International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 2 Article 1

January 2022

Survey on Security Issues and Protective Measures in Different Layers of Internet of Things (IoT)

Rasmita Jena
Udayanath (Auto.) College of Science and Technology, Adaspur Cuttack, Odisha, rasmitajena14@yahoo.com

Anil Kumar Biswal
Dept. of CSE, ITER, SOA(Deemed to be University), BBSR, Odisha, India, anil.biswal123@gmail.com

Debabrata Singh
Department of CA, ITER Siksha 'O' Anusandhan,(Deemed to be University) Bhubaneswar-751030, Odisha, India, debabratasingh@soa.ac.in

Arundhati Lenka
Udayanath (Auto.) College of Science and Technology, Adaspur Cuttack, Odisha, l_arundhati@yahoo.co.in

Recommended Citation

Jena, Rasmita; Biswal, Anil Kumar; Singh, Debabrata; and Lenka, Arundhati (2022) "Survey on Security Issues and Protective Measures in Different Layers of Internet of Things (IoT)," *International Journal of Smart Sensor and Adhoc Network*: Vol. 3 : Iss. 2 , Article 1.
DOI: 10.47893/IJSSAN.2022.1203
Available at: https://www.interscience.in/ijssan/vol3/iss2/1

Survey on Security Issues and Protective Measures in Different Layers of Internet of Things (IoT)

Cover Page Footnote

I would like to acknowledge that: • All authors of this research paper have directly participated in the planning, execution and analysis of this study. • This manuscript has not been published earlier and neither it is under consideration for publication elsewhere.

Survey on Security Issues and Protective Measures in Different Layers of Internet of Things (IoT)

Rasmita Jena[1], Anil Kumar Biswal[2], Debabrata Singh[3], Arundhati Lenka[4]

[1,4]Dept. of CS, Udayanath (Auto.) College of Science and Technology, Adaspur Cuttack, Odisha
[2]Dept. of CSE, ITER, Siksha O Anusandhan (Deemed to be University), BBSR, Odisha, India
[3]Dept. of CA, ITER, Siksha O Anusandhan (Deemed to be University), BBSR, Odisha, India

rasmitajena14@yahoo.com[1], anil.biswal123@gmail.com[2], debabratasingh@soa.ac.in[3], l_arundhati@yahoo.co.in[4]

Abstract: In general perspective, Internet of things is defined as a network of physical objects by connecting" things to things" through the sensors, actuators and processors, to communicate and exchange data and information among each other along with other related devices and systems spread over different locations, without human-to-human or human-to-computer interactions. This survey summarizes all the security threats along with privacy issues that may be confronted by the end users in Internet of Things (IoT). The majority of survey is to gather information about the current security requirements for IoT, the further scope and the challenges in IoT and the measures to prevent attacks upon the IoT systems.

Keywords: Threats, Internet of Things (IoT), Security, Wireless Sensor Networks (WSNs), Privacy

1. Introduction

With the emerging field in internet and communication technologies, we can take the human life virtual world step by step. As human live in a physical world, it is not at all possible for them to work, chat, keep pets and plants in the virtual world cannot be implemented fully in human activities. Hence, it is quite difficult to enhance the service excellence with the development of internet virtual world. The technology which combines both virtual world and real world is termed as Internet of Things (IoT). It will change the human life style by fulfilling the new demands of human being with future society as well as the business model by using a low cost sensor network and wireless communication technology [1] [2]. In IoT, many physical devices are connected to communicate and exchange vital information related to healthcare, office, house hold objects like kitchen appliances, humidity and temperature control etc.

This technology ensures to empower the commodity and successfully proven to handle any hazardous and repeated task. It also helps in replacing physical labor through technology, thus satisfying individual needs. Up-gradation of various technologies in IoT using computers and mobile devices emerge the remote access of smart homes, healthcare, smart energy, Military and industry automation systems, which are the real life applications of IoT. We will discuss briefly about the various application areas and role of IoT in COVID-19 of the current pandemic in health care systems. However, in coming future the huge implementation of IoT in different areas also need to face many security and privacy issues for smart, connected and mobile IoT devices and challenges of IoT.

In particular, the cryptographic properties such as data confidentiality, authenticity, integrity and authorization must be provided by IoT for the security solution of IoT nodes (i.e. things, users. servers, objects). In addition, the privacy protection must be considered [1].

