International Journal of Engineering Science and Applied Mathematics
Volume.13, Number 6; June-2022;
ISSN: 2836-9521| Impact Factor: 5.78
https://zapjournals.com/Journals/index.php/ijesam
Published By: Zendo Academic Publishing

HOLISTIC APPROACH TO IOT SECURITY: TACKLING CHALLENGES AND ENSURING PROTECTION

[1]Mahmoud, R., [2]Yousuf, T., [3]Aloul, F., and [4]Zualkernan, I.

Article Info

Keywords: Internet of Things, IoT, security challenges, privacy, cyber threats, countermeasures, network layer, perception layer, application layer, encryption techniques.

Abstract

The Internet of Things (IoT) has revolutionized the way technology and appliances operate by connecting them to the Internet, enabling seamless integration and the completion of complex tasks. With the convergence of various technologies, IoT devices such as smart watches, smart refrigerators, and medical sensors have been developed, impacting fields like healthcare, agriculture, transportation, and energy generation. The IoT aims to enhance people's lives by automating routine tasks and has found applications in individual, enterprise, transportation, and utility domains. However, the rapid growth of IoT has raised concerns regarding privacy and security.

This paper presents a comprehensive study of the security challenges faced by the Internet of Things and emphasizes the importance of security in IoT systems. The literature review in Section 2 highlights existing research on IoT security. Section 3 introduces the Internet of Things Architecture, focusing on the Network layer, Perception layer, and Application layer. In Section 4, the security challenges specific to IoT are discussed, shedding light on the vulnerabilities that make IoT devices prone to cyber threats.

Section 5 emphasizes the significance of security measures in IoT, considering the potential risks and implications of inadequate security. Recognizing the need for robust security standards, Section 6 presents proposed countermeasures for securing IoT devices and networks. Various approaches, protocols, and encryption techniques are discussed to address the security concerns and mitigate the risks associated with IoT systems.

In conclusion, this paper emphasizes the criticality of addressing security challenges in the Internet of Things. It underscores the necessity for well-documented security standards and effective countermeasures to

[1] University Utara Malaysia, Kedah, Malaysia[4]

protect IoT devices and networks from cyber threats. By implementing these measures, the IoT can continue to enhance people's lives and advance industries while maintaining privacy and security.

1 Introduction

The Internet of Things (IoT) refers to a new era in which all technologies and appliances are connected to the Internet and users can use them together to complete complex operations easily. It is a collection of several technologies that function in a coordinated manner to accomplish a shared purpose in various fields and applications. Several Internet of Things (IoT) devices have been developed, such as smartwatches, smart bicycles, smart refrigerators, smart mobiles, smart fire alarms, medical sensors, smart door locks, etc. Healthcare, agriculture, transportation and energy generation and distribution are just a few of the Internet of Things implementation fields.

The Internet of Things seeks to change people's lives by allowing intelligent technology to do routine chores. There are a variety of Internet of Things application domains, going from individual to enterprise [1]. Several types of the domains are in personal or individual domain, transportation domain, enterprise and industry domain, and also service and utility domain. The terms "smart houses", "smart cities", "smart transportation" and many others are used in relation with the Internet of Things [2].

The rapid rise of the Internet of Things has benefited businesses in a variety of ways, including improved market research and corporate strategies. Similarly, by introducing automated services, the Internet of Things has improved people's lives. Nevertheless, such an unchecked growth has raised concerns about privacy and security issues. Most security experts consider the Internet of Things to be a vulnerable site for cyber-attacks or cyber threats due to poor security measures and rules. Security standards are not adequately documented, despite the emergence of many security measures to protect Internet of Things devices from cyber threats [3].

The goal of this paper is to provide a study of the Internet of Things security challenges, the important of security to Internet of Things as well as its proposed countermeasure. The rest of the paper is divided into several sections. Section 2 is a review of current literature on security in the Internet of Things. Section 3 is the introduction to Internet of Things Architecture which will state about the Network layer, Perception layer and Application layer. Section 4 will talk about the security challenges in Internet of Things. Section 5 deals with the important of security in Internet of Things followed by section 6 which will present about Internet of Things proposed countermeasures. Lastly, section 7 which is the conclusion.

2 Literature review

The Internet of Things (IoT) is a collection of connected gadgets that communicate among each other via Internet connection without the need for human intervention [4]. Internet access is getting more accessible and affordable all around the globe. Micro and nanotechnology are being used in networked computers to lower their resources and energy consumption while increasing their storage space, making it easier to add actuators and sensors. They can interact through the internet thanks to this jumble of little equipment with many functions. RFID tags, NFC tags, or barcodes are affixed to actual items, and they are scanned using equipment like a smartphone, tablet, or RFID/ NFC reader [5]. By integrating this collection of the physical realm and cyberspace via smart gadgets, the world wide web potential could be expanded.

