International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 2379-2384 www.ijaem.net ISSN: 2395-5252

Security and Privacy Concerns with IoT

S.Punithavathi

Assistant Professor,Department of Computer Science,
Hindustan College of arts and Science, Chennai.

Submitted: 20-05-2022 Revised: 28-05-2022 Accepted: 30-05-2022

ABSTRACT: The Internet of Things (IoT) is the technology of the future, in which items may communicate with one another and connect to the internet to form self-configuring, intelligent systems. Aside from the benefits of IoT development, there is still a lot of uncertainty concerning security and privacy, which are seen as important difficulties in the adaptation and development of IoT design. The most pressing challenge in each IoT layer is security and privacy, which has yet to be properly solved. Many research have proposed security-related solutions. Protecting IoT necessitates a security framework that addresses all IoT layer-security concerns. This presentation examines the security and privacy risks and challenges in the Internet of Things. It also discussed security concerns in the IoT context and some potential solutions.

KEYWORDS: IoT architecture; security; privacy; Internet of Things (IoT).

I. INTRODUCTION

The Internet of Things (IoT) is a network of interconnected items (nodes) that may communicate and share data to complete common functions. People, cell phones, home appliances, doors, automobiles, animals, and everything else you can think of are examples of objects. Each object is equipped with a sensor that allows it to communicate with its surroundings. The Internet of Things connects personal, business, industrial, and public-sector devices so that data can be sorted, evaluated, and stored. Transportation, healthcare, energy generation, and distribution are just few of the areas where it can be used. "Global infrastructure for society, enabling sophisticated services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies," according to the International Telecommunication Union. [1]. IoT is a new Internet revolution that will alter our daily lives. It enables intelligent devices to carry out our daily chores.Almost every object in our environment will link to the internet in the future to communicate. IoT has given rise to new terms like smart home, smart office, smart car, and smart city. According to Gartner [2,] the number of IoT linked devices will rise to more than 50 billion by 2020, from around 25 billion now. This large network with a diverse nature introduces additional security challenges and hazards, increasing the targeted surface and allowing attackers to access more personal data from the IoT network, making the attack process easier. No defined rules or standards govern how IoT nodes communicate with one another or connect to the internet. Many security and privacy concerns arise as a result. At the same time, its enormous size and diverse nature present additional obstacles for potential solutions. The purpose of this study is to examine the security and privacy concerns raised by the Internet of Things. In this study, we used a systematic literature review to examine a number of current studies on IoT security and privacy issues. The review included publications from the Saudi Digital Library, Google Scholar, and the IEEE library that were found using the keywords: internet of things difficulties, IoT issues, IoT security issues, IoT security solutions, and IoT security and privacy. The following section presents an overview of IoT security at each architecture layer, followed by a brief introduction to the concept of IoT and its architecture in section 3. Section 4 discusses IoT security requirements, problems, and some possible solutions to these issues. Section 5 begins with an overview of the privacy issue in the Internet of Things, followed by a debate and conclusion..

II. IOT OVERVIEW

A. Evolution

The term "Internet of Things" was coined by Kevin Ashton of Massachusetts Institute of Technology in 1999, and it quickly gained traction in the market, although it was limited in its use due to network performance issues [3]. Sristava claimed in 2011 that in addition to RFID, additional technologies such as near field communication (NFC) and QR codes can be used to tag items. IoT devices will number more than 50 billion by 2020 [2]. IoT is a new internet generation in which communication moves from machine-to-machine to machine-to-machine. It is a network of items that includes cell phones, doors, wearable devices, automobiles, televisions, and more. Every device has a sensor and technology such as radio frequency identification (RFID). The Internet of Things changes the communication model to an M2M model. IoT has changed the way we think about computing, business, health care, manufacturing, and our daily lives. The current industry goal is to "connect the disconnected," which means that every device in our environment will be able to communicate and connect. Many IoT devices, on the other hand, are easy targets for attackers due to their diverse nature and tremendous processing power. One of the biggest issues that the IoT growth faces is security [4]. According to a survey, 71% of respondents agree that security concerns have influenced users' decisions to purchase IoT equipment [5].

