# SECURITY AND PRIVACY CHALLENGES IN INTERNET OF THINGS (IoT) -A SURVEY

*T. Janani*[1] *K. Prathapchandran*[2] *G. Manivasagam*[3]

**Abstract—**With the advent of the Internet of Things (IoT), the application of IoT faces security and privacy problems which could affect its sustainable development. Providing security in IoT is more challenging than doing so in the existing network because of its expanded range of communication protocols, device capacities and different standards, all of which bring considerable security issues, and also increase the complexity. This paper presents a broad survey of security-related issues in the current Internet of Things (IoT), and also an analysis of privacy challenges. This paper also delivers some IoT related attacks and security requirements in IoT. Keywords—Internet of Things (IoT), security, privacy, attacks.

## 1. INTRODUCTION

The primary concept of the Internet of Things (IoT) is free flow of data packets between different embedded devices, which communicate with the help of the internet. At first, "Internet of Things" was termed by Kevin Ashton in 1982[1]. IoT applications were rapidly developed, having gradually come to rule our day-to-day life. They cover from conventional gadgets to common domestic activities. Apart from its, there are several security issues and privacy challenges in IoT. It is very crucial to connect numerous devices in IoT applications due to its constraints including memory capacity, energy, processing capability and time. It is very costly to transfer a vast quantity of raw information in the heterogeneous and complicated network. So, IoT requires compression and fusion to decrease the amount of data. Therefore, future IoT needs knowledge of standardization of data processing. [2]. IoT faces a lot of critical challenges for the following reasons: 1) The IoT expands the 'internet' via the existing internet, sensor system, mobile network, etc. 2) All the 'things' in the network are linked through the 'internet', and 3) all the information is exchanged between various "things". Consequently, additional security issues and privacy challenges rose in the IoT. Therefore, extra consideration is needed for authenticity, confidentiality and integrity of the data in the IoT[3]. Reliable, cost-effective and constructive security and privacy are essential for IoT to provide accurate and definite classification, integrity, authentication, and access control[1]. The rest of this paper is arranged as follows: Section 2 describes some IoT attacks, section 3 the important security requirements needed for IoT, section 4 security challenges in IoT, section 5 security issues in different layers, section 6 privacy concerns in IoT and the final section gives the conclusion.

## 2. IoT ATTACKS

### 2.1 Man-in-the-Middle Attack

An adversary interrupts communication among the nodes. While two nodes communicate the illegitimate person can listen and manipulate all personal communications. Packet modification and eavesdropping are the two important kinds of Man-in-the-middle attacks[4]. The establishment of authentication between two devices involve sharing the identities of the devices. In the man-in-the-middle attack probability of identity theft is very high[5].

**2.2 Modification Attack:** An attacker maliciously modifies

[1]Research Scholar, Department of CA, CS & IT, Karpagam Academy of Higher Education, Coimbatore, India.

[2]Assistant Professor, Department of CA, CS & IT, Karpagam Academy of Higher Education, Coimbatore, India.

[3]Assistant Professor, Department of CA, CS & IT, Karpagam Academy of Higher Education, Coimbatore, India.

the data and attacks its integrity, causing distraction and misguides the authorized nodes in the network. The integrity of the message is critically affected in this attack. To identify these attacks, a well-suited Intrusion Detection System(IDS) is required[4].

**2.3 Eavesdropping:** Due to the wireless aspect of the RFID, an unauthorized person can easily break confidentiality. An adversary can detect the confidential data including password or some other data transfer between tag and reader. This kind of attack is easy because the intruder uses this information in wrong ways [7]. This kind of attack threatens message-confidentiality[4].

**2.4 Denial of Service Attack:** Due to low memory and limited computation resource in IoT devices, it is susceptible to resource exhaustion attack. An attacker can transfer the data or request the data from particular devices to deplete their resources. Because of a man-in-the-middle attack, the probability of the DOS attack is high[5]. In this attack, the adversary makes huge traffic with unnecessary data in the network, creating resource depletion in the particular device. Therefore, the user cannot access the network because of the network traffic. The adversary intends to stop the working system to block the services[7].