1.1 Contributions

The Internet of Things connects a massive number of devices, users, and their related services and apps, allowing them to interact with one another. While this improves the user experience, it also raises a number of security concerns. Numerous proposals have been proposed to handle IoT security challenges, including access control, privacy, trust, identity, and so forth. The majority of these are concerned with finding answers to specific problems. To the best of our knowledge, there is no complete set of standards for an IoT security architecture that satisfies all of the needs of an IoT system as of now. This complicates the safe, resilient, and scalable deployment of IoT applications and services. We emphasize that current security architectures do not adequately recognize and incorporate an IoT system's characteristics and security-specific requirements. The larger scale of IoT systems and the wide range of applications will necessitate the development of a security architecture that takes into account the many characteristics of such systems.

In this study, we attempt to bridge the gap by synthesizing existing recommendations for state-of-the-art IoT security criteria into a single publication. We intend to address the following key research topic in particular: what are the needs for the design and provision of security for the IoT? The majority of the preceding proposals make no distinction between various security concerns and IoT security requirements. In other words, they do not cover the technical issues and characteristics required to generate a list of IoT security criteria. While some of them address the needs on an individual basis, they do not provide a thorough survey.

Rest of the paper is organized as follows: section 2 gives overviews and background along with an analysis on architecture of IoT and real life application of IoT and section3 will provide a brief discussion on security and privacy of IoT, section 4 draws the conclusion of the review with references at the end.

2. Overviews and Backgrounds IoT

2.1 What is Internet of things?

In this Literature review, we discussed about the structure, various application areas, the security and privacy related issues of IoT along with some open challenges. With the help of communication technology, Radio Frequency

Identification (RFID) and Wireless Sensor Networks (WSNs), the sharing of data and information take place. IoT enables to connect people and smart things or objects around us, at anytime, anyplace, with anything and anyone, most preferably using network for exchanging data with each other without involvement of human. They are “Material objects connected to material objects in internet [3] which is shown in Figure 1.

There are several IoT technologies available, involving both hardware and software. The devices used to realize the IoT are classified as hardware, while the protocols and associated programs are classified as IoT software. Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Bluetooth, Wi-Fi, Smart Phones, and other devices are some of the most common and crucial IoT gadgets. Artificial Intelligence (AI), ZigBee, Near Filed Communicators (NFC), and other software are utilized to communicate these devices [2]. The hardware devices can collect data from installed sensors and send it to servers via local digital networks or the internet.

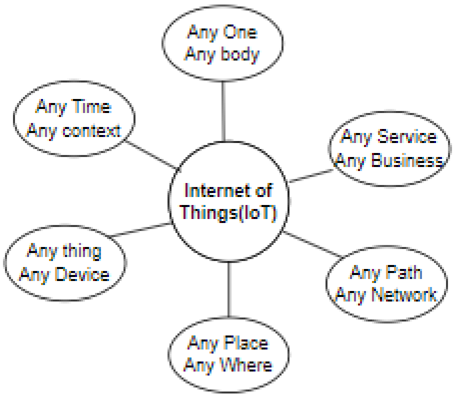

Figure 1: Test Scenario of IoT

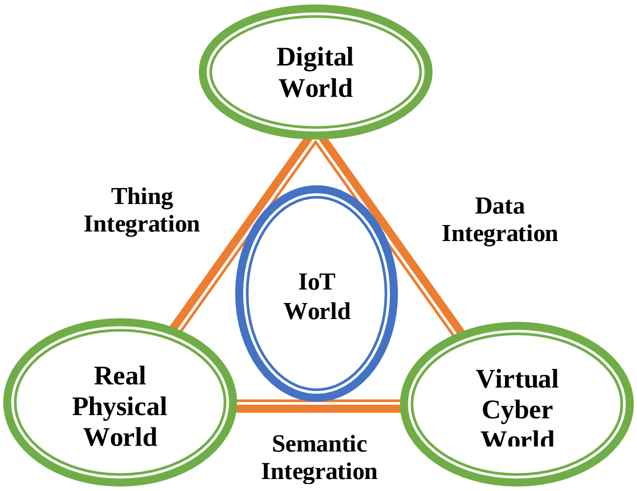

Figure 2: IoT: a symbolic interaction model with various world

A symbolic interaction model of IoT is fully interacted with the various world like: real physical world, digital world and virtual cyber world which is depicted in Figure 2. So these worlds are integrated with the three terms such as: thing, data, and semantic integration.

2.1 Evolution of Internet of Things (IoT)

The rapid development of internet commences, by connecting device to device to communicate and exchange data and information using various technologies. Then the mobile internet was introduced by connecting mobile devices to the internet and User. And finally people tried to connect physical objects or things to internet to make life more easy and comfortable, which leads to “Internet of Things” i.e. Internet of everything can refer to IoT [17].

