Yulei Wu, “Coordinate-Assisted Routing Approach to Bypass Routing Holes in Wireless Sensor Networks”, IEEE Communications Magazine, July 2017.

[77] Mian Muhammad Ahemd, Munam Ali Shah, Abdul Wahid, “IoT security: A layered approach for attacks & defenses”, International Conference on Communication Technologies (ComTech), 2017.

[78] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications, February 2015.

[79] Hemanta Kumar Kalita, Avijit Kar, “Wireless sensor network security analysis”, International journal of computer science & information Technology (IJCSIT), 2009.

2009.

[80] K. Aarika, Meriem Bouhlal, Rachida Ait Abdelouahid, Sanaa El Filali, “Perception layer security in the internet of things”, Procedia Computer Science, January 2020

[81] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, “Security in the Internet of Things: A Review”, International Conference on Computer Science and Electronics Engineering, 2012.

[82] David Jao, Stephen D. Miller, Ramarathnam Venkatesan, “Expander graphs based on GRH with an application to elliptic curve cryptography”, Journal of Number Theory, June 2009.

[83] Tony Chung, Utz Roedig, “DHB-KEY: An efficient key distribution scheme for wireless sensor networks”, IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008.

[84] Rahul Sharma, Nitin Pandey, Sunil Kumar Khatri, “Analysis of IoT security at network layer”, International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2017

[85] Hany F. Atlam, Gary B. Wills, “IoT Security, Privacy, Safety and Ethics”, Digital Twin Technologies and Smart Cities , Springer Nature Switzerland AG 2020 , March 2019.

[86] Engin Leloglu, Tolga Ayav, Burak Galip Aslan, “A review of cloud deployment models for e-learning systems”, Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2013

[87] Renya Nath N, Hiran V Nath , “Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges”, Computers and Electrical Engineering, May 2022.

[88] Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, Ioanna Kantzavelou, “IoT: Communication protocols and security threats”, Internet of Things and Cyber-Physical Systems, 2023

[89] Diptiben Ghelani, “Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review”, American Journal of Science, Engineering and Technology, 2022.

[90] Daniel Díaz López, María Blanco Uribe, Claudia Santiago Cely, Andrés Vega Torres, Nicolás Moreno Guataquira, Stefany Morón Castro, Pantaleone Nespoli, Félix Gómez Mármol, “Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM”, October 2018.

[91] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, “Internet of Things (IoT): A Literature Review”, Journal of Computer and Communication, January 2015.

[92] Pintu Kumar Sadhu, Venkata P. Yanambaka, Ahmed Abdelgawad, “Internet of Things: Security and Solutions Survey”, Sensors, 2022.

[93] Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios, “Securing the Internet of Things: Challenges, threats and solutions”, Internet of Things, March 2019.

[94] Engin Leloglu, “A Review of Security Concerns in Internet of Things”, Journal of Computer and Communications, January 2017.

[95] Baoan Lia, Jianjun Yub, “Research and application on the smart home based on component technologies and Internet of Things”, Procedia Engineering, 2011.

[96] Nick Johnston , “OWASP IoT Top 10”, 2019