An Overview Internet of Things in Vulnerabilities, Threats, Intruders and Attacks

Dr. Aniket Kumar, Dr. Neha Singh, Mr. Hamid Ali
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- aniket.kumar@shobhituniversity.ac.in, drnnehasingh@gmail.com, hamid.ali@shobhituniversity.ac.in

ABSTRACT: ***Internet of Things (IoT) devices are growing more common, and IoT services are becoming more widespread. Their success hasn't gone unnoticed, and the amount of threats and assaults targeting IoT devices and services is also on the rise. Cyber-attacks are nothing new in the IoT world, but as the IoT becomes more deeply ingrained in our lives and society, it will be essential to step up and take cyber security seriously. As a consequence, there is a pressing need to protect IoT, which necessitates a thorough understanding of the risks and attacks against IoT infrastructure. This article aims to identify threat categories as well as evaluate and describe intrusions and assaults that affect IoT devices and services. The Internet of Things (IoT) is a buzzword with major technical, social, and economic ramifications. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other commonplace objects are being connected to the Internet and equipped with sophisticated data processing capabilities to transform how we work, live, and play. According to some estimations, the impact of IoT on the Internet and economy by 2025 may be as high as 100 billion connected IoT devices and a global economic impact of more than $11 trillion.***

KEYWORDS: ***Exposure, Internet of things, Threats, Security, Vulnerability.***

1. INTRODUCTION

The Internet of Things (IoT) has become the fastest developing technology, with a significant effect on social life and corporate settings, thanks to its capacity to provide many kinds of services. The Internet of Things (IoT) has progressively pervaded many areas of contemporary human life, including education, healthcare, and business, including the storing of sensitive information about people and businesses, financial data exchanges, product creation, and marketing. In response to the increasing need for millions, if not billions, of linked devices and services across the globe, the IoT has generated a tremendous demand for strong security [1]. The number of threats is increasing every day, and assaults are becoming more numerous and sophisticated. Not only is the number of possible attackers increasing in tandem with the growth of networks, but the tools accessible to them are also improving in sophistication, efficiency, and effectiveness. As a result, in order for IoT to reach its full potential, it must be protected against attacks and vulnerabilities. Security has been described as a procedure that protects an item from physical damage, illegal access, theft, or loss by preserving high confidentiality and integrity of the object's information and making that information accessible whenever required [2].

According to Kizza, there is no such thing as a secure state of any item, physical or intangible, since no object can ever be completely safe while still being useful. When a process can retain its maximal inherent value under a variety of circumstances, it is said to be secure. The security standards for IoT systems are the same as for any other ICT system. As a result, securing IoT security necessitates preserving the greatest intrinsic value of both physical and intangible things (devices) (services, information and data). The Internet of Things (IoT) is an extension of the Internet into the real world that allows users to interact with actual objects in their environment [3]. Entities, devices, and services are important concepts in the IoT domain. Various projects have distinct definitions and meanings for them. As a result, a thorough knowledge of IoT entities, devices, and services [4].A person, animal, vehicle, logistic chain item, electronic device, or closed or open environment may all be considered entities in the IoT. Hardware components known as devices, such as mobile phones, sensors, actuators, or RFID tags, enable things to interact with one another by allowing them to connect to the digital world. Machine-to-Machine (M2M) is the most common IoT application at the moment. M2M is currently extensively used in sectors such as electricity, transportation,

retail, public service management, health, water, oil, and others to monitor and regulate users, equipment, and production processes. M2M apps are expected to surpass 12 billion connections and produce 714 billion euros in revenue by 2020, according to projections [5].

1.1 IoT device

This is a piece of hardware that enables the creature to interact with the digital world. A smart thing can be a home appliance, healthcare device, vehicle, building, factory, or almost anything networked and fitted with sensors providing information about the physical environment (e.g., temperature, humidity, presence detectors, and pollution), actuators (e.g., light switches, displays, motor-assisted shutters, or any other action that a device can perform), and software. A gadget that is part of the Internet of Things may communicate with other IoT devices and ICT systems. Cellular (3G or LTE), WLAN, wireless, and other technologies are used to connect between these devices. The size, i.e., small or normal; mobility, i.e., mobile or fixed; external or internal power source; whether they are connected intermittently or always-on; automated or non-automated; logical or physical objects; and, finally, whether they are IP-enabled objects or non-IP objects determine IoT device classification [6]. The ability to actuate and/or detect, the ability to restrict power/energy, connection to the real environment, intermittent connectivity, and mobility are all features of IoT device. Others may not need to be quick and dependable, or offer genuine security and privacy. Some of these gadgets are protected physically, while others are left unattended. In reality, devices in IoT settings should be secured from any attacks that may compromise their functioning. However, because of their features, most IoT devices are susceptible to both external and internal assaults. Due to resource limitations in terms of IoT computing capabilities, memory, and battery capacity, implementing and using a robust security mechanism is difficult [7].

