ARTICLE IN PRESS

Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

# An analytical study on security and future research of Internet of Things

V Srinadh [a,*], Mannava Srinivasa Rao [b], Manas Ranjan Sahoo [c], K. Rameshchandra [d]

[a] *Dept. of CSE, GMR Institute of Technology, Rajam, Andhra Pradesh, India*
[b] *Dept. of ECE, PVP Siddhartha Institute of Technology, Kanuru, Vijayawada, India*
[c] *Dept. of ME, Srinix College of Engineering, Balasore, Odisha, India*
[d] *Dept. of ECE, Vishnu Institute of Technology, Bhimavaram, India*

ARTICLE INFO

*Article history:*
Received 24 November 2020
Received in revised form 24 November 2020
Accepted 9 December 2020
Available online xxxx

*Keywords:*
Internet of Things
Characteristics of IoT
IoT security
IoT future development

ABSTRACT

Internet of Things (IoT) is the network of billions of interconnections, knowledge sharing and useful data devices, people and services. Increased comfort, performance and user automation are strongly confirmed in IoT applications. In order to enforce the automated IoT environment, the high level of safety and privacy, authentication and recovery from attacks is required. In this work, I present an overview of the architecture of IoT layers and attacks on layer protection. Moreover, this work provides an outline to resolve the risks to security and privacy. In this article, a thorough overview of the security threats and sources of menace in IoT applications is presented. In addition, the current state of IoT safety research and future research instructions regarding IoT safety and privacy will be addressed here.

## 1. Introduction

In 1999 the concept of IoT was first proposed by a Radio Frequency Identification (RFID) member. IoT is becoming increasingly relevant worldwide due to the rapid growth of mobile devices, networking, cloud computing and data analytics [13]. More than 7 billion people currently use the Internet to carry out various types of activities, including emails, social media data sharing, reading books, playing sports, searching, shopping online. This vast Internet use enables new trends to be carried forward, this worldwide networking infrastructure that enables machines to interact and decide on each other [8]. IoT is an environment in which the Internet Protocol (IP) links trillions of objects and communicates and shares information. These interconnected objects constantly produce a massive amount of data collected, analyzed and used for action, providing decision-making information (Patel and Patel, 2016).

Fig. 1 In virtually every sector for the development and distribution of transport, agriculture, health and electricity. The implementation of the IoT is shown in Fig. 1. IoT transforms the way we live today by developing smart devices that can conduct daily tasks, smart houses, smart towns and smart transports (Youxuf, Mahmoud, Aloul and Zualkernan, 2015).

The number of IoT devices connected increases every day. Burhan, Rehman, Khan, and Kim [7] clarify that connected equipment offers comfort and good results in comparison to humans. Fig. 2 shows the number of IoT devices linked between 2012 and 2020. As seen in Fig. 2, there are tremendous increases in the number of connected devices.

In addition to the advantages of these applications, they also face obstacles, one of the greatest issues in security and privacy. IoT apps eliminates human effort because they execute tasks automatically. Communication is the key component of the IoT since all connected devices have to be able to communicate.

In Fig. 3(a) Hardware, the major communication components of IoT are presented: consists of sensors, actuators, etc. (b) Middleware: used for data storage, includes calculation instruments used for data analyses and c) Presentation: software widely available for visualization and analysis on various platforms [15]. Alaba, Othman, Hashem and Alotaibi [3] clarify that IoT has established a universal relation between individuals, artefacts, sensors and services. IoT's main goal is to provide an infrastructure that allows a network that can connect with one another in any network, including data interchange, apps, physical/virtual sensors, computers, intelligent devices, cars and various real-life things.

[*] Corresponding author.
*E-mail address:* srinadh.v@gmrit.edu.in (V Srinadh).

https://doi.org/10.1016/j.matpr.2020.12.342
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