The Internet was first introduced in 1989 by connecting device to device to exchange data and information, and since from the evolution of internet, the trend of connecting various objects to internet have become very popular and widely adapted, Then the mobile devices connected to form mobile internet [4] [23].

The main advantage of IoT is to allow infinite number of machines to be connected with each other to produce and transmit information through a large scale of wireless network using automated device and sensor, which may not be useful in case of incorrect and insufficient data processing [18]. This section begins with a discussion over essential technology of IoT, Architecture and protocol required for IoT networks which is depicted in Figure 3.

IoT based on 5 different essential technologies for the successful deployment of IoT based services and products such as

i. RFIDs: Radio Frequency identification
ii. WSN: Wireless sensor Network
iii. Middleware
iv. Artificial Intelligence (AI)
v. ZigBee

i. Radio Frequency Identification: It has rendered capability to automatically identify and capture unique data using its different components such as RFID tag and RFID Reader. RFID Tag, Reader, and Antenna may be used to communicate data across systems. Tags with RFID technology can be used to transmit digital data and store data in EPC (Electronic Product Codes) format. [26]. It's similar to a smart barcode tracking system, with an exception of storing more data than a regular barcode system. Three different types of RFID tags are available, namely the active, passive and semi-passive. There is no battery in the tag and the power comes from a solar cell. An active RFID tag continuously broadcasts its own signal like a telephone and has its own power source [27]. It is basically used in the field of manufacturing, hospital laboratory equipment’s etc.

As compared to using an internal power source, a passive RFID tag is powered by the radio frequency energy that is transferred between a reader and a tag during the reading process. It is used in supply chains as well as electronic tolls and more. Batteries are used to power the microprocessor in semi-passive tags, which then communicated by sucking power from readers [16].

ii. Wireless Sensor Networks (WSNs): It is an infrastructure less wireless network. It has dedicated sen*sor* attached to cooperate with RFID sensor that monitor physical environment condition and passes the data (such as Temperature, pollution level, humidity and wind) through their network to the central system [22].

iii. Middleware: It is software lies in between Operating system and the application running on it [8].

iv. Artificial Intelligence (AI):

As the name implies, artificial intelligence (AI) serves as a substitute for human intelligence. It is responsible and sensitive enough to make decisions as individuals. In this current era, people expect devices to behave like people, to respond to their words and act accordingly, to function as if they were virtual persons [28].

v. ZigBee:

ZigBee, like Bluetooth, is a popular short-range wireless technology that can transport data at roughly 250 Kbps and has a range of about 100 meters. It is a less expensive, less energy-consuming, and more secure wireless networking solution. It can be found in star topology, mesh topology, and tree topology [29].

2.2 Architecture of IoT

The structure of IoTs consists of following 4 different layers such as perception layer, Gateway and Network Layer, management service layer and Application layer.

A. **The perception layer**

This layer is also called as device layer or recognition layer. It consists of various sensor networks, RFID tags, embedded systems, readers and actuator to gather information [15]. In this layer the sensor first receives data and information in analog form and converts it to its corresponding digital form. Each of these sensors recognizes the physical world, information storage (e.g. RFID tags) and information collection (e.g. sensor Network) [4].

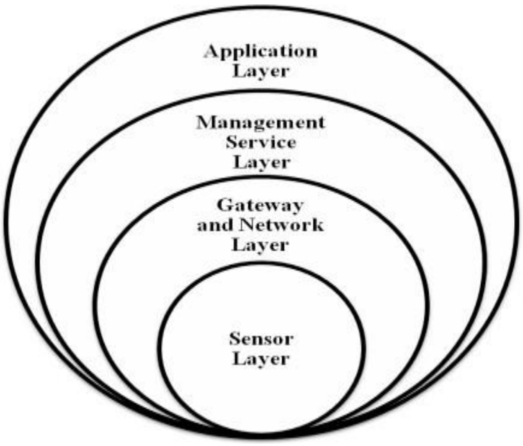

Figure 3: Architecture of IoT

B. Network and gateway layer

These two layers consist of physical component and network communication software. In network layer the relevant data and information, which are collected from sensor and actuator transforms to its next layer (i.e. Management Layer) through multiple communication protocols and processes the data to some extent and sends the particular information to the cloud [15]. It also provides intelligence by sending back the data received from the cloud. It should have robust network and high performance and support multiple organizations to exchange information

With each other independently [3].

C. Management Layer

In between application Layer and Network layer, it acts as an interface in a bidirectional mode. As a result, this layer is responsible for receiving large amount of raw data from different connecting devices and extracting important information from stored data as well as real-time data while guaranteeing security and privacy [6].