1.2 IoT services:

IoT services make it simple to integrate IoT things into the realm of web services architecture (SOA) and service science. An IoT service, according to Thoma, is a transaction between two parties: the service provider and the service user. It performs a predetermined function, allowing contact with the physical world by measuring the status of things or starting activities that cause the entities to change. A service is a well-defined and standardized interface that includes all of the essential capabilities for communicating with entities and processes. By accessing a device's hosted resources, the services reveal the device's capabilities [8].

1.3 Security in IoT devices and services:

Protecting both IoT devices and services against unwanted access from inside and outside the devices is part of ensuring security. Both in transit and storage, security should safeguard services, physical resources, information, and data. We found three major issues with IoT devices and services in this section: data confidentiality, privacy, and trust. In IoT devices and services, data confidentiality is a major concern [9]. In the framework of the Internet of Things, not only users but also approved objects have access to data. This necessitates addressing two critical aspects: first, a system for access control and authorization, and second, a mechanism for authentication and identity management (IdM). The IoT device must be able to confirm that the entity (human or other device) attempting to access the service is allowed to do so. Authorization determines whether a person or device is allowed to receive a service after identification. Access control refers to the process of giving or restricting access to resources based on a variety of criteria. Establishing a secure connection between a variety of devices and services requires authorization and access control. Making access control rules simpler to develop, understand, and modify is the primary problem to be addressed in this situation. Authentication and identity management are two additional aspects to consider when dealing with secrecy [10].

With reality, in the Internet of Things, this problem is important since many people, objects/things, and devices must authenticate each other via trusted services. The issue is to develop a safe way to handle the

identification of users, things/objects, and devices. Because of the pervasive nature of the IoT ecosystem, privacy is a major concern with IoT devices and services. Because entities are linked and data is transmitted and transferred via the internet, user privacy has become a sensitive topic in many study studies. Privacy in data collecting, data sharing and management, and data security are all outstanding research questions that need to be addressed. When a lot of objects interact in an unpredictable IoT context, trust plays an essential role in creating secure communication. In the Internet of Things, there are two types of trust to consider: trust in the interactions between entities and confidence in the system from the users' viewpoint. The trustworthiness of an IoT device, according to Kien, is determined by the device components, which include hardware such as processors, memory, sensors, and actuators, software resources such as hardware-based software, operating systems, drivers, and applications, and the power supply. In a dynamic and collaborative IoT context, there should be an effective method for defining trust in order to acquire user/services confidence.

1.4 Security Threats, Attacks, and Vulnerabilities in IoT:

- *Vulnerability* : Vulnerabilities are flaws in a system's architecture that enable an intruder to run commands, get access to unauthorized data, and/or launch denial-of-service attacks. In IoT systems, vulnerabilities may be discovered in a number of places. They may include flaws in system hardware or software, as well as flaws in system rules and processes, as well as flaws in the system users themselves. IoT systems are made up of two major components: system hardware and system software, both of which are prone to design errors. Hardware vulnerabilities are difficult to find and repair, even when they are found, owing to hardware compatibility and interoperability, as well as the time and effort required to address them. Operating systems, application software, and control software, such as communication protocols and device drivers, all have software vulnerabilities. Program design errors are caused by a variety of reasons, including human factors and software complexity. Human flaws are typically the source of technical vulnerabilities. Starting the project without a strategy, poor communication between developers and users, a lack of resources, skills, and expertise, and failing to manage and control the system are all consequences of not understanding the requirements.
- *Exposure* : An attacker may perform information collecting operations due to a flaw or error in the system setup. Resiliency against physical assaults is one of the most difficult problems in the IoT. In most IoT applications, devices are likely to be left unattended and located in areas that are readily accessible to attackers. As a result of this vulnerability, an attacker may be able to seize the device, extract cryptographic secrets, change its code, or replace it with a hostile device under the attacker's control.
- *Threats*: A threat is an activity that exploits a system's security flaws and has a negative effect on it . Humans and environment are the two main sources of threats. Natural disasters like earthquakes, hurricanes, floods, and fires may all cause significant damage to computer systems. Natural catastrophes are difficult to avoid, and no one can guarantee that they will not occur. Backup and contingency plans, as well as disaster recovery plans, are the greatest ways to protect systems against natural disasters. Malicious threats, such as internal (someone has allowed access) or external (individuals or groups operating outside the network) seeking to damage and disrupt a system, are examples of human threats.
- *Attacks*: Attacks are attempts to damage a system or interrupt regular operations by using different methods and tools to exploit vulnerabilities. Attackers carry out assaults for a variety of reasons, including personal pleasure or monetary gain. Attack cost is an assessment of an attacker's effort stated in terms of their skill, resources, and motivation. People who pose a danger to the digital realm are known as attack actors. Hackers, criminals, or even governments may be involved. Delves further into the subject. Active network assaults, such as monitoring unencrypted traffic in search of sensitive information; passive network communications monitoring to decode poorly encrypted