Software security, namely the practice of applying measures all through the development process to guarantee that key security targets are accomplished, is described on the basis of security for Internet of Things. Integrity, confidentiality, and availability are the three main objectives [6]. Security mechanisms are protections to counter or minimize security threats that may threaten the integrity, confidentiality, and the system's availability overall, and they are taken to improve protection.

Internet of Things are complicated systems with multiple architectural and conceptual levels, making it difficult to ensure their software security measure. As technology changes frequently, it becomes much harder to manage

and ensure security. The existence of hardware, software, and middleware elements working with one another characterizes the Internet of Things [7]. Thus, every element in the lnternet of Things model contains sensitive information that could be compromised, posing a vulnerability.

To avoid, recognize, and respond to every attack, a suitable security solution is needed and make up for the intrusion. As a result of the top-down strategy, protection is a priority. Information theft and infection both common dangers inside the application layer. Web service proliferation and botnet attack. Intruders in Internet of Things might take advantage of vulnerabilities in protocols and standards when at the network layer [8]. One of most prevalent risks in protocols and standards is corruption, denial of service (DoS) and session hijacking.

To interact with other end nodes inside a network, end points in a telecommunication network follow a set of rules and regulations. Several Internet of Things data protocols are briefly mentioned, and their interactions with the Internet of Things gateway are depicted in Figure 1 below.

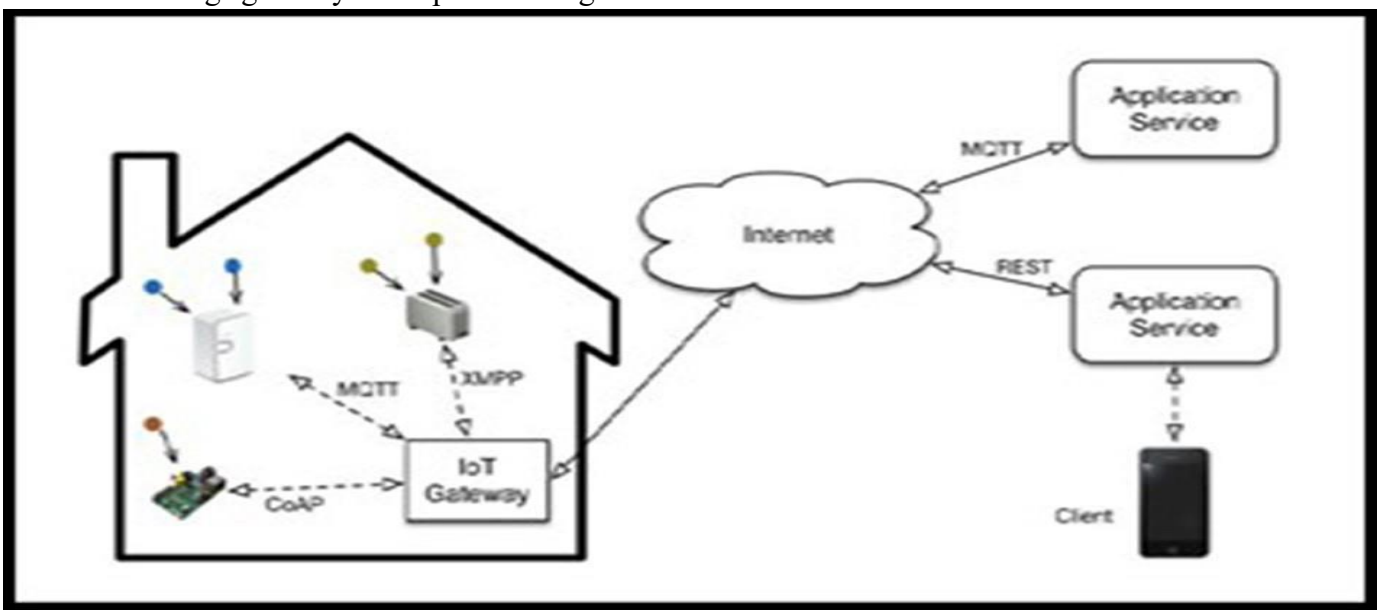

Fig. 1. The Internet of Things protocols [9]

MQTT (Message Queuing Telemetry Transport) is a protocol which provides seamless connectivity across Transmission Control Protocol/Internet Protocol (TCP/IP). It's a client-server messaging system that sends messages quickly and efficiently. MQTT has a fantastic method for notifying people when a connection is broken. The Advanced Message Queuing Protocol (AMQP) is an application layer protocol for text-oriented middleware that is available to all platforms. Message orientation, routing, queuing, and privacy are all characteristics of AMQP. XMPP (Extensible Messaging and Presence Technology) is a communication system that works in real time protocol that can be used in services such as audio and live video calls.

The term "things" is highly broad and encompasses a wide range of physical objects [10]. This network of various objects can provide numerous obstacles in the development of an application, as well as make current difficulties more challenging [11].