**2.5 Replay Attack:** when identity-based information or other confidential information is exchanged between two nodes, the adversary may be spoofed, modified or replayed to hold off the network traffic. This active attack is also one kind of man-in-the-middle attack[5].

**2.6 Fabrication:** An attacker may produce redundant information or perform an illegal activity that would not occur usually. This attack generates distraction among the nodes and this kind of attack threatens data-genuineness[4].

## 3. SECURITY CHALLENGE

Security challenges are broadly categorized into two types: one is technological challenge and the other security challenge. Technical challenges include energy constraint, large scale, wireless network, distributed environment, dynamic nature, and pervasive communication. Security challenges are associated with security services including authenticity, trust, confidentiality, and privacy. It also faces the problems of heterogeneity and security between end-to-end devices[5].

The following mechanisms are used to assure security in IoT:

- Only authorized software should be installed in the IoT devices.
- Before initiating a communication, all IoT devices should be authenticated in the network by its identity. The authenticated node only requests or receives the data from other nodes in the network.
- IoT devices only have restricted processing and memory capacities, IoT network requires a firewall to filter the data packets that transfer the devices.
- Device updates and patches should be designed without consuming extra bandwidth[6].

## 4. SECURITY REQUIREMENTS

To provide security during communication, the following security requirements are needed:

**4.1 Confidentiality:** Sensitive information should be denied for unauthorized devices or an adversary. The attacker uses various mechanisms to gain the confidential information. Therefore, IoT applications should ensure that only authenticated devices access confidential data. One of the common security mechanisms is encryption which provides confidentiality of the data.

**4.2 Integrity**: During data transmission, the information should be protected from outside intervention or from an adversary. Data integrity means securing data from attackers with some general method. This method should ensure freshness and correctness of data. The typical methods used to ensure integrity are Checksum and Cyclic Redundancy Check (CRC).

**4.3 Availability**: Data should be available to legitimate users without being attacked by denial of service attacks. Some methods are used to assure the data availability that is Fail-over backup, and redundancy gives a duplicate copy. This copy will be useful when the system fails assuring

availability of the data[7].

**4.4 Authentication:** In IoT, environment authentication checks the identity of a remote user/device on the network.

**4.5 Authorization**: Only the legitimate devices or users can get the services and resources of the IoT network

**4.6 Access control:** It is a selective restriction to access the data. It is needed to make sure that only authenticated devices access authorized services or resources[4].

**4.7 Heterogeneity:** The IoT combine various objects with various capacities, complexity, and from various dealers. Dates and the release versions of IoT devices are different and also functions use diverse technical interfaces. Therefore, protocols should be created to operate in all kinds of devices and also in any kind of situation.

**4.8 Policies**: Existing policies used in network security will not be applicable to IoT, because the devices used in IoT are dynamic in nature and heterogeneous. New policies and standards should be developed to ensure that the data are protect-able, manageable and can be effectively transferable. Each service should be distinctly detected by Service Level Agreements (SLAs).

**4.9 Key Management Systems In IoT:** To protect the confidentiality of the information, it is necessary to exchange some encryption materials between IoT devices and IoT sensors Therefore, the need for a lightweight key management system is important for all models that facilitate trust among various devices and provide the keys for constrained devices with less potential[6].

## 5. SECURITY ISSUES IN DIFFERENT LAYERS

Till now, no common architecture has been developed for IoT. As reported by ITU-T in the year 2002, the IoT architecture is classified into three different layers, namely Perception, Network and Application [2].

### 5.1 Perception layer

This layer is responsible for collecting information, device perception and device control. It can be classified into two different parts: one is perception node that contains sensors, actuators, controllers, etc. and used to obtain information and control the data packets and the other the perception network that is used to exchange information with the transportation network. This network transfers the collected information to the gateway or transfers the control instruction to the controller. WSNs, RFID, RSN, GPS are a few technologies used in the perception layer[2].

#### 5.1.1 Security issues in RFID technology

The cost of Radio frequency identification (RFID) is very minimal and it uses very little energy. It is wireless, works with an unobstructed path for automated identification and collects information from the surroundings. Further, it can scan several tags at the same time and work in hard environments [8].