B. Architecture of the Internet of Things

The Internet of Things requires a flexible layered architecture since it connects numerous heterogeneous components.

Although there is no universal IoT design, the most basic IoT model comprises three layers: application, network, and perception. Each IoT layer has its own set of functions and technology, hence each layer has its own set of security concerns [6]. These are the layers:

1. Perception Layer

The "sensors layer" is the name for this layer. This layer locates, collects, and processes data before sending it to the network layer.

It also displays IoT node collaboration in short-range networks and represents a sensor network. Radio Frequency Identification (RFID) technologies, GPS, and sensors are primarily used [7].

2. Network Layer

This layer is responsible for data routing or forwarding to various hubs via IoT and the Internet. The network layer includes switches, cloud computing platforms, routers, and internet gateways. It makes use of 2G/3G, Satellite Access, LTE, WIFI, Bluetooth, and ZigBee, among other technologies. At this layer, gateways collect, filter, and send data between sensors, acting as an interface between nodes [7].

3. Application Layer

At this layer, the aim of IoT is clearly realised by providing a variety of smart environment applications. IoT applications include smart homes, smart offices, smart cities, and smart transportation, among others. IoT offers personal applications like smart wearable device apps or mobile apps, as well as industrial ones like autonomous car apps [7].

III. IOT SECURITY ISSUES

Security goals such as confidentiality, integrity, and availability apply to all systems, including IoT. IoT has numerous restrictions that make security a difficult task, such as the diverse nature of nodes with internet connectivity and fewer embedded security devices [8]. This section begins with an overview of security challenges at each IoT layer, followed by a discussion of IoT security requirements and threats, as well as some potential IoT security solutions.

A. Security Issues at each Layer

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

1. Perception Layer

Typically, IoT nodes are installed outside and operate in an environment that exposes them to physical threats as well as natural disasters. These factors made IoT nodes easy targets for physical attacks; for example, once an attacker has physical access to a device element, he can tamper with it. Furthermore, IoT devices are especially vulnerable to such attacks because they must be mobile in many applications. Furthermore, this layer typically comprises of RFID-enabled sensors and wireless sensor networks, both of which have numerous security issues such as data leakage, replay attacks, cloning attacks, and man-in-the-middle attacks. These nodes are also vulnerable to a variety of attacks due to their poor storage space and limited compute performance. The replay attack, for instance, can readily exploit the confidentiality of this layer by faking or repeating device information identification. A timing attack is one in which the attacker obtains the encryption key by examining the encryption time. Assailant nodes might generate malicious data in this layer, endangering data integrity and increasing the likelihood of a DoS assault. Encryption, stenography, access restriction, and authentication to authenticate sender identity can handle most security challenges at this tier [9].

2. Network Layer

Data eavesdropping, DoS attacks, unlawful access, destruction, viruses, and Man-in-the-Middle assaults are all common targets for this layer. Attackers can use traffic analysis and eavesdropping to compromise network security and privacy.

IoT remote access and data exchange protocols increase the likelihood of such assaults. To safeguard against any adversary, the key exchange process must be highly secure. Communication in an IoT setting raises additional security concerns not seen on the Internet. IoT communication is between machines, whereas traditional internet communication is between humans and machines. These machines do not communicate using traditional security methods and share a lot of sensitive data. Network attackers can utilise his IoT devices to get more information about users and use that information for illicit purposes [10]. Object and network security are critical in IoT. Current network protocols provide effective protection methods, but they do not address the heterogeneous character of the Internet of Things. Objects must be able to detect and respond to aberrant network activities that could compromise their security. This level of security can be achieved with the help of good protocols and software [4].

3. Application Layer

Due to a lack of standards for managing interaction and the application development process, there are numerous challenges with application security.