In the Internet of Things ecosystem, guarantee threats like privacy, secure communication,access control, and secure data storage have now become major challenges. Additionally, each piece of equipment built, each new sensor installed, and every byte synced together inside the Internet of Things environment may all be analyzed at some time throughout an investigation [12]. As a result, there is a need specific tools, strategies, and methods for safeguarding Internet of Things connections, as well as gathering, conserving, and evaluating leftover proof from Internet of Things environments.

The unintentional use of credentials, the failure to change login details, as well as the inability of gadget updates have all worsened cybersecurity vulnerabilities by allowing malicious software to gain access to sensitive data in Internet of Things equipment. As a result of such lax security standards, data breaches and other threats are more

likely [3]. Most security experts consider the Internet of Things to be a vulnerable location for hacking attempts due to its insufficient security standards and procedures. It's sometimes pretty easy to exploit Internet of Things equipment than it is to hack traditional computers thanks to terrible Internet of Things security architecture [13]. An adversary's simple access to Internet of Things devices offers the potential to side channel assaults. Timing assaults, electromagnetic attacks, power monitoring attacks,and differential fault analysis are all examples of this type of attack [14].

A huge amount of work has been put into dealing with the issue of protection flaws in the Internet of Things paradigm over the last few years. Some of these techniques point to a specific layer of security, while others aim to defend the Internet of Things from end to end [15]. Some people have various ideas about where Internet of Things should be prioritized, but they all agree on one thing, security must be the primary concern. Because Internet of Things differs from traditional networks, new strategies are needed to protect these widely used open infrastructures [16]. Security difficulties and hurdles can be solved by giving adequate training to developers and designers on how to include security mechanisms into Internet of Things products, hence motivating consumers to use the gadgets' built-in security mechanisms [17].

The Internet of Things necessitating a diversity of deployment scenarios and requirements. The majority of these gadgets and services were not created with privacy or security in consideration. Academic research on privacy and security challenges for IoT devices has shown promising results. Presently, the offered strategies and protective measures are primarily based on traditional network security procedures [18]. Due to the variety of the protocols and devices as well as the size or number of nodes in the system, implementing security features in an Internet of Things system is somewhat more difficult than in a typical network.

3 Introduction to Internet of Things architecture

Acknowledging the Internet of Things environment necessitates establishing the Internet of Things layers and elements in order to define the various Internet of Things architectures based on the services and fields required. The actions that each level executes, as well as the device that it employs, are explained for each level. Various works have been proposed for Internet of Things scenarios [8]. As indicated in Figure 2, a typical Internet of Things design can be separated into five tiers which is Network layer, Perception layer, Middleware layer, Business layer and Application layer. The Internet of Things has a three-layered architecture in general. This is the most common version encountered in most articles, as well as the one on which this study will concentrate which is Network layer, Perception layer and Application layer. Quality of Service (QoS), confidentiality, reliability, and integrity are all important aspects of IoT design

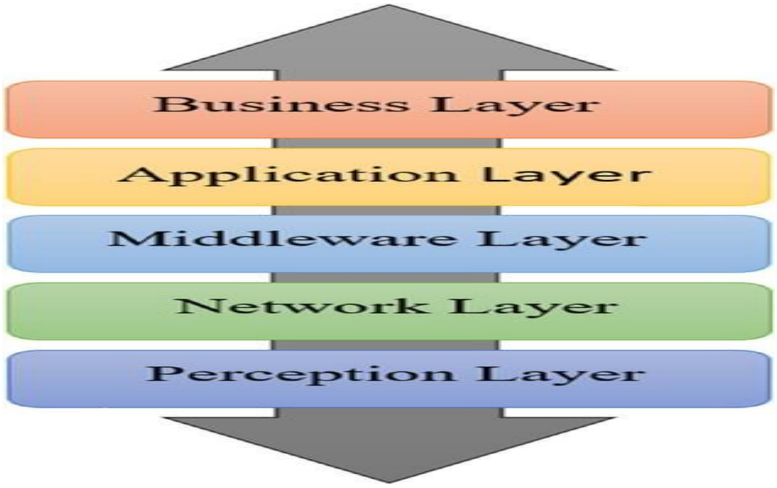

Fig. 2. The Internet of Things architecture [9]

3.1 Perception layer

The perception layer is identical to the physical layer, which contains several sorts of sensor devices and environmental components [10]. Sensor devices such as RFID, ZigBee, Quick Response (QR) code, and others

make up the perception layer, which is overall device management and the collecting of specialized data by each type of sensor device are the responsibility of this person. [9]. This layer is in charge of system's overall handling, which includes identifying and collecting particular data from various sensor devices. PH level, wind speed, humidity, vibration, percentage of pollution in the air and other data can be obtained. This obtained data is sent to a central information processing system via the Network layer for reliable communication.