**Fig. 1.** Internet of Things (Patel and Patel, 2016).

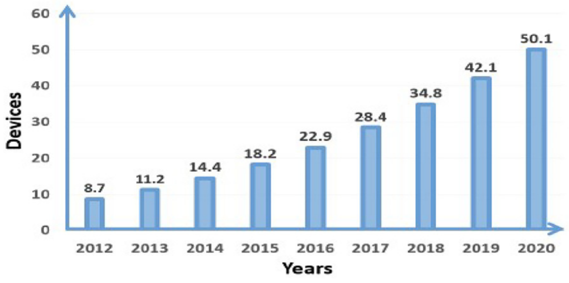

**Fig. 2.** Number of connected devices from 2012 to 2020.

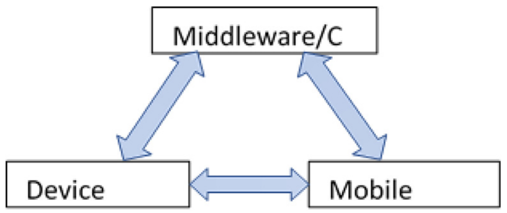

**Fig. 3.** IoT communication components.

The growing capacity for the various technologies such as RFID, Wireless Sensor Network (WSN) or increased storage capacity, would enhance interconnected devices. At least one identity, which enables people to interact with one another, will be available in the various objects of everyday life such as people, cars, computers, books, TVs, mobile phones, wardrobes, food, medicine, passports, luggage [1].

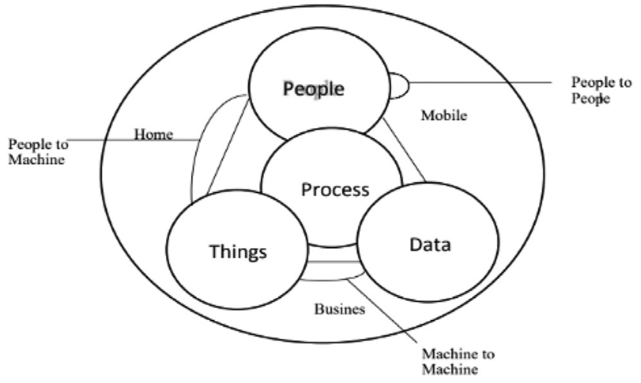

**Fig. 4.** Internet of Everything.

The Internet of Everything (IoE), a mixture of people, processes, and data, is helpful to turn the knowledge into action that increases companies, individuals and countries' economic opportunities (Cisco, 2012). The most pertinent and useful ways of linking the IoE I are shown by Fig. 4, (ii) smarter knowledge for better decision-making; (iii) the mechanism for providing the right person with the right information at the right time; and (iv) physical devices and Internet-based objects. IOE helps increase the influence of the Internet and the IoT advance [10], which will boost the industry's performance.

### 1.1. IoT devices

The IoT, talked about by Radoglou Grammatikis, Moscholios and Sarigiannidis (2019), consists of several networks where devices communicate through the Internet with each other. These devices are generally referred to as "things" and discussed in Fig. 5, each of which has its own characteristics.

**Identification:** The connected devices first have this property. To recognize each IoT device within the network, it is essential. The network objects are allocated with two IPV4 and IPV6 methods. First, IPV4 was used for addressing, but since IPV6 was increased, it was used because it was 128-bit address device [7].

**Sensing:** The actual world is used to collect knowledge (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019). Various sensors are used for data collection, such as smart sensors, actuators and RFID tags [7].

**Communication:** Data, messages, files, etc. sends and receives connected devices during this process. Various technologies are used to communicate between artefacts such as Bluetooth, wireless networks and RFIDs. Computation (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019) This approach is used for processing the data gathered from your computers. It is used to delete information that is redundant. Computer output is provided by various hardware and software systems [7].

**Services:** Apply to the users according to the functionality the systems have (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019). Last property of the connected apparatus is Semantics. They claim that IoT devices can get accurate physical information at the right time and provide information as services (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019).

### 1.2. IoT technologies

This interconnection between devices is being increased with the growth of the technology such as sensors, smartphones, cloud computing, communication capacities and the like [1]. IoT is used to link different products with the digital world. IoT is an assortment of different physical products such as cars, equipment, home appliances and more used to share data through the Internet with different technologies. The technology supporting the IoT principle is clarified in Table 1.

Technologies for identification: Connected devices must be identified uniquely in an IoT setting. In order to specific identification of linked equipment, the identification technologies such as RFID and WSN are used.

Technologies such as the GMS, UMTS, Wi-Fi, Bluetooth and ZigBee allow devices to communicate with other devices: Nets and communication technologies (TMTs): technology such as the Global Mobile communication system (GSM). Connected devices need to be communicated securely so that the user can access the network with complete trust and protection.

Software and technology: high communication devices that facilitate the rapid deployment of IoT applications will lead to the development of intelligent systems which provide high levels of intelligence and autonomy [1].