- **Uniform coding**: At present, there is no standard uniform international encoding for the RFID tag. As a result, errors may occur when reading the data, or, sometimes, RFID tag may not be accessed by the reader. The existing powerful standards are the Universal Identification standard(UID) promoted by Japan and the Electronic Product Code(EPC) standard launched by European[2].
- **Conflict collision:** when several RFID tags send data to the RFID reader at the same extent of time, there is a chance that the reader may read the data falsely[2].
- **RFID privacy protection:** Due to the cheapest rate of RFID tags, it has restricted resources including limited storage space and low processing capacity. Therefore it requires a lightweight solution to protect the privacy of data and location[2]. privacy of data: one of the effective solutions for information privacy is to store inessential data in RFID tag, and essential information in some other top-level services. Location privacy: even though these tags are not stored essential data, the adversary can gain the RFID tag identity information for tacking the current position of the RFID tags [9].
- **Unauthorized tag disabling**: As a result of the DoS(Denial of Service) attacks in the technology of RFID, temporary or permanent failure will occur in the

RFID tags[10].

- **RFID tag cloning Attack(Integrity Related Attack):** Identification-related information can be read by a rogue reader. Once it happens, the probability of creating a duplicate copy of the RFID tag (cloning) is very high[10].
- **RFID tag tracking (Confidentiality Related Attack)**: The RFID tag may be chased via malicious readers. which may result in giving up sensitive information like a person's address[10].

**5.1.2 Security issues in WSNs**

Wireless Sensor Networks(WSNs) are of a dynamic nature and have self-organizing capacity and broadly distributed environments with multi-hop networks. WSNs consist of restricted resources like insufficient storage capacity, low computation ability and limited sensing range. Due to its inadequate resources, the chance of risk in network security is very high. Data security issues are confidentiality, authenticity, integrity, and freshness of data. The solution for these kinds of issues is cryptography-based algorithms, secure routing, and key management.[2].

- **Cryptography algorithms**

The primary application of wireless sensor networks is very broad. These applications require extreme data security that should ensure the confidentiality and integrity of data. Data security can be achieved when using a data-encryption technique[11]. The cryptography method is the foundation of physical layer network security. The encryption algorithm can be classified into two categories: one is symmetric key and public-key encryption algorithms.

- **Symmetric Key Encryption**

The symmetric key encryption algorithm is popularly used in WSNs due to its strong security, faster performance, and fewer computing resources. It faces the following issues: (1) In symmetric cryptosystem, key exchange-based protocol creates more complexity and confidentiality-problem of the key [12].

- **Public key Encryption**

In public key encryption, every node contains its private key and the public key of the base station. In this public key encryption, the base station stores the public keys of all nodes in the network. The additional key management protocol is not required in this algorithm. The scalability of this public-key encryption algorithm is very easy without any complication. There are three existing public-key encryption algorithms used and are applicable in the wireless sensor networks that are NtruEncrypt, Rabin's scheme and Elliptic Curve Cryptography.

Both symmetric key encryption and public key encryption have own advantages and disadvantages. Due to the resource constraint in the wireless sensor networks, these encryption can not solve the security problem[2].

- **Key management in WSNs**

The tasks of key management are, creating a secret key and distributing, storing, updating and devastating the key. One of the problems is to in distributing the public and private keys to the authorized user securely. Therefore, developing a lightweight key distribution method is a primary problem for the sensor nodes with restricted resources. Due to the resource constraint, these sensor nodes do not support different protocols, services, and applications.

There are four methods available to distribute the key to authorized users.

1) Broadcasting method to distribute the key to the whole network.
2) Group-based key sharing
3) Master key distribution.
4) Exchange the key between two nodes[2]

- **WSNs Routing Protocol Security**

In Wireless sensor networks, routing protocol plays an important role in the network layer. However, WSNs face numerous routing-related attacks that disturb the network topology. Therefore, it is necessary to establish a protected and efficient routing protocol in the WSNs. 13]. Due to the constrained resources including low power, low computing capability, and low storage space, the existing routing

protocols cannot apply to wireless sensor networks. Even routing protocols used in the Ad hoc network are not suitable in WSNs and it creates new problems[2].