3.2 Network layer

Data is sent from the perception layer to the upper levels via the network layer, while protecting sensitive data from sensor devices [9]. Sensitive sensor data is safely transferred to the system for central data processing via the network layer and via UMTS, 4G, 3G, WiMAX, Satellite, Infrared, RFID, Wi-Fi and other methods. As a result, this layer is largely in charge of data transport from the Perception layer to the upper layer [10].

3.3 Application layer

In this layer of Internet of Things applications contains things such as smart glasses, smart house, smart car and smart postal [9]. Using the information gathered by the Middleware layer, the application layer is in charge of controlling all programmes [10].

4 Security challenges in Internet of Things

Internet of Things architecture can be divided into several layers which is Perception layer, Network layer, Middleware layer, Application layer and Business layer. Each one of these layers employs a variety of technologies, each of which poses its own set of problems and security risks. This section covers the Network layer, Perception layer, and Application layer security challenges in Internet of Things.

4.1 Type of security issues and challenges

Technology problems and security challenges are the two types of challenges that the Internet of Things faces. The technical obstacles are connected to the rules and functions that need be enforced to establish a safe network, while the security concerns are due to the various and the pervasiveness of Internet of Things devices [2]. Scalability, wireless technologies, energy and the distributed nature of Internet of Things pose challenges.

4.2 Security challenges

There are many different types of things for Internet of Things services, ranging from simple to complicated gadgets, and they communicate with each other over various networks. It means that any device or network layer poses a security risk, and that user privacy can be jeopardized in a number of ways. As a result, all attack scenarios in the previous IT environment should be examined with caution [19]. Today's digital infrastructures confront numerous risks. Our devices and systems have been always at risk, whether that's an organization's network, a home Wi-Fi network, or a smart TV. In the Internet of Things, this continual risk is just no different. Because of the open architecture of Internet of Things, securing these devices is significantly more challenging, posing many additional security concerns [16].

Security challenges in perception layers. Physical Internet of Things sensors and actuators are the focus of the perception layer. Sensors detect the physical phenomena that are taking place around them. Actuators, on the other hand, use sensed data to perform a specific action on the physical environment. Sensors for sensing various types of data exist in a variety of shapes and sizes [20]. The following are the major security concerns that can be found at the perception layer:

- **Node Capturing**: Various low-power nodes, such as sensors and actuators, are used in IoT applications. Adversaries can target these nodes in a number of ways. Intruders may attempt to capture or substitute the Internet of Things system's node with a malicious node. The invader has taken control of the new node, which looks to be a system member. This might jeopardize the protection of the entire Internet of Things application [20].
- **Malicious Code Injection Attack**: The intruder injects malicious code into the node's memory as part of the attack. In most situations, firmware or software for Internet of Things nodes is updated over the air, allowing hackers to add malicious malware. The intruders may use such malicious code to manipulate the nodes to perform undesired functions or even try to get access to the entire Internet of Things system.

- **False Data Injection Attack**: After capturing the node, the intruder can utilize it to inject false data into the Internet of Things system. This could result erroneous findings and the Internet of Things application crashing. This method might also be used to launch a DDoS assault.
- **Side-Channel Attacks (SCA)**: Aside from attacks based on the nodes, a variety of side-channel attacks could result in sensitive data being leaked. Processor microarchitectures, electromagnetic emission, and power usage all give enemies access to classified data. Power consumption, laser attacks, timing attacks are all examples of side channel attacks. While developing the cryptography modules, modern chips adopt a variety of safeguards to prevent side-channel attacks.
- **Eavesdropping and Interference**: Internet of Things applications are frequently made up of a variety of nodes that are deployed in open spaces. As a result, snoopers can gain access to Internet of Things apps. Attackers can eavesdrop and grab data during a variety of procedures, such as data transmission or authentication.
- **Sleep Deprivation Attacks**: In such assaults, the intruder attempt to deplete the battery of low-powered Internet of Things edge devices. Due to a flat battery, the nodes in the Internet of Things application experience a denial of service. This may be performed using malicious code to create endless spiral in peripheral devices or to purposefully increase the energy consumption of peripheral devices.
- **Booting Attacks**: Throughout the startup procedure, peripheral devices are exposed to a variety of assaults. This is due to the fact that the built-in security mechanisms are not operational at that time. Intruders may try to take advantage of this flaw by assaulting node devices when they are rebooting. Protecting the boot process is critical since peripheral devices are routinely low in powered and go through sleepwake cycles.