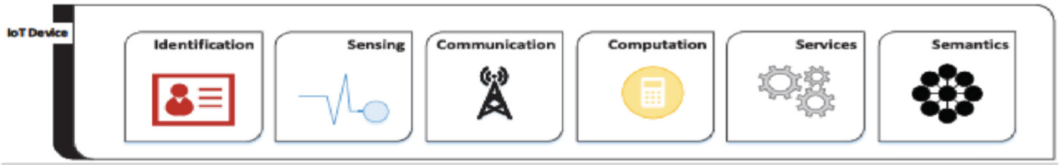

**Fig. 5.** The properties of IoT devices (Radoglou Grammatikis, Sarigiannidis and Moscholios, 2019).

**Table 1**
IoT technologies.

| IoT technologies | Supporting technologies |
|---|---|
| Identification technologies | RFID, WSN |
| Networks and Communication technologies | GSM, UMTS, Wi-Fi, Bluetooth, ZigBee |
| Software and Hardware technologies | Smart devices with enhanced interdevice communication |

## 2. Information security

Data protection for organizations and citizens using information systems is an integral part of their life. These systems store and exchange critical information requiring safeguards against a variety of threats requiring a number of safety controls. This information and the systems must be secured against unauthorized access, disclosure, interruption or alteration. Vashi et al. (2017) address the rapidly growing use of IoT, which improves protection and vulnerabilities. In Burg, Chattopadhyay and Lam [6] an enormous wireless and wired infrastructure that provides the connectivity between devices explains the communication and security of IoT.

IoT is built on the Internet, all of which face the same kind of security problems. The layer of awareness, the transport layer and the device layer contain three main layers of IoT. Each layer has its own safety issues. Security of information requires three priorities, i.e., Privacy, completeness and access to facilities [4]. Table 2 offers an overview of the goals of information security.

Table 2 addresses the key goals of security of information. The goals set out in the table below are the most frequency of all information security literatures, according to [4], but there are few other properties that are equally relevant for the protection of information. The characteristics are explained in Table 3.

IoT consists of three layers or five layers and it is a layered architecture. Three layers are the layer of perception, the network layer and the application layer, five layers are the layer of perception and the layer of the network and application. The security threats and attacks are vulnerable to each layer. They can be either active or passive. These threats may be from outside or in-house sources (Yousuf, Mahmoud, Aloul and Zualkernan, 2015). Next, attacks on the layer of understanding may be sensitive information leakage, denial of services, etc. Secondly, Network Layer attacks may be sybil attacks, sinkhole attacks, middle attack guy, etc. Finally, attacks on the application layer could include malicious injection of code, sniffing attachment, etc. Each layer has numerous security attacks as described in the previous section. Various security measures for the protection of data, such as encryption, authentication, privacy and access control are introduced.

**Table 2**
Objectives of information security.

| Objectives | Description |
|---|---|
| Confidentiality | Confidentiality means, information should not be available or disclosed to unauthorized persons. |
| Integrity | Integrity means, assurance of accuracy and reliability that no one can make changes without authorization. |
| Availability | Availability means, that data or information should be available when needed. |

**Table 3**
Objectives of information security.

| Objectives/ properties | Description |
|---|---|
| Authenticity | Authenticity means, that data/information is genuine and being able to be verified and trusted [4]. |
| Accountability | Accountability means, non-repudiation, deterrence, fault isolation, intrusion detection and prevention and legal action [4]. |
| Non-repudiation | Both the sender and receiver provide the proof of the sending and receiving the data [4]. |
| Reliability | Reliability means, the results are consistent and as they are intended. |

## 3. Background of IoT

IoT has many meanings. This concept is defined differently by various authors. This vary depends on the sense in which the word is used and the intent. (Patel and Patel, 2016) describe IoT as IoT is not just a computer network but also a network of all kinds of devices such as digital cameras, motor vehicles, mobile phones, home applications, medical instruments and industrial systems, people and buildings, all connected devices can communicate and share to achieve the requisite smart reorganizations; placement, online upgrade; process Dorsemaine et al. [9] describe IoT as the connected objects infrastructure, enabling its administration, data mining and access to created data." The International Telecommunications Union - Telecommunication Standardization Bureau (ITU-T) is recommending a more systematic and suggested definition of IoT. ITU-T (2012) describes IoT as a "global ICS infrastructure enabling advanced services through interconnection (physical, virtual) of existing and changing interoperable ICTs." The connection between the real world and the virtual world provides new possibilities that allow access from anywhere. This connection also raises the potential for new threats, safety risks and vulnerabilities.

As stated in the above definitions, the IoT can be interpreted in different ways. All these meanings are somehow mutually important. IoT can be defined as follows based on the above definitions, "IoT is the geographically connected device infrastructure, such as smartphones, industrial systems, vehicles, etc. connecting to and accessing data through communication technologies to ensure accurate positioning, security and administrative management."