**5.1.3 Problems of Integrating heterogeneous devices**

RFID is a popularly used sensor node in the Internet of Things(IoT). This network is combined with RFID and WSNs. When integrating data from these sources new issues arise because both WSNs and RFID are not using the same protocols. This creates difficulty in compatibility among data formats and communication protocols. So, it is required to develop a common standard for data encoding and data exchange in IoT [2].

**5.2 Network layer**

The main functions of the network layer are data routing and transferring the data to various IoT devices through the internet. This network layer uses different current technologies to support the IoT operations such as routing, cloud computing platforms, switching, and gateways. The gateway works as an intermediary among various IoT devices by collecting, prepossessing and sending information to and from various sensors. [6].

**5.2.1 WiFi security issues**

WiFi is the most commonly used wireless networking, also known as IEEE 802.11. Most of the IoT applications use WiFi to get the internet to send and receive data, get email, download video, etc. Two types of security issues are possible in WiFi technology, namely network trap and network-related attacks There is a lot of security problems in WiFi, some of which are Denial of Service attack, Phishing attack, data access attacks, etc. [2].

**5.2.2 3G network security issues**

In 3G networks various security-related attacks are possible leading to leaked user data, incomplete data, unauthorized attack, etc. The typical security problems in 3G networks are Denial of Service attack, malicious phishing and attacks related to identity.[2].

**5.2.3 Ad hoc security issues**

Independent wireless devices or nodes build the wireless Ad hoc network and these nodes coordinate with one another. It constructs the fixed infrastructure in a distributed network environment. This network has the capability of being self-organized, self-manageable and self-constructed[14]. Network and radio channels raise security attacks in existing ad hoc network. Wireless channels are susceptible to intrusion and eavesdropping. The security problems of ad hoc networks are access of unauthorized users to the nodes, information security issues and routing-related security issues.

**5.3 Application layer security issues**

**5.3.1 Application Support Layer**

This layer is a higher layer that is placed above the network layer. It assists all kinds of services, accomplishes intelligent computation and assigns resources to filter, select, create and process data.

l **Security Threat**

Security problem is one of the essential features of cloud computation. The platform of the cloud computation encrypts the information and takes the backup of the user information. This information will not be removed until a particular time. Cloud computation has particular key data of enterprises. Therefore, the adversary may target enterprises and personal data.[2].

l **Service interference and attack issue**

Some kind of common service interference will always happen in cloud computation services such as data center being offline, system being off and need for backup data. A DDOS attack is also possible. Thus, the authorized user cannot access cloud services. In cloud computing services, some services utilize more system resources including CPC, memory, bandwidth and disk space. Due to this attack, the cloud server will be largely slow, sometimes the entire cloud service will not respond [2].

**5.3.2 Application layer security issues**

This layer supports combined or distinctive application business. Other layers in the IoT architecture cannot solve the security problems that are handled by an application layer.

For example, a privacy protection problem does not arise in the network layer or perception layer. The application layer is very useful in a particular context like positioning. This layer faces security issues of privacy including location and query privacy. Location privacy means the user's previous and current location, and query privacy means some kind of sensitive information[2].

**6. PRIVACY CHALLENGES IN IoT**

It is important to preserve privacy in the IoT devices and storage location, when communication takes place during the processing. It will be helpful to protect sensitive information. Protecting the end-user privacy and their data is a significant challenges in the IoT which should be addressed[15].

**6.1 Privacy in Device**

IoT consists of a vast number of interconnected and distributed devices that need to communicate with one another. While working with devices sensitive information(such as Biometric, health information) may be accessed by unauthorized persons/objects. For example, an unauthorized person may rewrite the code for a surveillance camera to transfer the data to both the authorized server and also the unauthorized persons. Therefore, the data collected by the IoT devices need to be robust and resist attack. To protect privacy in the IoT devices, trusted calculating technologies such as check the device integrity, attack-resistant framework and trusted execution platform are required [15].

To assure device privacy, several privacy issues need to be fixed. The problem may include location information about the device owner, preserving the identity of the IoT device and personal information. By using the algorithm Multi-Routing Random walk, Location privacy is preserved in the Wireless Sensor Networks. When devices are left or stolen, the adversary can accomplish access using Quick Response(QR) codes technique. Therefore preserving display information and personal identifiable data is essential[16].