D. An application layer

It is the top most layer of IoT. This layer is known as the user interface layer. It provides same type of services to all its connected devices, and responsible for delivering application specific services to the user. It acts as end user layer, where the user can access different applications on various fields such as health care, military, transportation, supply chain, agriculture, government, retail etc. [10] [14].

3. Applications of IoT in various fields

A survey has been done based on 270 responses from 31 countries to solve day-to- day problems on various fields such as Smart home, Smart city, Retail, Agriculture, smart Factory, Supply Chain, Healthcare, User Interaction, Environment and Energy, etc. In this part we discussed briefly on IoT Applications in Medical (health care), Smart Home, Smart cities, Agriculture and Education which is also shown in Figure 4.

A. IoT in Medical Application

Due to growing population, rural urbanization, ageing population, economic growth and socially unbalanced resource utilization, some problems [some social problems] in the health care f have become increasingly apparent

Due to rapid growth in diseases and inadequate healthcare facilities, numbers of patients are increasing. Elderly people with multiple diseases are suffering, which has turned to be a serious social issue

- In rural areas, lack of medical facilities, limited medical staff, and inadequate health care system, and shortage of institutional facilities has become a major issue to avail medical services as well as people's Livelihood [12].
- Because the national strategy to protect the health of citizens is taking long time to be implemented, a heavy burden is placed on the economy, individuals, families, and states.
- Inadequate disease prevention and early detection capability [2].

To solve the above issues, IoT play a vital role to improve the health care system in society irrespective of location, time, and user's activity. The Remote Monitoring and Management platform of Health care information (RMMP-HI), can improve quality of human life by performing some basic tasks such as a sensor that can be placed in patient's body and collect information regarding the healthcare of the patient and transmit information to internet making the important health information available to doctors, family members of the patient and others who opted to get it. It is also used to monitor patient's current medicine and assess the expected health hazards against new medicine in terms of any allergic and other reaction. A person's body temperature, heart beat and blood pressure can also be tracked by the help of the sensors and technology used in IoT [3]. In the recent years, IoT has been received a substantial attention to fight against infectious diseases, i.e. COVID-19. This disease has similar symptoms like normal cough and fever. The diagnosis of COVID-19 is addressed in following phases such as early diagnosis, quarantine time [30].

In the early diagnosis phase, a patient needs faster diagnosis due to contagiousness nature of the disease. So, it is important to diagnose the patient as soon as possible to prevent the virus from spreading. Devices such as sensors are used in this phase to detect and capture information about patient's health condition, including body temperature and taking blood samples from suspicious cases. The next phase is called as quarantine phase, where he or she requires being isolated for a particular period of time depending on the patient's age and infected condition; it may take 14 days or more. During this period, a patient may be monitored remotely with the help of IoT device for treatment. In this current Pandemic situation, the IoT technology has been proved to be a safe and efficient method of detecting and treating with COVID -19 [13].

B. IoT in smart Home

Now a day, smart home is termed as a residence where the telecommunication networks interconnect essential home appliances, to provide proactive services such as monitoring light, room temperature, humidity, and reduce cost against the communication technology, information technology and electronics. Home automation controls all the function and features of smart home automatically by using one or more computer. The main aim of this system is to enhance the quality of life, reduce operating costs and optimize the energy consumption and also windows, doors Air conditioning as well as Refrigerator, washing machine can manipulate and control by remote platform and programs [5].

C. IoT in Design of Smart Cities

It is possible to design smart cities using the Internet of Things (IoT) e.g. monitoring traffic and air quality, discovering emergency routes, efficient lighting up of the city, watering gardens, etc. [5]. People in this current day require a smart system. Users must perform their tasks intelligently. They are looking for such user-friendly programme that would allow them to do item monitoring, home security, handling various appliances, workspaces, and so on. Object tracking refers to the tracking of various user objects such as smart phones, monitoring things using Global Positioning System (GPS), and so on.

D. IoT in Agriculture

Farmers find it difficult to check the soil's PH, nutrition, humidity, and other parameters on a regular basis. The temperature of the green house can become unpredictable at times, resulting in poor plant growth or death. In this case, IoT will automatically check the PH value, nutrition value, amount of humidity in the soil, and so on, and will supply the necessary nutrients to the soil or plants as needed. IoT can also monitor the temperature of the green house and automatically set the temperatures that are appropriate for the plants. IoT can also monitor the water quality provided for plantation purposes [20]. It can also provide the necessary amount of fertilizer for various plants. IoT may be used on both the ground and in the air. In the bottom level, IoT devices can readily identify crop health, crop length, insects if any are detected in the crops, toxins collected at the roots of the plants, and so on.