The Internet of Things is the blend of various technical hardware and software. The IoT-based solutions, i.e., hardware and software, used for data store, storage and processing integration [13]. The Internet provides the key communication sources for wireless technologies such as RFID and WSN connectivity among various devices. Sensors are employed for sensing and monitoring the environment, the computing, memory, storage and energy capacities of these devices are low [2].

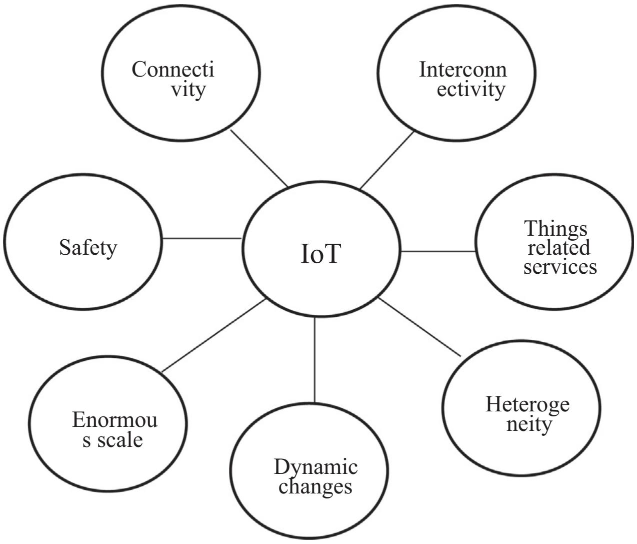

**Fig. 6.** Characteristics of IoT.

Fig. 6 displays the fundamental features of IoT. Interconnectivity and services related to stuff, heterogeneity, dynamic shifts, huge size, protection and accessibility (Patel and Patel, 2016) are all IoT-based features.

Interconnectivity: IoT is the interaction of the various devices that can be connected by means of some network between the devices. At geographically scattered places, the linked devices can be placed. Connected devices can create and share a large number of data stored and processed in central locations like the cloud.

These services are delivered in the sense of issues like privacy and continuity between physical and virtual items (Patel and Patel, 2016).

Heterogeneity: Every computer has its own software and hardware and is connected to a variable type of device and follows a different protocol. These instruments can interact across various networks (Viriyasitavat, Anuphaptrirong, and Hoonsopon, 2019).

Dynamic changes: a very dynamic IoT climate, which continually adopts changes. At geographical places, the connected devices can be distributed via IoT framework. Dynamically the status of devices, such as network connection and disconnection, changes. In addition, there can be complex changes to the number of devices connected and disconnected (Patel and Patel, 2016).

Enormous scale: The interconnected equipment produces a great amount of data. The data generated by these devices must be systematically controlled.

Safety: this is the main element of IoT. We need to secure personal data and our physical well-being. Likewise, networks and data passing across the network must be protected in any way.

Connectivity: Allows connectivity and compatibility to the network. Accessibility is accessed via the network while compatibility enables data to be consumed and generated (Patel and Patel, 2016).

### 3.1. IoT architecture

Multiple devices including sensors, actuators, processors and transceivers consist of IoT devices. IoT consists of a number of co-operating technologies. Sensors and actuators are instruments used for physical environment interaction. In order to extract valuable data from it (Sethi and Sarangi, 2017), data from sensors must be intelligently stored and processed. The contact between IoT devices is wireless because they are located geographically. Wireless contact has often a high chance of untrustworthiness and distortion.

### 3.2. Three layers architecture

The IoT architecture consists of three or five layers (Sethi and Sarangi, 2017). Three-layer architecture is considered the most basic architecture.

The architecture of IoT is presented in Fig. 7. The following is defined above the layer architecture:

(i) The layer of sensing is the physical layer: The layer comprises sensors for environmental information sensing and collection. All devices in the physical world are specified in this layer.

(ii) The network layer of this layer is connected to other smart things, network devices and servers. This layer is often used to data transfer between connected devices and to process them.

(iii) The consumer is responsible for the provision of the required application services in the application layer for which this layer is responsible. This layer defines a variety of applications for the use of the IoT in smart homes, smart cities and smart health for example.

### 3.3. Five layers architecture

The five layers architecture is the most detailed description of IoT architecture. Fig. 6 shows the five layers IoT. Five-layer architecture is the provide the information definition of IoT layer while the three-layer architecture describes the main concept. The Fig. 8 describe the five-layer design, business layer, processing layer and transport layer added for the information definition of the IoT architecture. These layers are explained below:

(i) The transport layer: This layer used to transport data form the from the perception layer to the processing layer and vice versa across networks such as wireless, 3G, Local area network (LAN), Bluetooth, RFID, and Close filed contact (NFC).