It's challenging to ensure identity and data protection in applications using different authentication systems. This layer is in charge of traffic control, making it vulnerable to DoS attacks. Furthermore, the large number of connected devices and generated data can cause overhead in data analysis programmes, affecting service availability. When creating IoT applications, the different user interactions as well as the amount of data that will be generated must be taken into account [4]

B. Security Requirements and Challenges in the Internet of Things

[4] [11] [12] [13] explore the main security requirements of the Internet of Things from several perspectives. Table 1 summarises the five basic needs for IoT security. Due to the constraints of IoT devices in terms of capacity and competence to deploy standard security solutions, meeting these needs is a big issue.

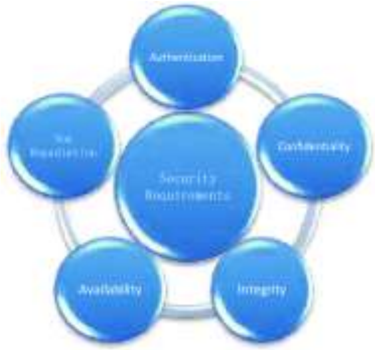

FIGURE I. INTERNET OF THINGS (IOT) SECURITY REQUIREMENTS

There are also additional problems to meeting IoT security needs, as described in [4], [11], [13], and [14], which are summarised as follows:

- **Date Volume: Despite the fact that most IoT applications use short communication channels, many IoT systems may require a substantial volume of data at the central network [4].**
- **Constraints in resources:** Because most IoT nodes have limited storage and processing capabilities, they typically have low-bandwidth communication channels, limiting the usage of some security solutions such the public key encryption algorithm [14].
- **Autonomic control: Nodes in the Internet of Things should be able to connect to one another and arrange themselves to adjust at the platform. As a result, it must include methods and procedures such as self-configuration, self-management, and self-healing. All of this automation necessitates greater control and security for IoT [13].**
- **Scalability**: IoT is made up of a large number of nodes that grows with time. As a result, its security system should be scalable [13].
- **Protection**: It is simple to monitor tags and identify things because most RFID systems have a weak authentication mechanism. Data will be read, modified, and potentially deleted by the intruder [14].

C. Some potential IoT security solutions

Some research have been conducted with the goal of improving IoT security and proposing solutions to security challenges. In [15], Tahir and colleagues presented the ICMetric framework for protecting IoT using cryptography keys. The ICMetric technology provides an extra layer of cryptographic algorithms to tackle key theft issues, which may then be utilised to prevent illegal access.

ICMetric technology is used in a healthcare setting to provide encryption that enables for the safe and secure usage of electronic devices, which is a critical necessity for IoT-based healthcare applications. Data saved on and exchanged between devices is likewise protected using ICMetric technology. In [16], Liu et al. developed an IoT security approach based on the biological immune system. The proposed method employs a dynamic defence framework for IoT security, where static security strategies may be ineffective. Security threat recognition, risk calculation, security reactions, security defence, and defence strategy formulation are the five linkages outlined in the circular defence.

The connection in the frame is linked to relative IoT security data. Researchers used an immunity-based antigen and a real IoT detector to imitate a real IoT platform. They are simulating the methods that biological systems utilise to recognise infections. Zhou and Chao [17] created and assessed a traffic management strategy for media-aware traffic and developed a security architecture for it. The media-aware traffic security architecture (MTSA) ensures that multimedia communication, computing, and IoT services are secure. Physically unclonable functions (PUFs) are an example of how security primitives and protocols for IoT devices are implemented, according to Rose [18]. He explained that the PUF has the potential to enable security advancements in the IoT context, such as robust authentication or secret key creation. Lessa dos Santos [19] build an architecture that allows IoT restricted devices to communicate with devices on the Internet using "Datagram Transport Layer Security (DTLS)" with authentication.

This IoT security architecture is built on a third-party device called the IoT Security Support Provider (IoTSSP), as well as two techniques for the 6LoWPAN Border Router (6LBR) to redirect DTLS handshaking to the IoTSSP. Zegzhda and Stepanova [20] present a method for improving IoT security by utilising topological sustainability to address security threats aimed at disrupting, degrading, or destroying any IoT components or services.