Security challenges in network layers. The network layer's primary duty is to send data from the perception layer to the computer system for processing. The fundamental security concern is ensuring the authenticity and dependability of data being transmitted at the network layer [20]. The following are some of the network layer's security challenges:

- **DDoS/DoS Attack**: The intruder sends a large number of unsolicited requests to the target servers in this sort of attack. The target server gets disabled as a result, causing real users' services to be disrupted. A DDoS (distributed denial of service) assault occurs when an attacker uses many sources to overwhelm the target server. Although such attacks are not unique to Internet of Things applications, because to the diversity and complexity of Internet of Things networks, the network layer of the Internet of Things is likely to be vulnerable to them [20]. Servers or computers are cannot provide services to users as a result of a DoS attack. Due to a denial-of- service attack, data transfer among devices and associated sources is disabled [20].
- **Phishing Attack**: Phishing attacks are attacks where a single hacker might quickly and easily exploit a vast group of Internet of Things devices. As per the intruders,

at minimum a few of the machines will fall victim to the strike. Users may stumble upon phishing sites while searching for information available on the internet. Once a user's identity and credentials are compromised, the user's entire Internet of Things ecosystem is vulnerable to hacking. Phishing site scams have no defense against the network level of something like the Internet of Things [20].

- **Man-in-Middle Attack**: In this exploit, the intruder would not need to be available in person at a network's location; instead, he simply uses the IoT communication protocol to interrupt with two sensor nodes in order to obtain classified data [20].
- **Data Transit Attacks**: In Internet of Things applications, data storage and exchange are frequent. Cyber-attacks and other opponents are always pursuing data since it is valuable. Cyber-attacks can affect data stored on data centers or in the cloud, but data in transit or It is quite dangerous to travel from one region to another. In Internet of Things applications, sensors, actuators, the cloud, and other devices exchange a lot of data. Internet of Things applications are prone to data assaults due to the different communication protocols used in such communication channels [20].

- **Gateway Attack**: The sensors' interconnection as well as the internet infrastructure is broken as a result of this procedure. This assault also includes a denial-of-service (DoS) or routing assault, which the internet sends false or no data to the node or sensors [20].

Security challenges in application layers. The application layer deals directly with end users and provides services to them. Smart homes, smart meters, smart cities, smart grids, and other Internet of Things devices are included in this layer. This layer has unique security risks, such as data theft and privacy concerns, that are not represented in other layers [20]. Due to security problems, the application can be easily compromised and shut down. The malicious attack may cause a virus to infect the application programmed code, causing the application to malfunction. Occasionally, programmed fail to bring authenticated services that they had meant to deliver or provide the feature incorrectly [20].

- **Malicious Code Injection Attacks**: Intruders frequently use the simplest or most direct route to gain access to a system. If the system is vulnerable to malicious scripts and misdirection as a consequence of insufficient code checks, an intruder will use that as their first point of entry. Intruders employ XSS (cross-site scripting) to inject malicious code into a webpage that is otherwise trustworthy. An Internet of Things account can be hijacked and the Internet of Things system can be paralyzed if an XSS outbreak occurs [20]. This could be a dangerous "worm" virus that infect Internet-connected devices such as surveillance cameras and wireless modems. This type of attack might disable a car's Wi-Fi and gain control of the steering wheel, resulting in a terrible accident [20].
- **Software Defenselessness**: Non-standard code written by programmers might likewise expose security issues. Unauthorized intruders employ this method to achieve their unethical goals [20].
- **Data Thefts**: Internet of Things apps handle a lot of personal and sensitive information. Information in route is much more prone to assaults than data at rest, and there is a lot of information mobility in Internet of Things applications. If Internet of Things applications become susceptible to data theft threats, users would be hesitant to share their personal details. User and network authentication, data separation, encryption, and privacy management, and other tactics and standards are being used to safeguard Internet of Things applications from information theft [20].
- **Access Control Attacks**: The definition of access control is that, system that restricts access to sensitive data or accounts to only authorized people or operations. In Internet of Things, an access control attack is crucial because if then once access is obtained, all application has now become exposed to threats.
- **Service Interruption Attacks**: These operations are also known as DDoS attacks or unauthorized interruption attacks. There have been a number of assaults on Internet of Things in the past. By intentionally causing the machines or networks too hectic to react, such threats prevent genuine users from using the services of Internet of Things.

4.3 Internet of Things security principle

According to the usual Internet of Things architecture, some equipment or perception sensors are installed publicly with no control mechanism in place, leaving outside intruders vulnerable. Intruders can gain access to this equipment and programme them such that the sensors can transmit information to both the register servers and the intruders' group. Following the ideas and guidelines outlined below, a foundation for communication that is safe for things, processes, software, and people can all be created [5].

- ***Confidentiality***

It is critical to guarantee that information is protected and accessible only to authorized individuals. A user in the Internet of Things can be a person, a computer, or a service, as well as internally and externally things (items that make up the system) and (devices that aren't connected to the internet). It is critical, for example, to ensure that sensors do not divulge acquired information to surrounding nodes. How the information will be handled is also another issue of secrecy which must be considered [1]. The users of the Internet of Things must be informed of the information management method that will be used and it should guarantee that the information is kept safe throughout the Internet of Things operation [5].