(ii) The processing layer: It's generally known as the layer of middleware. The data from the transport layer are collected, analyzed and processed. This layer also offers different facilities in the lower layers. Various technologies are also introduced in this layer, such as database, cloud storage, and large data processing modules.

(iii) The business layer: It handle all applications, business and benefits models and user confidentiality within the entire IoT system.

## 4. Discussion

### 4.1. IoT security

The IoT world is rising quickly and has a big effect on social and business life. The connected devices produce huge amounts of data through this environment. The data exchanged over the network by 2020 is expected to be over 44 ZettaBytes (ZB) according to

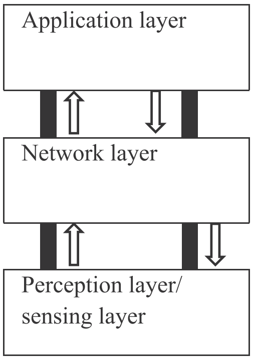

**Fig. 7.** Three layers architecture of IoT.

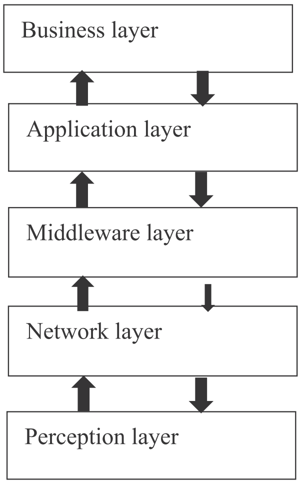

**Fig. 8.** Five layers architecture of IoT.

Sahinaslan (2019). Each linked individual in the world (about 75% of the total population of that time) will also have more than 4,900 digital data interactions every day by 2025, approximately once every 18 s. In 2025, over 90 ZB of data is generated by the IoT devices.

This rapid expansion poses many risks and threats. Examples of IoTs are the different fields of operation such as intelligent homes, intelligent industries, intelligent cars and etc. If a user is searching for some form of IoT service, he needs to connect different types of networks that can pose a serious risk to security and data protection. Hardware and software bugs are the key reason for these assaults. Protection is required to fix these vulnerabilities in hardware and software. Any of the current vulnerability solutions are rather costly. Lightweight, well-scaled protocols with low costs are therefore needed.

### 4.2. IoT security vs traditional IT security

According to Alaba, Othman, Hashem and Alotaibi [3] there are many variations in terms of protection and privacy between IoT and traditional wireless networks. The IOT system's devices are limited to hardware and software (i.e., sensor or RFID), but conventional IT mainly relies on resourceful devices. Frustaci, Speed, Aloy and Fortino [12] clarify Therefore, IoT devices only use lightweight algorithms to balance higher and lower security levels. In addition to these concerns, IoT has its personal security challenges, such as privacy, Authentication, management problems, storage of information, etc. and IoT apps will lose all ability without a trustworthy IoT ecosystem, as Hassija et al. (2019). Hassija et al. (2019) explains.

Table 4 addresses the difference between IoT security and conventional IT security. The conventional safety design is constructed from the user's point of view, which does not function for system communication. There may be similar security problems in both networks, but various methods and approaches for dealing with these problems are being used [3].

**Table 4**
IoT security vs Traditional IT security.

| Traditional IT security | IoT security |
|---|---|
| Add-on Security | Built in Security |
| Complex algorithms | Lightweight algorithms |
| User control | Privacy issues because IoT collect information automatically |
| Small technological heterogeneity | Large technological heterogeneity |
| Many security guards | Few security guards |
| In closed area, IT devices are located | In open environments IoT devices are installed. |

### 4.3. IoT vulnerabilities

IoT is the network of several devices and perhaps the most significant safety hazards. Bertino and Islam [5] clarified that for several reasons, IoT systems have higher security risks, I these systems do not have clearly specified perimeters, ii) these systems are highly heterogeneous in communication media and protocols, iii) smart telephone applications require installation permissions and other interactions, but such permissions may not be possible in IoT devices due to Similarly, the IoT devices and similarities in Radoglou Grammatics, Sarigiannidis and Moscholios (2019) clarify the possible cyber physical safety vulnerabilities which various cyber-attackers might take advantage from. The IoT vulnerabilities are explained in Table 5 Table 6 Table 7 Table 8 Table 9.

