

# Internet of Things: A Survey on Architecture and Security Attacks

Sivaranjani Ramachandran<sup>1</sup> Satheesh Thangavel<sup>2</sup>

<sup>1,2</sup>Department of Computer Science & Engineering

<sup>1,2</sup>Tamilnadu College of Engineering, Coimbatore, India

**Abstract**— IoT is an interconnected network of heterogeneous devices where these devices communicate with each other. However various vulnerabilities are observed which shall keep IoT as a technology in danger. As a result, there are so many attacks on IoT have been invented before actual commercial implementation of it. This paper provides an overview of Internet of Things (IoT) with an architecture and security attacks. At scratch, it provides an horizontal overview of Iot, and followed by overview of technical details that pertain to the architecture followed by its requirements and its security issues.

**Keywords:** Internet of Things (IoT), Vulnerabilities, Attacks, security issues

## I. INTRODUCTION

The rate of human has been increasing rapidly by using different technologies. The technology called computing power has been increased exponentially [2]. With the increase, a graph of cost and size decreases, whereas performance and number of users keep on increasing. There is a huge growth increase in the number of network connections where every networks are connected to different devices like desktop, laptops, PDA, smart phones, tablets and so on[6]. The future will be communicating with various entities of an object through internet and it is nothing but Internet of Things (IoT).

Internet of things is a group of devices that are interconnected. Many areas uses Internet of Things such as Agriculture, smart cities, transportation, health care and so on [4]. The major advantage of using Internet of Things is it can communicate between various devices. Internet of Things is one of the most developing technologies in India [5]. There is also many opening opportunities for exchanging of knowledge between various entity, growth and innovation.

The term Internet of Things was first introduced by Kevin Ashton, which evolved into a reality that connects electronic devices, sensors and systems to the Internet. In the year of 2005, International Telecommunication Union (ITU) had released an annual report on IoT. In that report, RFID and intelligent computing technology had opened an era that interconnects global things.

Internet is the important factor for Internet of things, we can say the internet as the heart of IoT and it is the supporting center. The threats in security will lie within the internet that propagates to IoT. The large privacy problem is introduced as the devices collects and transfer the data that are more sensitive. This becomes even larger issue with collecting the data, financial devices, tracking devices and most importantly cameras. These collects sensitive information. IoT is not designed with keeping security in mind.

In this paper, several layers of Iot and the attacks are been discussed with the adaptive solution. In IoT there are several layer namely application layer that depicts about middleware, network devices that functions by using gateway

and the perception layer depicts about the sensors cameras and RFID. IoT attacks are further classified into several attacks that are based on network. In those attacks several attacks are said to be dangerous attacks according to their detection. IoT Architecture contains some common layers between them. The below figure 1 shows one of the layered Architecture for IoT.

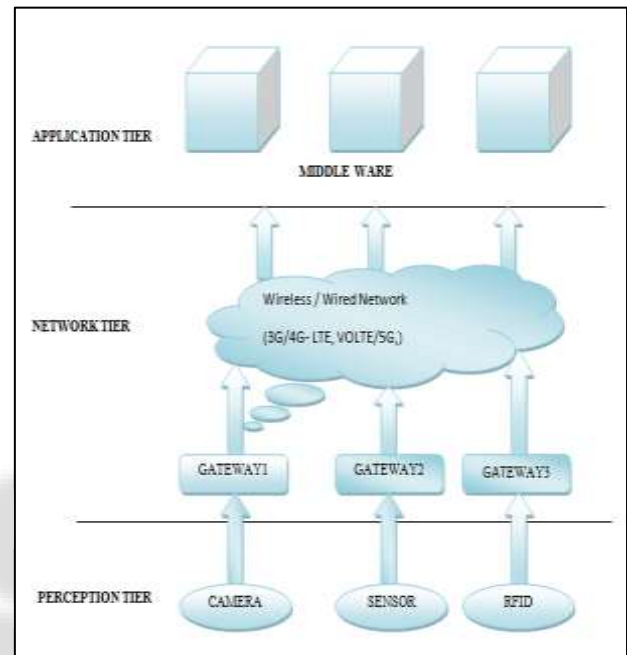


Fig. 1: Architecture of IoT

The paper is organized as follows. Section II gives the overview of ease of IoT security architecture and requirements. Section III is the IoT attacks, Section IV concludes the paper and gives the future work.

## II. EASE OF IOT SECURITY ARCHITECTURE AND REQUIREMENTS

Among the layers in IoT, the network layer faces the greatest security challenges. There is requirements of security in processing, sensor storage and transmitting the information that will prevents accessing the unauthorized information and doing illegal operation. Some of the security requirements include failure tolerance, authentication, control of access, privacy [3]. In failure tolerance when there is an occurrence of failure in one node, alternative node should be chosen by the system to avoid failure.