- ***Integrity***

Because the Internet of Things is dependent on transferring information and data amongst a variety of devices, it's critical to assure data accuracy, that data is accessed from the correct source, and that it isn't altered during transmission due to intentional or unintentional interruption. Ensuring end-to-end protection in Internet of Things communications can enforce the integrity characteristic. Firewalls and protocols are commonly used to govern traffic flows, but due to the low computational capacity of Internet of Things nodes which do not accept these mechanisms properly, these mechanisms may not always ensure the integrity of data at destinations in Internet of Things [2]. Because of the distinctive nature of limited computing capacity at Internet of Things nodes, data traffic is regulated using firewalls and protocols, but this does not increase the protection at destinations [1]. Information is transferred between numerous devices in the Internet of Things; therefore, precision is critical. This implies that information must be controlled to ensure that it is originating from the correct originator and reaching the appropriate Internet of Things node with no intentional or inadvertent intervention. Communication integrity in the Internet of Things is ensured through end-to-end security [5]. Because Internet of Things endpoints have little computational capability, implementing security or cryptography algorithms on these devices is problematic.

- ***Availability***

The Internet of Things (IoT) aims to unite everything and making it accessible worldwide. Internet of Things data ought to be ready to Internet of Things users at any time and from any location, and information from Internet of Things devices must also be obtainable to Internet of Things users at any time [5]. Data isn't the only element in use in the Internet of Things, devices and services would also have to be accessible and readily available in a fast manner to meet the Internet of Thing's goals [2].

- ***Authentication***

Each Internet of Things object should be capable of recognizing and authenticate another Internet of Things object. Every asset or node in the Internet of Things ought to verify the authenticity of other entities and nodes, but this procedure is complex and time-consuming because the Internet of Things is so diverse [5]. However, due to its obvious nature of the Internet of Things, this procedure can also be difficult; numerous parties are engaged (people, devices, service providers, services, and processing units), and items may have to engage with each other for the first time (items they are unfamiliar with) [1]. As a result, a system to mutually verify parties throughout every Internet of Things transaction is required.

- ***Lightweight Solutions***

Even though Internet of Things may bring unique features and constraints to each of the above described goals, they are still not distinctive to it. Nevertheless, in principle, every machine or internet security aim should include integrity, confidentiality, authentication and availability. Lightweight solutions, on the other hand, are a distinctive protection mechanism that has been established as a result of the computation and power limits of the Internet of Things devices. It is not an objective in and of itself, but instead a constraint which must be taken into account when designing and applying protocols for information and device encryption and authentication inside the Internet of Things [2]. These techniques or methods should be suitable with device capabilities as they are designed to function on Internet of Things devices with limited capability.

- ***Heterogeneity***

In the Internet of Things, there seem to be a variety of devices and sensors from many producers, each with its own set of capabilities depending on a complicated or basic architecture. Multiple versions of the Internet of Things entities' releases are also available. As they have different technological interfaces and serve diverse duties, Internet of Things protocols should also be built so that all heterogeneous elements can work with each other in a variety of settings. The Internet of Things' main purpose is to link things, people to devices and people to people, resulting in a network of heterogeneous objects [5]. Furthermore, an effective cryptography system with proper key management and security policies is required to assure protection.

- ***Policies***

There should be laws and regulations in place to make sure that information is managed, secured, and transferred properly, but more importantly, a process must be in place to ensure that all organizations follow the policies and procedures. Each service that is engaged should have unambiguous Service Level Agreements (SLO). Because of its varied and dynamic nature, latest computer and network security policies may not have been suitable to Internet of Things [2]. The implementation of such rules will instill trust in the Internet of Things among human users, resulting in its development and expandability.

5 Important of security in Internet of Things

Since before the inception of communication networks, data security has always been a major concern. As the Internet became more sophisticated and commercialized, privacy concerns grew to include individual privacy, banking transactions, and the threat of computer hackers [7].

5.1 The important of security based on each level

Security system are inextricably linked in the Internet of Things. Interfering with the settings of a car, a pacemaker, or a nuclear reactor, either accidentally or maliciously, puts people's lives at danger. As mentioned below, security must always be handled at all layers of the machine's lifespan, from preliminary concept to operational area:

•Hardware/Physical Level

Gadgets must be protected. The protection of sensing devices as well as the protection of information collecting are the two most important safety concerns. The lnternet of Things cannot provide a complete security protection scheme and is prone to intrusion and exploitation due to diversity, uncomplicated, energy restricted, and poor protective capabilities of sensing nodes, which are typically installed in unattended hostile environments without either a unique standard. Node physical obtain, catch gateway node, sensing data leak (the position of the viewer and user, private data, as well as other information), replay attacks, energy depletion attacks, congestion attacks, unfair attacks, integrity attacks, denial of service attacks, interfering, forward attack and man-in-the-middle assault and node replication assault are some of the security issues that this layer faces. The danger of theft, destruction, and subscription data attack for M2M terminal equipment is mostly linked to installation before linking and unsupervised M2M devices [7]. It is necessary to include a smart network that detects each node that has failed and self-organizes the connection without destroying it.