An essential part of securing trust between systems is. Threat and risk analyses are the foundation of the strategy for protecting these networks. There are several different security architectures to solve such risks. The IoT environments securing process is an arduous mission, with several different scenarios and different types of devices for each scenario. Each protection solution looks different, as these systems may have entities that are in various ways limited.

Such as many interconnected devices, one of the properties of IoT is its planned "large scale." Software protection would not only cover security analysis or threat and risk analysis, because devices that are out of the perimeter of a safety area and are deparametrized are more important to physical threats. A standardized safety level needs to be established which provides the necessary protection without too much impact on functionality.

### 4.4. IoT security issues

The IoT is a layer architecture with its own functionalities and the use of various technologies. The rapid growth of IoT equipment also raises safety hazards. This section addresses potential threats to security in IoT layers. The main feature for protecting IoT technologies is the confidentiality, integrity, availability, authentication and self-organization.

**Table 5**
Common vulnerabilities of IoT.

| Security Concerns | Example |
|---|---|
| Insecure web interface | Lack of ability to alter default password and username, exposed credential, poor passwords, lack of robust password recovery etc. |
| Insufficient authentication/ authorization | Privilege escalation (design flaw or configuration error in an application or operating system) |
| Insecure network services | DoS, buffer overflow, fuzzing attacks etc. |
| Lack data encryption and verification | Transmission of unencrypted data and credential |
| Privacy concerns | Unnecessary collection of user data; personal data exposed and inadequate checks on who accesses user data |
| Insecure cloud interface | Account listing, no lock-out, network traffic exposed credentials |
| Insecure mobile interface | Insufficient authentication, lack of encryption and listing of accounts |
| Insecure security configuration | Poor password rules, no data encryption and no security logging |
| Insecure software/firmware | Failure to secure update, not checked files before uploading |
| Poor physical security | Simple to disassemble unit, USB port access to applications, storage media removable |

**Table 6**
Perception layer types of attacks.

| Attack | Countermeasure |
|---|---|
| Node capture Attacks | Authentication, encryptions |
| Malicious code Injection attack | Continuously observe the behavior of running system. |
| False data injection attack | Authentication |
| Tampering | Prevent sensor physical damage |
| Eavesdropping and interface attacks | Encryption techniques, Access controls, access restriction etc. |
| Jamming | Use of low transmission power, channel surfing etc. |

**Table 7**
Network layer attacks.

| Attack | Countermeasure |
|---|---|
| Phishing site attack | Do not open unknow emails |
| Access Attack/Man-in-the-Middle attack | Encryption method between client and server, identification and authentication techniques. |
| DoS attack | Intrusion Detection Systems (IDS) and an Intrusion Protection Systems (IPS) |
| Sybil attack | Unique shared key between the node and the base station |
| Routing attacks/sinkhole attack | Continuous monitoring the nodes. |
| Hello Flood attack | Authentication of adjacent nodes using a protocol for identity checks. |

**Table 8**
Middleware layer attacks.

| Attack | Countermeasure |
|---|---|
| Flooding attack in cloud | User authentication |
| De-synchronization | Authenticate each forward packet |
| SQL injection attack | Validate user input, encryption, limited rights |
| Man-in-the-Middle attack | Encryption method between client and server, identification and authentication techniques. |

**Table 9**
Application layer attacks.

| Attack | Countermeasure |
|---|---|
| Data theft attacks | Data encryption, user and network authentications etc. |
| Data corruption | Anti-virus, firewalls, spy-ware etc. |
| Sniffing attacks | Security protocols |
| DOS attacks | Intrusion Detection Systems (IDS) and an Intrusion Protection Systems (IPS) |
| Malicious code injection attacks | Continuously observe the behavior of running system. |
| Reprogram attacks | Protect programming process |

Each layer has its own security attacks and is a lay architecture. There are a variety of safety issues that needs to be tackled. The focus of recent studies is mainly on IoT authentication and access control protocols, but rapid technological progress requires the introduction of new networking protocols like IPv6 and 5G in order to achieve the future IoT security requirements.

### 4.5. Perception layer/sensing layer threats

The key feature of the perception layer is knowledge collection. This layer is used to collect information via sensors, RFIDs, barcodes, etc. Due to its wireless nature, the attacker can attack his sensor node (Vashi et al., 2017). All kinds of sensors like RFID, NFC and sensor nodes are key technologies of the perception layer. It consists of two sections: the sensor, controller and perception network (including [3]. The perceptual network interlinked between network layer.

