International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 10 | Oct - 2021 ISSN: 2582-3930

A Review of Security Vulnerabilities in Internet of Things (IoT) Devices

Mrs. Farhana Jalal[1], Dr. Senthilkumar.S[2], Mr. Peer Mohamed Ziyath[3]

[1]*Department of ECE & M.E.T. Engineering College, Nagercoil*
[2]*Department of CSE & University college of Engineering, Pattukottai.*
[3]*Department of Computer Applications & B.S. Abdur Rahman Crescent Institute of Science and Technology.*

---***---

Abstract - The Internet of Things (IoT) has a significant impact on our everyday lives in a range of aspects, from small wearable gadgets to massive industrial systems. The significance of the Internet of Things is projected to grow dramatically in the next years. The Internet of Things (IoT) intends to improve people's quality of life. The Internet of Things (IoT) is a collection of devices that interact together using wireless technology, including software, sensors, and electronic gadgets. Smart healthcare, intelligent transportation, smart buildings, military, and industrial applications are some of the major areas where the Internet of Things provides considerable attention. In spite of the use cases to make the life smarter, IoT is subject to a variety of threats, demanding the use of difficult procedures to ensure its security. As the world's population grows, data must be automatically handled digitally and securely. But IoT networks are vulnerable to security concerns as the number of IoT devices grows. The primary goal of IoT security is to safeguard consumer's data integrity and privacy, the security of infrastructural facilities and IoT devices, and the accessibility of services supplied by an IoT ecosystem. The paper discusses various IoT security issues and remedies. The IoT feature varies from one organization to another based on its requirements. Aside from security, interoperability has to be facilitated as a result of the diversity of IoT standards. As a result, all IoT users must guarantee that all security problems are addressed.

Key Words**:** IoT. Smart Home, smart phones, sensors, threats, attacks. Data integrity

1. INTRODUCTION

The Internet of Things (IoT) is one of the most active and fascinating innovations in information and communications technology. Despite network services have grown more widely used in recent years, such technological services were formerly limited to interconnect traditional end systems such as desktop computers, mainframes computers, and laptops, and, more recently, tablets and smartphones too.

The Internet of Things (IoT) is a global network of trillion of devices or things that access the internet and connect to one another via wireless medium. The internet of things, or IoT, is a network of interconnected computing devices, mechanical machines and digital systems, items, animals, and people with unique identities (UIDs) and has the potential to transmit data without the help of human-to-human or human-to-computer communication.

One of the most essential features of an IoT device is its capacity to connect to the internet and interact and react with its surroundings by retrieving and exchanging data. Most of the IoT devices are equipped with restricted computational power and just a few particular purposes. Because devices come in such a wide range of shapes and sizes, IoT may be utilised and used in a variety of environmental settings.

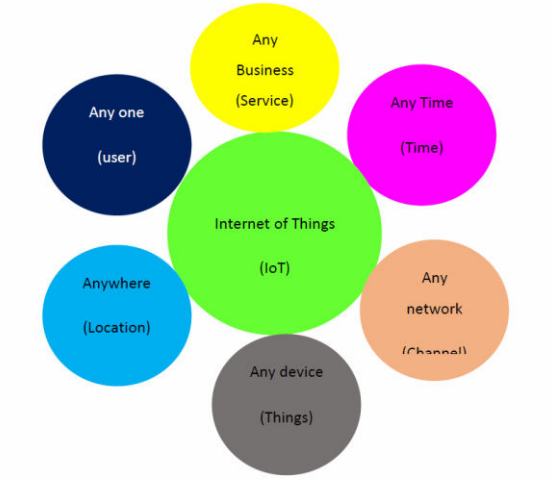


Fig- 1. Internet of Things

Smart homes show how easily IoT devices may be used by normal people. The individuals may modernise and upgrade their home's surveillance system by using smart locks, IP cameras, and motion sensors) or upgrade their entertainment system by using smart speakers, smart TVs, and linked gaming consoles by purchasing such specific items. IoT devices are typically movable and communicate to any available network. The users bring their gadgets like smart watches and e-readers from home to office is a good example of mobile IoT devices. Consumers have a huge variety of gadgets to choose from in the modern world, which is one of the causes for the IoT's dispersion .and most of its security problems. Interoperability difficulties have arisen as a result of the absence of industry vision and standardization, further complicating the security issue. Because of the mobility of devices, there is a larger risk of attacks infecting several networks.