•Software/Communication/Protocols Level

Intruders can easily compromise the communication infrastructure in lnternet of Things. Unauthorized admission, information eavesdropping, integrity, confidentiality, and damage, as well as man-in-the-middle assaults, denial of service attacks, and malware infection, are all hazards that arise in the present lnternet of Things communication network. Some other danger is the breach of privacy as a result of Internet of Things devices that gather private data. Because the majority of communication is cordless, snooping is simple. Authentication is especially difficult since it necessitates the use of appropriate authentication facilities, that are commonly lacking in the Internet of Things. Unlike to today's computing and communication technologies, lnternet of Things devices have limited capabilities. The main issue is that even the credentials cannot be produced since they require the assistance of end hosts, which are insufficient in lnternet of Things devices because to their limited power, capacity, communication capabilities and network bandwidth. Poor encryption technologies could be used as an alternative.

•Storage of the Data Level/ Application Layer

Information should be kept in a storage and encrypted manner. Because the Internet of Things senses a wide range of devices, collects data in many different of formats, and also has humongous, heterogeneous characteristics and multisource, it will also introduce many other difficult and complicated aspects of internet security concerns to the network level, including such big data transfer necessities due to the huge amount of nodes inside the Internet of Things, likely to result in network problems hence a denial of service attack. As a viable alternative, data mining, cloud computing, data backup, data storage, authentication methods, and data management are used in Internet of Things applications [7].

6 Proposed countermeasures

Unprotected web and cloud services are application – level weaknesses that could be used to attack an Internet of Things system [21]. As a result, cloud gateway security measures are needed to prevent unauthorized activity from changing settings.

6.1 Authentication measures

The methods of determining devices and users in a channel and giving access to authorized people and non-manipulated equipment is known as authentication. The reply attack, the Sybil attack and impersonation attack are all examples of assaults on Internet of Things that can be mitigated via authentication [21]. A platform-to-terminal-node reciprocal authentication mechanism for the Internet of Things Hashing and provides several tools are used in the technique [1]. To mitigate collision assaults, the extracted features was integrated with the hashing algorithm. Wen et al., provide an alternate method for identifying people at Internet of Things sensor nodes [2]. This is a request-reply mechanism-based one-time cypher technique. The sender and receiver use a pre-shared structure to construct this dynamic variable encryption. The participants can choose an arbitrary coordinate to act as the key coordinate. Because the key can be reused for multiple coordinates, this cypher could be used where safeguarding Internet of Things is not oversensitive and critical. Regarding privacy, establishing appropriate access controls is just as vital as authentication, and so both functions work side by side in safeguarding Internet of Things.

6.2 Trust establishment

Because objects or equipment inside the Internet of Things might physically migrate by one owner to another, respective owners must create confidence in order for the Internet of Things device to migrate smoothly in terms of permissions and access control [2]. According to Zhang et al., trustworthiness computing for Trust-Based Access Control (TBAC), Internet of Things network access control, is still pretty new but it has been effectively applied in commercial applications [21]. Bernal et al., presented a multi – dimensional believe control scheme for the Internet of Things [21]. Because of the limited resources available on the machines, the trust assessment is centralized. Two techniques build this confidence: the production key as well as the token. An entitlement method allocates a production key to any new machine that is produced. This key must be requested from the machine's vendor. The vendor, or current holder, creates the token, which is then coupled with the machine's RFID identifier [1]. When a new premise or building is purchased, this method is identical to replacing old key.

6.3 Federated countermeasures

To address the heterogeneity of multiple machines, protocols and software, it is critical for Internet of Things architecture to own a combined architecture with an inside autonomous or centralized component [1]. It is hard to manage the safety of Internet of Things since there are no uniform rules and guidelines to regulate the planning and development of the systems. Other effort has been made to create a framework for critical systems named Secure Mediation GateWay (SMGW). This method is an Internet of Things abstraction since it can be applied to any type of decentralized network, regardless of its origin or function. SMGW can identify all important distributed data from diverse nodes, solve the heterogeneity of heterogeneous nodes, whether they are electrical, telecommunication or water systems nodes, and transfer all signals through the Internet's unsecured network. It wasn't enough to having guidelines and rules in place to assure safety, enforcement measures are indeed required. Due to the obvious changing nature of Internet of Things, conventional regulations may not even be effective. The suggested regulatory framework has the potential to significantly improve Internet of Things security.