traffic and get user credentials; close-in attacks; insider exploitation, and so on are all examples of attacks.

1.5 Primary security goals of IoT:

- *Maintaining Confidentiality*; Although confidentiality is an essential security element in the Internet of Things, it may not be required in certain situations when data is shown publicly. However, sensitive data must not be shared or accessed by unauthorized individuals in the majority of circumstances and scenarios. Patient information, confidential corporate information, and/or military information, as well as security credentials and secret keys, must all be kept private from unauthorized parties.
- *Reliability*: In most instances, integrity is a required security characteristic to offer dependable services to IoT consumers. Different IoT systems have different integrity requirements. For example, owing to information sensitivities, a remote patient monitoring system will include strong integrity checking against random mistakes. Communication may result in data loss or manipulation, which can result in human lives being lost.
- *Authentication and authorization*: Because of the nature of IoT settings, where potential communication may take place from device to device (M2M), human to device, and/or human to human, ubiquitous connectivity of the IoT exacerbates the issue of authentication. Various authentication needs demand various solutions in various systems. Some solutions, such as verification of bank cards or bank systems, must be robust. However, most will need to be worldwide, such as Passport, while others will need to be local [6]. Only authorized entities (any authenticated entity) are allowed to execute specific network activities using the authorization property.
- *Accessibility*: A device's user (or the device itself) must be able to access services at any time and in any location. Different hardware and software components of IoT devices must be resilient in order to deliver services even when hostile entities or unfavorable circumstances are present. Various systems have different needs for availability. For example, roadside pollution sensors would most likely have greater availability needs than fire or healthcare monitoring systems.
- *Responsibility*: Accountability provides redundancy and responsibility to specific activities, responsibilities, and planning of the execution of network security rules while creating security methods to be utilized in a secure network. Accountability cannot prevent attacks on its own, but it may assist ensure that other security measures are functioning correctly. Integrity and secrecy, for example, may be rendered worthless if they are not subjected to accountability. Also, in the event of a repudiation issue, an entity's activities would be tracked via an accountability procedure, which may be helpful for determining the inside story of what occurred and who was really accountable.
- *Internal Auditing*: A security audit is a methodical assessment of a device's or service's security by determining how well it complies with a set of predetermined criteria. Because most systems include many faults and vulnerabilities, security auditing is critical in identifying any exploitable flaws that put data at risk. In the Internet of Things, the requirement for auditing is determined by the application and its value.
- *Non-repudiation*: When a user or device cannot refute an activity, the characteristic of non-repudiation generates definite proof. For the most part, non-repudiation is not regarded a critical security characteristic in IoT. It may be appropriate in certain situations, such as payment systems where consumers or suppliers cannot refuse a payment action.