E. IoT in Education

Smart education refers to the use of smart technologies to teach students in a way that not only attracts kids to learn new things but also allows individual students to learn according to their comprehension standards. By reducing costs, IoT enables students to learn new and inventive things. It not only benefits the students, but it also allows academicians and administrators to quickly manage the students and respond to or provide feedback on their performance [31].

The development of smart boards or digital boards entices students to combine photos, videos, audios, and other media to facilitate their learning process. The digital boards are so efficient, both electronically and technologically, that they make it easier for kids to learn new topics. Students used to digitally design posters, change existing ones, share such files to anyone, and so on. The concept of interactive learning through various applications assists students in analyzing problems and finding solutions. These interactive movies are so effective that kids may comprehend any topic with ease.

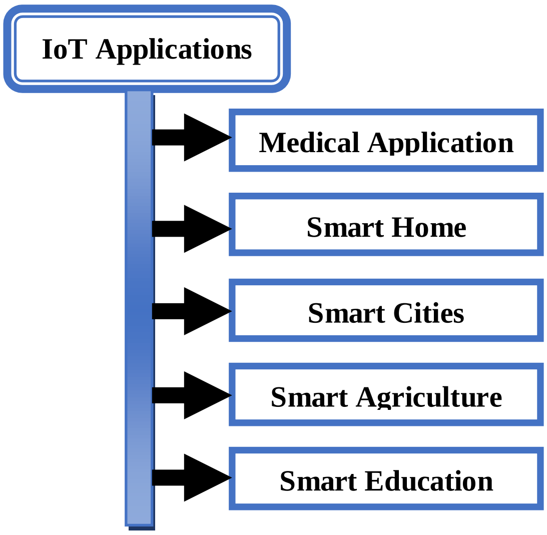

Figure 4: Application of IoT in various fields

4. Security, Privacy and Challenges in IoT Layers

Due to the popularity and high acceptance of IoT, the main challenge is to provide complete security and privacy to user's private and sensitive data. This section describes the various security challenges faced at the different layers of the IoT.

4.1 Security issues in the Perception Layer

In perception layer, various IoT devices are connected with each other to communicate or exchange data and information. The hardware attack is the most general attack in this layer,which are describe as follows:

- **Forged node insertion:**

It's possible for an attacker to destroy IoT devices and stop data transmission between them by using a Forged Node Insertion (FNI) attack. Here, the attacker inserts an invalid node in order to gain control over a network's data stream, causingit to be unavailable [15].

- **Hardware Jamming:**

Attacker can obtain information relating to communication keys, routing table, cryptographic key by replacing original parts of hardware and also by capturing the gateway node [15].

- **Unauthorized access to tags:**

The device tags can be accessed and modified by unauthorized user without authorization [9].

- **Spoofing:**

In spoofing, attacker can make RFID system false by transmitting false and manipulated information to RFID system and making it appear as authenticate and original source [9].

4.2 Security issues in the Network Layer

Some security challenges in network layer are given below:

- **Denial of services:**

In DOS attack, the attacker enforces to shut down a machine or network, making it inaccessible or unavailable to the intended users by overwhelming or flooding with alots of useless traffic [14] [19].

- **Man in Middle Attack:**

In this assault, the attacker does not need to be physically present on the network. When an attacker interrupts a communication channel, it can be observed andmanipulated [9].

- **Sinkhole Attack:**

It is one of the most damaging routing assaults on the Internet of Things. Attackers collapse network connectivity to prevent data packets delivery to their intended destination. [9].

4.3 Security issues in the Network Layer Application Layer

- **Phishing Attacks:**

By faking the user's authenticated identity, the attacker can gain access to sensitive and confidential data and information through an infected email or phishing website [14][15].

- **Virus, Worms, Spyware, Trojan horse:**

As a result of an adversary infecting the system with malicious software code, a variety of events can occur such as information theft, data manipulation, denial of services, or incorrect data [15].

Summary of security challenges of IoT:

Layer	Possible Attack	Description
Perception Layer	Forged Node Insertion	Insert a invalid node in between the actual data of network, to get access and causes the Unavailability of Network services.
	Hardware Jamming	Damage the node by replacing original parts of device hardware and get information regarding communication Keys, routing table, cryptographic keys.
	Unauthorized access	Attacker can get access and modify RFID tags without authorization.
	Spoofing	Make RFID system falsely by transmitting incorrect information but appear like authenticate and original source.
Network Layer	Denial of services(DOS)	DOS attack occurs when attacker hacks with overwhelming or flooding a lot of useless traffic.