6.4 Security awareness

Intruders have used vulnerable gadgets as "thingbots" to hack the Internet of Things network, culminating in real-life disasters. This is compelling proof that Internet of Things security is a major worry. The Internet of Things is also predicted to grow and be the focus and threat channel for many coming years [21]. Other crucial safety mechanism for the sustainability and evolution of the Internet of Things framework is knowledge between multiple beings who are connected to it. The repercussions of not protecting the Internet of Things with real numbers are frightening [1]. Hackers used no-password or the default credential to obtain access to Internet of

Things devices (SCADA devices, traffic control devices, device webcams and printing machines) which were completely publicly available. The recorded results were fascinating, revealing that most of these technologies were all it indeed employable. If users tend to be unconcerned about privacy and employ the bare minimum of encryption, like the given password that includes with the product when buying, the Internet of Things will do more damage than good things [2]. To address this problem, individuals ought to be more knowledgeable of cyber threats in the Internet of Things while also applying all security protocols and precautions, as attackers would have more chances to target the entire system when one of its machines is not protected.

7 Conclusion

Through each tier, the Internet of Things framework is vulnerable to assaults. As a result, there are numerous privacy issues and obligations to meet. The present state of Internet of Things research is focused primarily on access control protocols and authentication, however with the digital revolution, new networking protocols such as 5G and IPv6 are necessary to accomplish the dynamic mixing of Internet of Things topology. The most significant breakthroughs in Internet of Things have occurred on a tiny level, primarily among firms and then in a few industry sectors. Multiple security risks must be tackled in order to extend the Internet of Things framework through one firm to a batch of diverse companies and technologies. The Internet of Things has enormous capacity to alter people's current lifestyles. However, security is a crucial consideration in the development of entirely intelligent systems. If security challenges such as confidentiality, privacy, access control, authentication, trust management, endto-end security, global rules, and standards are fully handled, the Internet of Things can be expected to revolutionize everything including the future.

8 Acknowledgment

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by University Utara Malaysia.

9 References

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of Things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336–341). IEEE. https://doi.org/10.1109/ICITST.2015.7412116

Yousuf, T., Mahmoud, R., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and countermeasures. International Journal for Information Security Research (IJISR), 5(4), 608–616. https://doi.org/10.20533/ijisr.2042.4639.2015.0070

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102. K. Elissa, “Title of paper if known,” unpublished. https://doi.org/10.3390/app10124102

Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1577–1581). IEEE. https://doi.org/10.1109/ICGCIoT.2015.7380718

Ahmad, M., Younis, T., Habib, M. A., Ashraf, R., & Ahmed, S. H. (2019). A review of current security issues in Internet of Things. Recent trends and advances in wireless and IoT-enabled networks, 11–23.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989. https://doi.org/10.1007/978–3–319–99966–1_2

Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017, May). Security challenges in IoT development: A software engineering perspective. In Proceedings of the XP2017 Scientific Workshops (pp. 1–5). https://doi.org/10.1145/3120459.3120471

Billure, R., Tayur, V. M., & Mahesh, V. (2015, June). Internet of Things – a study on the security challenges. In 2015 IEEE International Advance Computing Conference (IACC) (pp. 247–252). IEEE. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989. https://doi.org/10.1109/IADCC.2015.7154707

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on Internet of Things security: Requirements, challenges, and solutions. Internet of Things, 100129. https://doi.org/10.1016/j.iot.2019.100129

Datta, P., & Sharma, B. (2017, July). A survey on IoT architectures, protocols, security and smart city based applications. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1–5). IEEE. https://doi.org/10.1109/ ICCCNT.2017.8203943

Kraijak, S., & Tuwanut, P. (2015, September). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015) (pp. 1–6). IET. https://doi.org/10.1049/cp.2015.0714

Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017, February). Internet of Things (IoT): A vision, architectural elements, and security issues. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 492–496). IEEE. https://doi.org/10.1109/I-SMAC.2017.8058399

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. https://doi.org/10.1016/j.future.2017.07.060

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, 326–337. https://doi. org/10.1016/j.future.2018.01.059

Aman, M. N., Chua, K. C., & Sikdar, B. (2016, May). Position paper: Physical unclonable functions for iot security. In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security (pp. 10–13). https://doi.org/10.1145/2899007.2899013

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/ j.future.2017.11.022

Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018, August). Securing the Internet of Things (IoT): A security taxonomy for IoT. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 163–168). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

Aldowah, H., Rehman, S. U., & Umar, I. (2018, June). Security in Internet of Things: issues, challenges and solutions. In International Conference of Reliable Information and Communication Technology (pp. 396–405). Springer, Cham. https://doi. org/10.1007/978-3-319-99007-1_38

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. In 2015 IEEE World Congress on Services (pp. 21–28). IEEE. https://doi.org/10.1109/SERVICES.2015.12

Hwang, Y. H. (2015, April). Iot security & privacy: Threats and challenges. In Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security (pp. 1–1). https://doi. org/10.1145/2732209.2732216

Rao, T. A., & Haq, E. U. (2018). Security challenges facing IoT layers and its protective measures. International Journal of Computer Applications, 179(27), 31–35. https://doi. org/10.5120/ijca2018916607

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025