The goal is to maintain IoT security by preserving adaptive d-regular graph topology and taking into account various internet of things needs, such as limiting computation resources at IoT devices. For resource-constrained IoT devices, Raza [21] designed Scalable Security with Symmetric Keys, which introduces a highly scalable and flexible key management strategy for the DTLS security standard. Table 1 summarises the proposed solutions as well as the security requirement they addressed.

TABLE I. PROPOSED SOLUTIONS FOR IOT SECURITY

Author	**Methods for achieving Security main Requirements covered security**	**Main Security Requirements covered**			
		Confidentia lity	**Integrit y**	**Authenticat ion**	**Availabi lity**
Tahir et al. [15]	ICMetric coupled with CRRP	Yes	Yes	Yes	Yes
Liu et al. [16]	IoT dynamic security based on immune system principles	No	No	No	No
Zhou et al. [17]	Key management, watermarking	No	No	Yes	No
Lessa dos Santos [17]	ECC cryptography	Yes	Yes	Yes	Yes
Rose [18]	Nano-electronic security primitives	Yes	No	Yes	Yes
Zegzhda [20]	Graph topology	No	Yes	No	No
Raza et al. [21]	shared keys	Yes	Yes	Yes	Yes

IV. IOT SECURITY ISSUES

The Internet security glossary [22] defines privacy in the Internet of Things as "the right of an entity (normally a person) acting on its own behalf to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." In the Internet of Things, a network of devices attempts to collect data from the environment and then broadcasts it along with some events to a server with applications. Privacy must be managed across all of these processes, including in the device, storage, communication, and processing. One of the important challenges that needs to be addressed in IoT is privacy and the safeguarding of sensitive information [23].

A. Device Privacy

When unwanted access to hardware or software occurs in the IoT, sensitive data may be targeted. For example, an intruder who can re-program a camera to broadcast information to invaders as well as the authorised server. Many issues must be addressed to provide privacy in devices, such as device location privacy, which can be achieved using the Multi-Routing Random Walk Algorithm for Wireless Sensor Networks (WSN), protecting the identification of device nature by adding noise, and protecting sensitive information even in the event of device theft using the Quick Response Code technique [23].

B. Confidentiality During Communication

When data is transmitted through network channels, encryption techniques are routinely used to ensure data secrecy. In some circumstances, encryption adds data to packets to enable tracing capabilities. Security communication protocols may offer some privacy options. Pseudonyms can be used for encryption during communication, which can help to reduce susceptibility. To decrease privacy exposure during communication, devices should only communicate

when absolutely essential. In order to prevent location data from being tracked, devices must be able to detach from the network when it is inactive. Only approved devices are allowed to communicate, and once turned on, they must re-authenticate themselves to the network before dealing with any data [23].

B. Privacy in Storage

To safeguard the privacy of your data, keep only the necessary and vital data on hand. Only when there is a "need-to-know" is information sent. Anonymization could be used to hide the source of the data. Only statistical data should be available in a database. Differential privacy or the adding noise technique [23] can be used to assure output independence from other database records.

C. Privacy at Processing

Personal and sensitive data must be processed appropriately and solely for the purpose of processing. Before disclosing personal information to third parties, acceptance and data owner confirmation are required.

Digital Rights Management (DRM) system is an excellent approach for controlling data rights conveyed and defending against illicit processing.

To be successful, DRM relies on trusted and secure devices.

Before processing or even interacting with personal data, the permission and knowledge of the data owner must be sought. Notifying users helps to prevent the misuse of private data and sensitive information [23].

D. DISCUSSION

Issues of security and privacy have a huge impact on IoT adoption. The rising body of research in this field should meet the security and privacy needs at each layer and development point. The complexity of implementing security solutions is increasing as the number of linked heterogeneous nodes grows rapidly, and the majority of data in the IoT is sensitive and/or personal data. Because IoT is easy to hack at each layer, addressing security concerns is a major topic of research. Confidentiality, authorisation, authenticity, integrity, and availability are among the most important IoT security requirements. Security difficulties in the IoT, such as service quality, confidentiality and dependability, managing and securing massive data, software and hardware vulnerability, and developing applicable standards, are still open and unresolved [9].