	Man In The attack	Attacker target the communication channel between two parties and the channel can monitor and control by unauthorized user.
	Sinkhole	An adversary drops the entire data packet instead of delivering at its proper destination.
Application Layer	Phishing attack	Attacker can get access confidential information by spoofing user's authentication.
	Virus, worms, spyware, Trojan horse	An Adversary can infect the system with malicious software code resulting Denial of Services or corrupt data.

4.3 Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a computer software or device that detects fraudulent behaviour or policy violations in a system or systems. The intrusion detection system (IDS) defines intrusion detection as "the identification of acts designed to impact trust, honesty, or available resources" [24]. Every detected action or breach is relayed to or efficiently collected by the Admin via the SIEM system. This SIEM combines all results from many sources in order to distinguish fraudulent behavior and counterfeit warning indicators from alert filters. The firewall appears to be distinct from the IDS, where both firewalls and IDS contribute to network security.

For network troubleshooting, make strategic network notes or markers. It examines the traffic flow throughout the entire sub-net and represents the congestion caused by documented sub-network attacks. The Host intrusion detection (HIDS) system is active on network access hosts [25]. This HIDS checks packets for incoming and outgoing devices and alerts your user or administrator to any unusual behavior. IDS stands for intrusion detection system, which searches for specified patterns such as network bit stream sequences or specific excellently sequences of a suspect's harmful instructions.

5. Protective Measures for different Layer of IoT Structure

In IoT, multiple physical Devices, technologies and companies have been involved, to transmit a lot of data through the smart sensors. It has been recognized that four interconnected and interactive components such as people, object, hardware and software are communicated over public and entrusted network, hence there may be a possibility of loss of private data in case of unauthorized manipulation of hardware and software.

i. **In Perception layer**, the temperature sensors, sound sensors, vibration sensors, pressure sensors are different types of controlling modules and also acts as collecting module to gather and interchange data in between them for which IoT is designed**.** The security issues can be raised in perception layer by the detecting a faulty node or abnormal sensor node. This can be happened when a cyber-attacker physically attacked, to destroy or disabled the sensor node. To avoid degradation of service in perception layer, it needs to detect the damage node and the take needful actions. Chen et al. [32], intended a localized fault detection algorithm to discover the faulty nodes in WSN.

Da Silva et al. [33], intended a decentralized intrusion detection system model for the WSN. Wang et al. [34] derived the intrusion detection probability in both homogeneous and heterogeneous WSN. Another way to protect the perception layer is the use of key exchange algorithm and cryptographic algorithm. Public key algorithm has used for node authentication and can be better secured the entire network as compare to key exchange algorithm [35].

According to Gaubatz et al. [36], Rabin's scheme, NtruEncrypt, and elliptic curve cryptography are three low-power public key encryption algorithms used for WSNs. Key management includes secret key generation, distribution, storage, updating, and destruction. But presently, internet applications like Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE) developed by some standardize bodies were used to solve all the security and communication related problems in internet network. These applications provide a protocol stack for the different layer of IoT, i.e. the standardized body IEEE 802.15.4 which is a group of Wireless Personal Area Networks (WPANs), emphasis for the secure communication between low resources like power, memory & bandwidth, with constrained environment devices. Hence it secures perception layer and the logical medium access layer (MAC) [16] [17].

ii. **In Network layer**, for IoT devices in WSN the data packets are transmitting to the transport layer by the help of the IPv6 protocol over low power wireless personal area networks (6LoWPAN) to enable IPSec communication with IPv6 nodes. Hence it is not necessary to modify existing end points on internet to communicate securely with WSN, which results the actual E2E security implementation without need of a trustworthy gateway. This IPv6 is controlled by Internet engineering task forces (IETE) application and defines many open standard protocols like UDP, TCP & HTTP. IPv6 can be helped in the packet encapsulation, packet fragmentation, header compression & reassembly the fragmented packets to recreate the original IPv6 packets. Raza et al. [37] intended an E2E secure communication between IP enabled sensor networks and the traditional Internet proposed an E2E secure communication between IP enabled sensor networks and the traditional Internet [16] [17].

iii. **In transport Layer**, two protocols are used i.e. UDP and TCP. UDP is lighter and much faster than TCP, so it is mostly used by the IOT scenarios. UDP is a connection oriented protocol and guarantee on the packet delivery. Header size of TCP is much greater than UDP. CoAP is higher level IoT protocol uses UDP in its application layer instead TCP [38]. As a consequence, regarding users, server and trusted third party must be addressed and ensure the IoT security trusted technologies which include device integrity, tamper_ resistant modules and trusted execution environments.