Despite the fact that the phrase "Internet of Things" is new, many people are comfortable with the terms "smart homes" or "connected homes," which refer to the various IoT gadgets that make life easier and improve the lifestyle at home. IoT gadgets, on the other hand, may be located in and around the home. They can range from a Wi-Fi pet camera to an implanted pacemaker that can save a person's life. As long as an IoT device can access the internet, the sensors in IoT devices can t transfer data, to connected devices.

An individual with a cardiac monitor transplanted, a pet animal with a biochip transceiver, a motor vehicles with built-in sensors to warn the driver or any other natural or man-made thing that can be allotted an Internet Protocol (IP) address and can exchange data over the internet are all examples of things in the Internet of Things. IoT devices have sensors and computing processors that use machine learning to process the data obtained by the sensors. IoT gadgets are typically small computers that are interconnected to the internet and are susceptible to viruses and hacking threats.

An IoT ecosystem is made up of internet enabled smart devices that capture, send, and process the data from their surroundings using embedded systems such as CPUs, sensors, and different communication hardware devices. By connecting to an Access point or other end systems, IoT devices may exchange sensor data that is either transmitted to the cloud for the local processing. These gadgets may occasionally interact with each other and process the information they receive. Although individuals may engage with the devices to set them up, send commands, or retrieve data, the gadgets conduct the majority of work without human interaction.

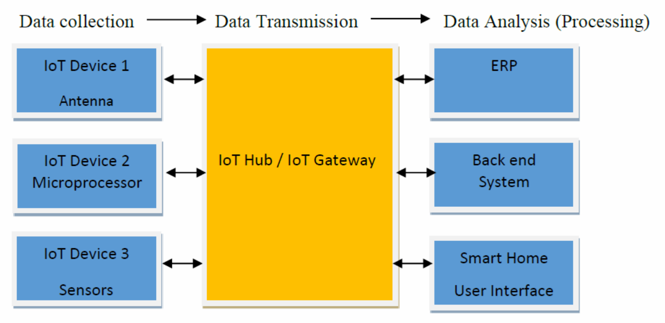


Fig-2. IoT Process

2. Significance of IoT

People may use the internet of things to work and live smartly and have total sense of control over their life. IoT is also important to business enterprises and also provide smart devices to control smarter homes. IoT gives organisations a true perspective of how their systems function, providing information on anything from machine performance to supply chain and logistical operations. Companies may use the Internet of Things to automate business operations and save money on manpower. It also reduces waste and enhances service delivery by lowering the cost of manufacturing and delivering items and providing openness to consumer transactions.

Organizations may profit from the internet of things in a variety of ways. Some advantages are business specific, while others are relevant to a variety of sectors. Businesses may use IoT to track and manage their whole business operations, boost up customer satisfaction, save energy and cost, increase staff performance, incorporate and customize business models, create better business choices, and create more revenue, among other things.

IoT drives organisations to evaluate how they do business and provides them with the tools to better their strategy. In general, IoT is prominent in transportation, manufacturing, , and service businesses, where sensors and other IoT devices also are used; but, it is used in different fields like infrastructure, agriculture, and smart home, leading certain businesses towards digital transformation.

Farmers may profit from the Internet of Things by making their work easier. Sensors can gather information on temperature, rainfall, humidity, and soil composition, among other things, to aid in the automation of farming operations.

The responsibility to track infrastructure operations is another area that IoT plays a vital role. Sensors might be used to track activities or variations in architectural constructions, bridges, and other infrastructures. In infrastructure operations, IoT facilitates a number of advantages, including cost reductions, savings in time, quality-of-life and reliable operational improvements.

IoT may be used by a smart home provider to regulate and manage electrical, electronic and mechanical systems in a building. Smart cities can help residents to cut down the usage of energy and waste on a larger scale. Every industry is affected by the Internet of Things, including manufacturing, healthcare, retail and banking sector

3. Security Concerns in IoT

. The Internet of Things can provide significant benefits to businesses (IoT). However, as the IoT ecosystem becomes more sophisticated, security vulnerabilities will rise from the edge to the cloud. Unfortunately, many businesses continue to delay implementing an IoT security strategy, failing to recognise IoT security threats until it is too late. The most significant problem with IoT is security. Industrial, corporate, consumer, or personal data might be used in IoT applications. Such application's information must be kept safe and protected against theft and manipulation. IoT applications may keep a record of a patient's health or shopping store. The Internet of Things improves device connectivity, but there are still difficulties with scaling, accessibility, and reaction time. When data is sent over the internet, security is a problem. While transmitting the data across country boundaries, governmental safety measure act such as the Health Insurance Portability and Accountability Act (HIPAA) may be imposed. The most critical security concerns related to IoT are highlighted among various security challenges.