Node capture attacks: The combination of multiple low-power nodes is an IoT application. These knots are prone to a range of attacks. It is possible for an intruder to capture the node and to obtain all information and data (Hassijah et al, 2019).

Malicious code Injection attack: The attacker will insert a certain malicious code into the node memory during this form of attack. The attacker will compel the node to perform such unintended functions by inserting this type of code (Vashi et al. 2017), (Li, S et al. 2016). (Hassija et al. 2019).

False Data injection attack: When the node is captured by the attacker, the IoT device is able to insert wrong data. This results in wrong results, which can be used to trigger a DoS attack (Hassija et al., 2019).

Tampering: The assailant can reach the sensors physically. The intruder will use this method to acquire sensitive data, such as encryption/decoding keys [8].

Eavesdropping and interference: IoT framework consists of different nodes used in an open environment, exposing eavesdropper to IoT applications. During the various stages (Vashi et al., 2017) the target will catch the date [8].

Jamming: This attack disrupts the radio link, and the attacker sends useless data to corrupt or lost the post. Such attacks can be broken down into four categories: persistent jamming, misleading jamming, spontaneous jamming and reactive jamming.

### 4.6. Network layer/transportation layer

This layer relay on information gathered by the perception layer, is also known as a transport layer (Vashi et al., 2017). The layer provides network transmission, protection of information and the distribution in the perception layer of data transmission and sensitivity for storage. Alaba, Othman, Hashem and Alotaibi [3] are the network layers which include mobile devices, cloud and the Internet. This layer gives the application and the service an interaction. An appropriate safety policy for defending against attacks should be established (Li, S et al., 2016).

Phishing site attack: The attacker attempts to catch the different IoT devices in this kind of attack by reducing efforts. The attacker attempts to intercept one person's username and password, rendering the entire IoT device open to cyber assault (Hassija et al., 2019).

Access attack: An unauthorized entity would have access to the IoT network during this attack. The intruder will remain undetected on the network for a long time. This kind of attack is intended to gather useful information rather than to destroy the network (Hassija et al., 2019).

DoS attack: This link overflows the network with excessively high traffic from an attacker, causing the targeted system and network to run out of resources (Vashi et al., 2017) (Li, S et al., 2016). Many IoT devices are not completely equipped, making the attack simple (Hassija et al., 2019).

Sybil attack: During the sybil attack, malicious nodes may establish further identities so that other nodes can be fooled. The attacker's goal in this situation, without any physical node, is to take control of various areas of the network (Radoglou et al., 2019) [8].

Routing attacks/sinkhole attack: In a malicious node such as this, attempt to redirect the routing path and drag the nodes into this node. (Cerullo et coll., 2018) (Hassija et coll., 2019).

Hello flood attacks: HELLO was used by a node to connect to the network. Hello Flood Attack is the transmission of a large part of this message such that the networks flood and hence other forms of message cannot be exchanged. [Radoglou et al. 2019] [8].

### 4.7. Middleware layer

The IoT middleware layer is built to interface the network layer and the application layer. This layer also has good strengths in computation and storage. Layer of Middleware includes device discovery and administration, big data analysis, security etc. A safe and stable IoT interface is also available for Middleware layer and vulnerable to various attacks (Hassija et al., 2019). Furthermore, this level has two major functions, i.e., service management and storage into the database of lower layer information, to collect, process, compute and then automatically evaluate middleware layers based on computable performance (Vashi et al., 2017).

Flooding attack in cloud: By rising the cloud service load, this attack has a significant effect on the cloud system. This attack operates in the cloud in the same way as the DoS, impacting service quality (QoS). The intruder sends numerous requests to a provider on a daily basis (Hassija et al. 2019) [8].

SQL Injection Attack: Attackers can integrate malicious SQL statements into a programme in such attacks. The assailant can receive some user's private data or may even change the database record (Hassija et al., 2019).

De-Synchronization: An attacker sends a fake sequence number to decompose endpoints and generate data transfer [8].

Man-in-the-Middle attack: This is the type of the attack by arousal in which the communication channel is the object of an attack. The unauthorized party can control without identification the communication between the two parties (Vashi et al., 2017).

### 4.8. Application layer

The application is the highest layer which can be perceived by the end user. Such applications include SMT, SMT, healthcare and intelligent protocols [3]. Applications are also included in this layer. This layer has specific concerns about protection, including data theft and privacy problems that are not present in other layers. Most IoT applications are often made up of sub-layers between a network and a typically referred to as a support layer or a middleware layer. (France et al., 2019).