To ensure security in IoT, the main focus should be on confidentiality, integrity, authentication and availability of data. Confidentiality refers to secure information from unauthorized persons, parties or system during transmission of data packets [39]. Encryption is the common approach, which ensures the data confidentiality through encode and decode process as well as prevent unauthorized access of network generated data e.g. Domain specific information such as user identity, positions.

Transmitting data via a network with integrity ensures its accuracy and consistency. In this context, the use of sensor values or control orders to prevent data change by unauthorized users or systems during transmission of data over the network [40]. To prevent information alteration via message injection, message reply, and message delay on the network, integrity plays an important role which denies information change. Integrity violation can be a major reason for some security issues such as Modified data which may damage the control systems and facility which includes Communication and security system, lighting, heating and hydro systems [5].

The availability of the system resources ensures that the authorized individual can access them without being denied access to those resources. According to the term "availability of services", only authenticated real-time objects have access to the necessary resources when needed. An individual's life can be put at risk if they aren't available when they need to be when it's most important to be [21].

When a system, user or item is authentic, the system's internal principle can be mapped to this identity. In case of Device Authentication, the Forged data flow in the network could be prevented by ensuring device authentication before getting into network which results to keep away the malicious device from IoT environment. The Cryptographic hash algorithm can be used to validate the integrity and authentication of software on various devices of the IoT network when it comes to Safe Booting. The WH and NH cryptographic algorithm can be implemented on end device of network instead of hash algorithm as these devices posses very low computing power. Moving on to Web Firewall Application, Web firewall application should use to protect the IoT environment by identifying a possible attacker. It's also important to secure the security, authenticity, confidentiality and stability of the IoT environment by using anti-virus and anti-spyware software [15].

6. Conclusion

In this paper, the survey is based on the application areas of IoT where IoT plays an important role but still needs more research work in different fields. The scope of the study is to make life of the disabled and old age people easier and comfortable by providing best possible services to its users by communicating the embedded devices with remote objects or people through internet. The other future aspect of the study is to maintain privacy, data protection, authentication and security of the user which will became the challenge to the future trends.

References

[1] Andersson, K., You, I., & Palmieri, F. (2018). Security and Privacy for Smart, Connected, and Mobile IoT Devices and Platforms.

[2] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).

[3] Soumyalatha, S. G. H. (2016, May). Study of IoT: understanding IoT architecture, applications, issues and challenges. In 1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications (No. 478).

[4] Malik, A., Magar, A. T., Verma, H., Singh, M., &Sagar, P. (2019). A detailed study of an internet of things (IoT). International Journal of Scientific and Technology Research, 8(12), 2989-2994.

[5] Desai, D., &Upadhyay, H. (2014). Security and privacy consideration for internet of things in smart home environments. International Journal of Engineering Research and Development, 10(11), 73-83.

[6] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.

[7] Borgohain, T., Kumar, U., &Sanyal, S. (2015). Survey of security and privacy issuesof internet of things. arXiv preprint arXiv:1501.02211.

[8] Abomhara, M., &Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In 2014 international conference on privacy and security in mobile systems (PRISMS) (pp. 1-8). IEEE.

[9] Alferidah, D. K., &Jhanjhi, N. Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. International Journal of Computer Science andNetwork Security IJCSNS, 20(4), 263-286.

[10] Leloglu, E. (2016). A review of security concerns in Internet of Things. Journal ofComputer and Communications, 5(1), 121-136.

[11] Ravindran, R., Yomas, J., &Jubin Sebastian, E. (2015). IoT: A review on security issues and measures. International Journal of Engineering Science and Technology, 5(6), 348-351.

[12] Zhao, W., Wang, C., &Nakahira, Y. (2011, October). Medical application

on internet of things. In IET international conference on communication technology andapplication (ICCTA 2011) (pp. 660-665). IET.

[13] Nasajpour, M., Pouriyeh, S., Parizi, R. M., Dorodchi, M., Valero, M., &Arabnia, H. R. (2020). Internet of Things for current COVID-19 and future pandemics: An exploratory study. Journal of healthcare informatics research, 1-40.

[14] Andrea, I., Chrysostomou, C., &Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.

[15] 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.

[16] Anil Kumar Biswal, Debabrata Singh, Binod Kumar Pattanayak, Debabrata Samanta, Shehzad Ashraf Chaudhry, Azeem Irshad, "Adaptive Fault-Tolerant System and Optimal Power Allocation for Smart Vehicles in Smart Cities Using Controller Area Network", Security and Communication Networks, vol. 2021, Article ID 2147958, 13 pages, 2021. https://doi.org/10.1155/2021/214795

[17] Biswal, A. K., Singh, D., Pattanayak, B. K., Samanta, D., & Yang, M. H. (2021). IoT-Based Smart Alert System for Drowsy Driver Detection. Wireless Communications and Mobile Computing, 2021.