Getting comprehensive knowledge of IoT security concerns and working on a plan to mitigate the risks can assist to protect the business and boost trust in digitalization efforts. The trustworthiness of digital data is based on six key IoT security issues:

- Password security is insufficient
- Updates are infrequent, and the updates are unreliable.
- Interfaces that are insecure
- Inadequate data security
- IoT device management is insufficient.
- IoT skills and training are in short supply.

The number of IoT applications is growing every day, indicating that the technology will have a bigger influence on our lives in the future. IoT unsurprisingly comes with risks like any other technology. The level of concern in IoT, on the other hand, is considerably higher since these devices have the capacity to do physical harm, damage people, and cause systemic failures. Many additional components have been added to the IoT technological stack notably IoT protocols, sensors, gateways, and administration platforms. In particular, standard web programs and cloud platforms are used in the backend services of IoT infrastructure. There are three serious problems to detecting threats across these components:

IoT devices are placed in the thousands at various places, and security agents cannot supervise each device with individual attention. So it becomes so essential to supervise real time traffic information at the gateway or network level, which necessitates huge data processing. Zigbee, Digital Data Service (DDS), CoAP, Message Queue Telemetry Transport (MQTT), and Advanced Message Queuing Protocol (AMQP), are just a few of the IoT technologies available today. These protocols are either brand new or have been adapted for IoT from a previous version that was employed for other reasons. To identify dangers in these protocols, there are only a few recognised regulations or signatures. As a result, rather than a rule-based monitoring system, it becomes so essential for the additional anomaly identification, pattern matching, outlier, and abnormal identification technologies. IoT management solutions, on the other hand, are cloud-based and web interfaces. They are vulnerable to online usage and cloud infrastructure threats. Some of issues that can arise and weaken the security of IoT are as follows:

1) Data Privacy: Because some smart TV makers collect information about consumers in order to evaluate their watching habits, the data acquired by smart TVs may pose a data privacy problem during transmission.

2) Data Security: Data security is another major issue. It is critical to remain hidden from listening devices on the internet while transferring data in a smooth manner.

3) Concerns regarding insurance: Insurance providers deploy IoT devices on automobiles acquire data on the driver's health and driving habits in favour of making insurance decisions.

4) Lack of Universal Platform: There are a variety of standards for IoT devices and the IoT manufacturing sector. As a result, distinguishing between internet-connected gadgets that are authorised and those that are not is difficult.

5) Technical Issues: As the number of IoT devices grows, so does the amount of traffic generated by them. As a result, there is a need to expand network capacity, and storing the massive amounts of data for analysis and final storage is also a real challenge.

In case of IoT security, a great deal of effort has been performed so far. System Security measures, application security measure, and network security measure are the three major categories of the security to be considered in IoT.

a) System Security: System security emphasizes on the whole IoT system to recognise distinct security vulnerabilities, develop different security frameworks, and give adequate security measure in order to keep a network secure.

b) Application security: Application security is used to manage security concerns in IoT applications based on situation needs.

c) Network security is concerned with protecting the IoT communication network for the exchange of data between various IoT devices.

The IoT is vulnerable to a variety of assaults, including active and passive attacks, which may quickly destroy its operation and make its services useless. An attacker in a passive attack steals the information, but it never assaults the information physically. Active assaults, on the other hand, physically disrupt the operation. The active attacks are further divided into two classifications: internal attacks and external attacks. Such susceptible attacks can make it impossible for machines to interact intelligently. As a result, security limitations must be implemented to avoid malicious assaults on devices.

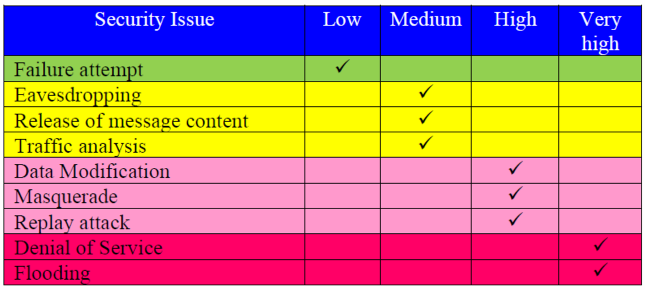
The attacks, their nature/behaviour, and the degree of danger of such attacks are to be considered for executing security measure of IoT. Various levels of threats are classified into four kinds based on their behaviour, and remedies to threats/attacks are proposed.

1) A low-level attack occurs when an attacker attempts to assault a network but fails.