Data thefts: In IoT applications, many important and private data are dealt with. The transit data is more fragile than the rest of the data. Users are continually unable to transmit their private IoT data (Hassija et al., 2019).

Data corruption: The potential attacks on this layer involve malicious codes such as viruses, spyware, worms etc. Malicious codes will modify sensor data, and the recipient will receive incorrect data and carry out incorrect action [8].

Sniffing attacks: The attackers will use sniffer to track IoT application network traffic. This could allow attackers to access sensitive user information.

Denial-of-Service attack: Such attacks stop authentication users from using the IoT-program by making servers or networks artificially too busy to respond.

Malicious code injection attacks: An attacker can insert the wrong code into a script, as this is the easiest way to break the protection. Because of this attack, an IoT account can be hacked and an IoT device paralyzed.

Reprogram Attacks: If the programming process is not secured, attackers may attempt to remotely reprogram the IoT object. The IoT network may be deprived.

## 5. Conclusion

The inference is that IoT is an incredibly fascinating idea that provides many new opportunities in the form of services and innovations. IoT provides various applications that facilitate our lives, such as healthcare, travel, and agriculture. IoT enables individuals, intelligent objects to connect to any network, anytime, anywhere. Network open to a number of security and privacy issues that have a high priority to remember. This work was aimed ultimately at educating the reader on the IoT definition, with special emphasis on IoT protection and privacy. IoT is faced with numerous security and privacy concerns due to the exponential rise in security and privacy problems, including computers, individuals, vehicles and networks from anywhere and at any time.

This work also discusses numerous attacks on all levels of an IoT architecture on security threats. It discussed security problems relating to the layer of understanding, network layer, middleware layer and application layer. In this work we discuss all the IoT security risks, including DoS, Tempering, Tempering, etc. IoT protection was also discussed with some of the future research recommendations for improving IoT security. This analysis of the literature can be a valuable guide for understanding safety concerns at each IoT layer.

Lastly, much research in different IoT areas is available, but protection and privacy remain the weakest part of it. Different investigators have suggested a wide range of lightweight protocol adaptations and IoT authentication methods, making it difficult to find the best solution. IoT therefore needs formal standards to connect any type of instrument, protocol, application, etc. IoT requires standardization guidelines.

## CRediT authorship contribution statement

**V Srinadh:** Conceptualization, Methodology, Software. **Mannava Srinivasa Rao:** Data curation, Supervision, Software, Validation. **Manas Ranjan Sahoo:** Writing - review & editing, Visualization. **K. Rameshchandra:** Investigation, Writing - original draft.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

[1] M. Abomhara, G. Koien, Security and privacy in the Internet of Things: Current status and open issues, 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014.

[2] G.A. Akpakwu, B.J. Silva, G.P. Hancke, A.M. Abu-Mahfouz, A survey on 5G networks for the internet of things: Communication technologies and challenges, IEEE Access 6 (2018) 3619–3647.

[3] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: A survey, J. Netw. Comput. Appl. 88 (2017) 10–28.

[4] Awad, Ali Ismail Fairhurst, Michael. (2018). Information Security - Foundations, Technologies and Applications. (pp. 13-15). Institution of Engineering and Technology. Retrieved from .

[5] E. Bertino, N. Islam, Botnets and internet of things security, Computer 50 (2) (2017) 76–79.

[6] A. Burg, A. Chattopadhyay, K.-Y. Lam, Wireless communication and security issues for cyber-physical systems and the internet-of-things, Proc. IEEE 106 (1) (2018) 38–60.

[7] M. Burhan, R. Rehman, B. Khan, B. Kim, IoT elements, layered architectures and security issues: A comprehensive survey, Sensors 18 (9) (2018) 2796.

[8] Cerullo Gianfranco, Mezzo Giovanni, Papale Gaetano, Ragucci Bruno, Sgaglione Luigi. (2018). IoT and Sensor Networks Security.

[9] B. Dorsemaine, J. Gaulier, J. Wary, N. Kheir, P. Urien. 2015. Internet of Things: A Definition & Taxonomy. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.

[10] Evans, D., 2012. [online] Cisco.com. Available at: <https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf> [Accessed 21 May 2020].

[12] M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the IoT world: Present and future challenges, IEEE Internet Things J. 5 (4) (2018) 2483–2495.

[13] Q. Gou, L. Yan, Y. Liu, Y. Li, 2013. Construction and Strategies in IoT Security System. 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[15] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generat. Comput. Syst. 29 (7) (2013) 1645–1660.