[18] Biswal, A. K., Singh, D., & Pattanayak, B. K. (2021). IoT-Based Voice-Controlled Energy-Efficient Intelligent Traffic and Street Light Monitoring System. In Green Technology for Smart City and Society (pp. 43-54). Springer, Singapore.

[19] Singh, D., Pati, B., Panigrahi, C. R., & Swagatika, S. (2020). Security issues in iot and their countermeasures in smart city applications. *Advanced Computing and Intelligent Engineering*, *1089*, 301-313.

[20] N. P. Mohanty, D. Singh, A. Hota and S. Kumar, "Cultivation of Cash Crops under Automated Greenhouse using Internet of Things (IoT)," *2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0235-0239, doi: 10.1109/ICCSP.2019.8697930.

[21] Singh, D., Mishra, P. M., Lamba, A., & Swagatika, S. (2020). Security Issues in Different Layer of IoT and Their Possible Mitigation. *International Journal of Scientific & Technology Research*, *9*(04), 2762-2771.

[22] Bhanipati, J., Singh, D., Biswal, A. K., & Rout, S. K. (2021). Minimization of Collision Through Retransmission and Optimal Power Allocation in Wireless Sensor Networks (WSNs). In *Advances in Intelligent Computing and Communication* (pp. 653-665). Springer, Singapore.

[23] Chakraborty, S., Singh, D., & Biswal, A. K. (2021). NAARI: An Intelligent Android App for Women Safety. In *Applications of Artificial Intelligence in Engineering* (pp. 625-637). Springer, Singapore.

[24] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, *7*(8), 6882-6897.

[25] Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M. A., Mukherjee, M., & Khan, F. A. (2019). Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors*, *19*(14), 3119.

[26] Bashir, U., Jha, K. R., Mishra, G., Singh, G., & Sharma, S. K. (2017). Octahedron-shaped linearly polarized antenna for multistandard services including RFID and IoT. *IEEE Transactions on Antennas and Propagation*, *65*(7), 3364-3373.

[27] Mamun, M., Miyaji, A., Luv, R., & Su, C. (2021). A lightweight multi-party authentication in insecure reader-server channel in RFID-based IoT. *Peer-to-Peer Networking and Applications*, *14*(2), 708-721.

[28] Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT security for smart cities. *ACM Transactions on Internet Technology*, *21*(4), 1-21.

[29] Adi, P. D. P., Sihombing, V., Siregar, V. M. M., Yanris, G. J., Sianturi, F. A., Purba, W., ... & Prasetya, D. A. (2021, April). A Performance Evaluation of ZigBee Mesh Communication on the Internet of Things (IoT). In *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)* (pp. 7-13). IEEE.

[30] Singh D, Prusty SK, Sarangi SS, Sahoo S, Biswal AK. Attitude, anxiety, psychological effects and prevention during COVID-19 in India. Indian J Pharm Educ Res. 2020;54(3s):s400-10. doi: 10.5530/ijper.54.3s.138.

[31] Lei, T., Cai, Z., & Hua, L. (2021). 5G-oriented IoT coverage enhancement and physical education resource management. *Microprocessors and Microsystems*, *80*, 103346.

[32] Chen, J., Kher, S., & Somani, A. (2006, September). Distributed fault detection of wireless sensor networks. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks* (pp. 65-72).

[33] da Silva, A. P. R., Martins, M. H., Rocha, B. P., Loureiro, A. A., Ruiz, L. B., & Wong, H. C. (2005, October). Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks* (pp. 16-23).

[34] Wang, Y., Wang, X., Xie, B., Wang, D., & Agrawal, D. P. (2008). Intrusion detection in homogeneous and heterogeneous wireless sensor networks. *IEEE transactions on mobile computing*, *7*(6), 698-711.

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

[36] Gaubatz, G., Kaps, J. P., Ozturk, E., & Sunar, B. (2005, March). State

of the art in ultra-low power public key cryptography for wireless sensor networks. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 146-150). IEEE.

[37] Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T., & Roedig, U. (2011, June). Securing communication in 6LoWPAN with compressed IPsec. *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)* (pp. 1-8). IEEE.

[38] Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2020). CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In *Digital Twin Technologies and Smart Cities* (pp. 151-175). Springer, Cham.

[39] Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581.

[40] Tukur, Y. M., Thakker, D., & Awan, I. U. (2021). Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4158.