2) A medium-level attack occurs when an assaulter or eavesdropper just listens to the channel without altering data integrity.

3) An assault happens on a network that compromises data integrity or changes data is referred to as a High-level attack.

4) Extremely High-Level Attack occurs when an intruder or attacker gains unauthorized access to a network and uses it to carry out an unlawful action, such as keeping the network inaccessible by overloading the network through sending bulk of spam messages.



Security Issue	Low	Medium	High	Very high
Failure attempt	✓			
Eavesdropping		✓		
Release of message content		✓		
Traffic analysis		✓		
Data Modification			✓	
Masquerade			✓	
Replay attack			✓	
Denial of Service				✓
Flooding				✓

Table 1. Types of Attacks and Level of threat

4. Security models – A comparative study

The security measure in IoT is performed using the security metrics such as Confidentiality, Integrity, Trust, Authentication and Availability (CITA1A2).

- Confidentiality is basically comparable to "privacy." Confidentiality mechanisms are in place to protect sensitive data from unapproved access. Data is frequently classified according to the quantity and those classifications can then be used to impose more or less rigorous restrictions.
- Data integrity refers to the consistency, correctness, and reliability of data throughout its lifespan. It should not be altered during transmission, and efforts must be followed to guarantee that unauthorised persons cannot modify data.
- Availability ensures that authorised parties should have constant and easy access to information. Availability ensures keeping the hardware, technological infrastructure, and systems that store and show the data in good working order.
- Authentication is a critical component of identity verification, since it verifies credentials and grants the appropriate degree of access. Identity verification includes a variety of features, including identity lifecycle monitoring, authentication and authorization and validation.
- Trust is the amount of confidence that an entity can guarantee to others for unique services in a given environment. Trust is normally applied to individuals, but it can also be applied to a device or a system which highlights

the significance of assessing the amount of trust in a digital community.

Xin Zhang and Fengtong Wen (2019) suggested the three-part authentication model that undergoes four phases of authentication such as re-deployment phase, registration phase, login and authentication phase, and password-change phase. The proposed authentication model satisfies authentication and trust, but falls short in terms of Confidentiality Integrity and Availability requirements, making it vulnerable to DDoS attacks as well as tracking.

Pooja Shree Singh and Vineet Khanna (2019) offered a security solution that uses MFCC security coefficients to meet confidentiality and integrity security needs. However, the approach falls short in terms of achieving availability, trust, and authentication.

Confidentiality and Trust security criteria are met by a Trust-based security Model proposed by Mohammad Dahman Alshehri and Farookh Khadeer Hussain (2019). A trust solution should be flexible enough to adjust to variations in network size. A cluster-based fuzzy-logic solution is presented to handle the crucial problem, in which connected devices are organised into clusters. In order to allow dependable cluster-based trust management in IoT, a unique technique is presented to overcome the essential challenges. But the model fails to satisfy Availability, Integrity, and Authentication requirements.

Chifor et al.(2016) suggested another security architecture in which social networks ser serve an adaptive sensing system . The system proposes a framework for autonomic computing, in which smart gadgets' reputation is measured based on input from humans and other connected devices. All devices that have participated to the transmission of valid information are given a certain amount of trust.

Hongsong Chen et al. (2019) proposed a model in which the non-stationary tiny signal produced by the LDoS assault is analysed using a Hilbert–Huang transform (HHT) time–frequency joint analysis method. False intrinsic mode function (IMF) components, on the other hand, provide a significant barrier in accurately detecting an LDoS assault. The correlation coefficient and the Kolmogorov–Smirnov (KS) test are combined to assess the reliability of IMF components. Hilbert-Huang transformation satisfies the availability and trust security criteria but the model can be compromised in the Confidentiality, Integrity, and Authentication security parameters.

Security Model	C	I	T	A_1	A_2
Three part Authentication model			✓	✓	
Fuzzy logic security Model	✓		✓		
Security Model using MFCC	✓	✓			
Hilbert-Huang transformation Security model			✓		✓
Reputation based security model	✓		✓		
Data Encryption model			✓	✓	

Table 2. Security Table

For accessing and operating the IoT infrastructure, specific regulations and permissions must be followed. Policies are made up of a collection of rules to regulate the access and operations. The policies are made up of a condition and an action (allow/deny). Access control policies can allow or disallow outgoing/incoming traffic, as well as the system's access requests. Anti-virus, anti-adware, and anti-spyware should all be deployed immediately to maintain the security, consistency, secrecy, and dependability of the IoT domain. Risk assessment approaches helps to uncover vulnerabilities to the IoT system, therefore risk assessment should be used to safeguard the IoT applications. The firmware of the system devices have to be upgraded to strengthen security measures. The information exchanged between two nodes should be secure and reliable. To secure the privacy, data integrity, and accessibility of the IoT domain, cryptographic methods such as hash-based encryption and PKI-based encryptions must be deployed. The algorithms also aid in the authentication of authorised users, limiting unauthorised access. The authentication procedure ensures that the data received is genuine and trustworthy. By incorporating these factors, IoT will emerge as secured smart domain for all use cases.