2. DISCUSSION

The exponential development of the Internet of Things has resulted in increased security and privacy concerns. Many of these dangers are caused by device vulnerabilities caused by cybercrime and poor use of system resources. The Internet of Things must be designed in such a manner that it can be controlled easily

and safely. Consumers must have faith in the IoT in order to reap its advantages while avoiding security and privacy concerns. As previously said, the majority of IoT devices and services are vulnerable to a variety of typical threats, such as viruses and denial-of-service assaults. Simple measures to prevent such risks and address system vulnerabilities are insufficient; instead, a seamless policy implementation process backed by robust processes is required. The security development process requires a comprehensive knowledge of a system's assets, as well as the identification of potential vulnerabilities and threats. It's crucial to figure out what the system's assets are and how they should be safeguarded. Assets were described in this article as all valuable items in the system, both physical and intangible, that needed to be protected. System hardware, software, data, and information, as well as assets linked to services, such as service reputation, are examples of generic IoT assets. It has been shown that understanding threats and system vulnerabilities is critical for improved system mitigation. Furthermore, having a greater knowledge of possible threats enables system engineers to make better decisions about where money should be invested. DoS assaults, physical attacks, and attacks on privacy are the most well-known dangers. Individual assaults, organized organizations, and intelligence agencies were the three kinds of invaders addressed in this article. Each kind of attacker has a distinct degree of expertise, money, motivation, and risk tolerance.

It's critical to research the many kinds of attack actors and figure out which ones are most likely to assault a system. It's simpler to see which threat may exploit which system vulnerability after describing and documenting all threats and their associated actors. In general, an IoT intruder is considered to have full DY intruder skills as well as some physical compromise power. We'll assume that physical compromise attacks don't scale, and that they'll only impact a small percentage of the total number of IoT devices at worst. As a result, IoT architecture must be capable of dealing with hacked devices and identifying such events. To accomplish their aims or objectives, attackers use a variety of methods, tools, and strategies to exploit vulnerabilities in a system. To avoid possible harm, an organization must first understand the motivations and capabilities of the attackers. More research is required to address the gaps in information about threats and cybercrime, as well as offer the essential measures to prevent such assaults, in order to minimize both prospective threats and their effects.

3. CONCLUSION

The Internet of Things is vulnerable to a variety of dangers that must be identified before preventive measures may be implemented. Security issues and dangers to IoT were discussed in this study. The main objective was to identify assets as well as describe possible threats, assaults, and weaknesses that the Internet of Things could encounter. An overview of the most pressing IoT security issues was presented, with an emphasis on security issues relating to IoT devices and services. Confidentiality, privacy, and entity trust were highlighted as security issues. We demonstrated that security and privacy issues must be addressed in order to create more safe and widely accessible IoT devices and services. The debate also focused on cyber threats, which include actors, motive, and capacity, all of which are fueled by cyberspace's unique features. Attacks from intelligence agencies and criminal organizations have been shown to be more difficult to counter than threats from individual hackers. The rationale for this is because their targets are likely to be less predictable, and the effect of a single assault is likely to be less severe. It was determined that both manufacturers and end-users still have a lot of work to do in the area of IoT security. It is critical that future standards address the flaws in existing IoT security methods. The goal of future research is to acquire a better knowledge of the risks to IoT infrastructure, as well as to determine the probability and effects of such attacks. Early in the product development process, definitions of appropriate security methods for access control, authentication, identity management, and a flexible trust management framework should be addressed. We believe that by identifying the main problems in IoT security and giving a better knowledge of the risks and their characteristics coming from different invaders such as companies and intelligence agencies, this study would be helpful to security experts.

REFERENCES

[1] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2016.2615180.

[2] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal*. 2016, doi: 10.1109/JIOT.2016.2584538.

[3] S. S. Joshi and K. R. Kulkarni, "Internet of Things: An Overview," *IOSR J. Comput. Eng.*, 2016, doi: 10.9790/0661-180405117121.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2015.2444095.

[5] A. Abdul Qawy, E. Magesh, and S. Tadisetty, "The Internet of Things (IoT): An Overview," *Int. J. Eng. Res. Appl.*, 2015.

[6] S. S. Pai, Vikhyath, Shivani, Sanket, and Shruti, "IOT Application in Education," *Int. J. Adv. Res. Dev.*, 2017.

[7] International Telecommunication Union, "Overview of the Internet of things," *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model.*, 2012.

[8] D. M. Hartley *et al.*, "An overview of internet biosurveillance," *Clinical Microbiology and Infection*. 2013, doi: 10.1111/1469-0691.12273.

[9] M. M. Spada, "An overview of problematic Internet use," *Addictive Behaviors*. 2014, doi: 10.1016/j.addbeh.2013.09.007.

[10] W. J. Drake, V. G. Cerf, and W. Kleinwachter, "Internet Fragmentation: An Overview," *Futur. Internet Initiat. White Pap.*, 2016.