IoT data privacy is dependent on authentication and identification, which is also a major security concern. However, it is frequently overlooked, despite the fact that it must be retained throughout the IoT. Protecting the Internet of Things necessitates suitable security frameworks that address all IoT layer-security concerns. More research is needed to create and design effective security solutions for IoT that take into account the devices' limitations. Furthermore, holistic security and privacy frameworks must be developed that address the highlighted issues at each tier and take into account influencing factors.

V. CONCLUSION

This paper gave a brief overview of the Internet of Things (IoT) and its three-layer architecture, examined the primary IoT security difficulties and needs, highlighted various proposed security solutions for IoT, and discussed IoT privacy issues. The adoption of IoT may be hampered by security and privacy concerns.

It is necessary to establish comprehensive security and privacy frameworks that take into account the problems of the IoT ecosystem as well as key influencing factors. Proposed security solutions should also take into account the resource constraints of IoT devices.

REFERENCES

[1]. Zhang, C.Liu and Z. H, "A Novel Approach to IoT Security Based on Immunology," in Ninth International Conference on Computational Intelligence and Security, 2013.

[2]. C. L. and Zhou, "Multimedia traffic security architecture for the internet of things," vol. 25, no. 3, pp. 35-40, 2011.

[3]. Rose, "Security meets nanoelectronics for Internet of things," in International Great Lakes Symposium on VLSI, 2016.

[4]. L. Santos, Guimarães, d. C. Rodrigues, Granville and Tarouco, "A DTLSbased security architecture for the Internet of Things," in IEEE Symposium on Computers and Communication, 2015.

[5]. Stepanova and Zegzhda, "Achieving Internet of Things security via providing topological sustainability," in Science and Information, London, 2015.

[6]. Raza, L.Seitz, D.Sitenkov and G.Selander, "S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the

Internet of Things," IEEE Transactions on Automation Science and Engineering, vol. 13, no.3, 2016.

[7]. "RFC 2828, Internet Security Glossary," May 2000. [Online]. Available:https://www.ietf.org/rfc/rfc2828.txt.

[8]. J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications ,vol.90, no. 11, 2014.

[9]. K.Zhao and LGeo, "A survey on the internet of things security," in Int'lConf. on Computational Intelligence and Security (CIS)," pp. 663-667, 2013.

[10]. H.Suo, Zou, W. J and J. C.Liu, "Security in the Internet of Things: A Review," IEEE International Conference on Computer Science and Electronics Engineering,, Vols. 648-651, pp. 23-25, March 2012.

[11]. "Wind River Systems Security in the Internet of Things," 2015. [Online]. Available: http://www.windriver.com/whitepapers/security-in-theinternet- of-things/wr_security-in-the-internet-of-things.pdf.

[12]. Nguyen, K. Laurent and O. M, "Survey on Secure Communication," Protocols for the Internet of Things. Ad Hoc Networks, vol. 32, pp. 17-31, 2015.

[13]. Arseni, S. Halunga, S.Fratu, O.Vulpe and S. A., "Analysis of the Security Solutions Implemented in Current Internet of Things Platforms," IEEE Grid, Cloud & High Performance Computing in Science , Romania, pp.28-30, 2015

[14]. M. Mohammadi, M. Aledhari, A. Al-Fuqaha, M. Guizani and M. Ayyash, "Internet of Things: A Survey on Enabling," IEEE, 5 NOV 2015.

[15]. L.Atzori, A.Iera, G. Morabito and N. M, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks,, vol. 56,no. 3594-3608, 2012.

[16]. R. Zejun, L. Xiangang, Y. Runguo and Z. Tao, "Security and privacy on internet of things," in Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference, July 2017.

[17]. Zhang, Q. Wen and X. D. R, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 2012.

[18]. E. Leloglu, "A Review of Security Concerns in Internet of Things," Journal of Computer and Communications, vol. 5, pp. 121-136, 2017.

[19]. "Gartner Inc. Press Release," 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2905717.

[20]. J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-supported Internet of Things," IEEE Internet ofthings Journal, vol. 3, 2016.