5. CONCLUSIONS

The Internet of Things (IoT) is a new digital revolution that leverages the internet to enable a networking infrastructure made up of a large number of devices to gather data and communicate with one another in order to make processed, intelligent decisions. The Internet of Things (IoT) has emerged as a significant technological advancement in which data sent by sensor may include confidential material that must be protected from unauthorised access. Because IoT connection between pair of nodes is unsecure, IoT security procedures should not be compromised. For critical infrastructure, IoT must incorporate security services such as Cryptography for end-to-end communication and access control protection. Better security for smart devices, as well as higher privacy requirements for IoT connection, are predicted in the future, allowing users safely carry out activities. Various security models are compared in terms of security parameters like confidentiality, integrity, trust, authentication and availability. Better privacy, data security, and ethical standards in IoT will definitely increase consumer trust and provide businesses a competitive edge in the digital market.

REFERENCES

1. Abdul-Ghani Hezam A, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. International Journal of Advanced Computer Science Applications 9:355–373
2. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M (2020) Internet of Things (IoT) enabling technologies, requirements, and security challenges. Advances in data and information sciences. Springer, Singapore, pp 119–126
3. Alshehri MD, Hussain FK (2019) A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101(7):791–818
4. Bhattacharjya A, Zhong X, Wang J, and Li X (2019) Security challenges and concerns of Internet of Things (IoT). In: Cyber-Physical Systems: architecture, security and application, Springer, Cham, pp 153–185
5. Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G (2017) Security and attack vector analysis of IoT devices. In: International Conference on Security, Privacy and Anonymity in Computation, Communication

6. Chen H, Meng C, Shan Z, Zhongchuan Fu, Bhargava BK (2019) A Novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang transformation and trust evaluation. IEEE Access 7:32853–32866
7. Chifor, B.-C., Bica, I., Patriciu, V.-V.: Sensing service architecture for smart cities using social network platforms. Soft Comput. 1–10 (2016)
8. Coman FL, Malarski KM, Petersen MN, Ruepp S (2019) Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In: 2019 Global IoT Summit (GIoTS), IEEE, pp 1–6
9. Jaiswal S, D Gupta (2017) Security requirements for internet of things (IoT). In: Proceedings of International Conference on Communication and Networks, Springer, Singapore, pp 419–427
10. Li Y, Chen M (2015) Software-defined network function virtualization: a survey. IEEE Access 3:2542–2553
11. Mukhandi M, David P, Pereira S, and MS Couceiro (2019) A novel solution for securing robot communications based on the MQTT protocol and ROS. In: IEEE/SICE International Symposium on System Integration (SII), pp 608–613
12. Radanliev P, De Roure DC, Nurse JRC, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C (2020) Future developments in standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci 2(2):169
13. Rutten E, Marchand N, Simon D (2017) Feedback control as MAPE-K loop in autonomic computing. Software engineering for self-adaptive systems III Assurances. Springer, Cham, pp 349–373
14. Safkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. Journal of Supercomputer 73(8):3579–3585
15. Sharma K, Bhatt S (2019) SQL injection attacks-a systematic review. International Journal Computer Security 11(4–5):493–509
16. Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH (2019) Ultralightweight mutual authentication RFID protocol for block chain enabled supply chains. IEEE Access 7:7273–7285
17. Singh P S, and V Khanna (2019) A MFCC based Novel approach of User Authentication in IOT. In: 2nd International Conference on Emerging Trends in Engineering and Applied Science, ISSN: 2454-4248, 5(1)
18. Sood K, Shui Yu, Xiang Y (2016) Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet Things J 3(4):453–463
19. Urla PA, Mohan G, Tyagi S, Pai SN (2019) A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, Singapore, pp 251–259
20. Wang Li, Dinghao Wu (2019) Bridging the gap between security tools and SDN controllers. ICST Transaction on Security Saf 5(17):156242
21. Zhang X, Wen F (2019) An novel anonymous user WSN authentication for Internet of Things. Soft Computer 23(14):5683–5691.