**6.2 Privacy during Communication**

Protecting "data in motion" is achieved by maintaining the confidentiality and integrity of the connection between devices. Encryption is used to provide secure communication. In encryption, data packets are combined to provide a technique for discovering the pattern. Examples are IPsec, Security parameter index and sequence number. This information can be used for associating data packets to examine and determine similar data flow traffic. Therefore, secure communication protocols are needed to protect the data when they are transferred. 15].

**6.3 Privacy in Storage**

Securing "data at rest" is ensured by encrypting the data and storing them in a secure location. For securing personal information in storage, the following fundamental rules should be followed:

Only limited data should be saved.

Only private information must be maintained in an essential situation.

Data should be exposed only when it is needed [5].

**6.4 Privacy at Processing**

Protecting "data in use" can be achieved in two ways. The first is, by using private data only for the destined purpose and by not sharing private information with unknown persons. To provide personal information for one needs to get permission from the owner of the information. From the above-mentioned points, Digital Rights Management (DRM) systems are found to be more compatible. It prevents the user data from marketing department, commercial media and preserve the information from improper re-distribution[16].

**7. CONCLUSION**

Although, IoT rapidly developing framework, it meets new complication and drastic challenges. This paper presented a summary of the concept of some IoT related attacks, security requirements needed for IoT and security challenges. This paper also described security issues from the application layer, network layer and perceptual layer. Finally, this paper discussed privacy concerns in the IoT.

**REFERENCES**

[1]Alex Roney Mathew, Study Of Security & Privacy Challenges Of Using IoT(Internet Of Things) In New Era Of Technology, International Journal of Engineering & Scientific Research (IJMRA Publications) Vol. 6 Issue 4, April 2018, ISSN: 2347-6532

[2] Qi Jing Athanasios V. Vasilakos Jiafu Wan Jingwei Lu Dechao Qiu, Security of the Internet of Things: perspectives and challenges, Wireless Netw DOI 10.1007/s11276-014-0761-7, Springer, 2014.

[3]Hui Suoa, Jiafu Wana,b,Caifeng Zoua, Jianqi Liua ,Security in the Internet of Things: A Review,2012 International Conference on Computer Science and Electronics Engineering

[4]Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, Conference Paper, June 2015 DOI: 10.1109/SERVICES.2015.12-.4\

[5]P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability-based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[6]Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges, and Prospective Measures,2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), Publication Year: 2015, Page(s):336 - 341.

[7]M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

[8] Lv, B. Y., Pan, J. X., Ma, Q., & Xiao, Z. H. (2008). Research progress and application of RFID anti-collision algorithm. In Proceedings of the international conference on telecommunication engineering (vo1. 48, no. 7, pp. 124–128)

[9] Lakafosis, V., Traille, A., & Lee, H. (2011). RFID-CoA: The RFID tags as certificates of authenticity. In Proceedings of the IEEE international conference on RFID (pp. 207–214).

[10]Tuhin Borgohain.Uday Kumar,Sugata Sanyal, Survey of Security and Privacy Issues of Internet of Things, Published 2015 in ArXiv.

[11] Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link-layer security architecture for wireless sensor networks. In Proceedings of the second ACM conference on embedded networked sensor systems (pp. 162–175).

[12] Chen, M., Lai, C., & Wang, H. (2011). Mobile multimedia sensor networks: Architecture and routing. EURASIP Journal on Wireless Communications and Networking, 2011(1), 1–9.

[13] Cao, Z., Hu, J. B., Chen, Z., Xu, M. X., & Zhou, X. (2006). Feedback: towards dynamic behavior and secure routing in wireless sensor networks. In Proceedings of the IEEE workshop on pervasive computing and ad-hoc communication (PCAC'06) (vol. 2, pp. 160–164).

[14] Liu, Z. Y., & Yang, Z. C. (2006). Ad hoc network and security analysis. The Computer Technology and Development, 16(1), 231.

[15]Samiksha Ravindra Suryawanshi, A Study on Privacy and Security concerns in Internet of Things,International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 4, Issue 9, September 2016

[16]J. Sathish Kumar, Dhiren R. Patel, A Survey on Internet of Things: Security and Privacy Issues, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014