The authentication is used to authenticate the information source and object. The control of access is usually implemented on the data provided by the providers. The privacy deals with the information provider observing the specific customer. The other security requirements that must be considered while implementing IoT are, user identification, secure network access, secure storage, secure execution environment, secure data communication. There are four levels of IOT security architecture they are described below:

A. Physical Layer

The physical layer collects data and information with the help of peripheral devices and identifies the information about the physical world such as environmental condition and properties of the object. It includes sensors, RFID reader equipment, Global Positioning System and other equipments [3]. The important element in the physical layer is sensors which represent the real world information in the digital world. Since the storage nodes and the power capacity is very short the public key encryption algorithm cannot be used for secure protection because the physical layer is highly vulnerable to attacks[10]. In this un authorized access of the node can be prevented with the help of authentication, and data encryption can be used to prevent confidentiality.

B. Network layer

The network layer deals with reliable transfer of information that depends on mobile communication network, satellite communication network and communication protocols that are necessary for exchanging data between the devices [3]. Here Man-In-the-Middle-Attack attack exist hence providing security at this level is very important in IoT and in addition denial of service attack exist [10]. But this layer is very difficult for implementing the security in communication. Some of the protection mechanism need to be implemented includes authentication, confidentiality and integrity of data.

C. Support layer

The main concern of the support layer is to provide a reliable platform and this platform supports every kind of smart computing power that will be organized by the cloud computing and network grid. It plays the role in the top layer and the network layer to the bottom as a combined application. The data processing is done to do an intelligent

decision for network behavior in support layer, so it considered to be a challenge to improve the ability of identifying the harmful information. This layer needs too many of security application structure such as secure cloud computing and multi-party computation, strong encryption algorithms and protocol for encryption, anti-virus technology and stronger security system[10].

D. Application Layer

The application layer is at the top-level of the security architecture. The application layer provides personalized services according to the user’ s needs. The user’ s can login to the Internet of things through the application interface layer of the mobile, computer, TV or equipment and so on[9]. There are different applications used in this layer, among them sharing of data is one of the feature of the application layer, which create data privacy problems, information disclosure and access control [3]. There are two aspects needed to solve the problem of security in this layer. The first is the authentication and key agreement across the heterogeneous network, the second is protection of the user’ s privacy [3] .

The IoT is divided into three layers based on the IoT infrastructure the layers are perception layer, network layer, application layer and some of the security risks in this layer are discussed. The perception layer gathers information from the surrounding environment, hence it is very easy for attackers to eavesdrop the communication and they can easily capture the information about the user. The network layer which is mainly used for communication exchanges huge amount of data result in network congestion. The application layer provides real time information for developing IoT [10]. The security features and security requirements of each layers are represented in figure 2.

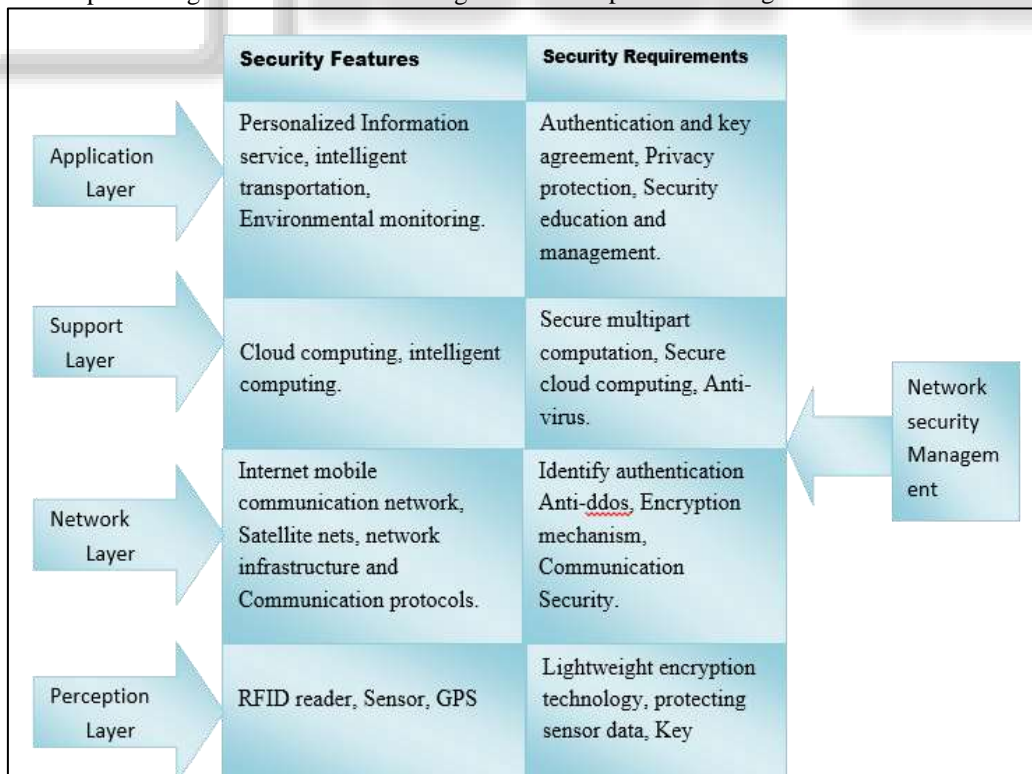


Fig. 2: Security features and security requirements.

### III. IOT ATTACKS

The security of IoT is a big challenge because of complexity, heterogeneity and a large number of interconnected

resources. The adversary can perform the attack on IoT system by damaging the nodes. There are several security attacks and they are listed in below figure 3.

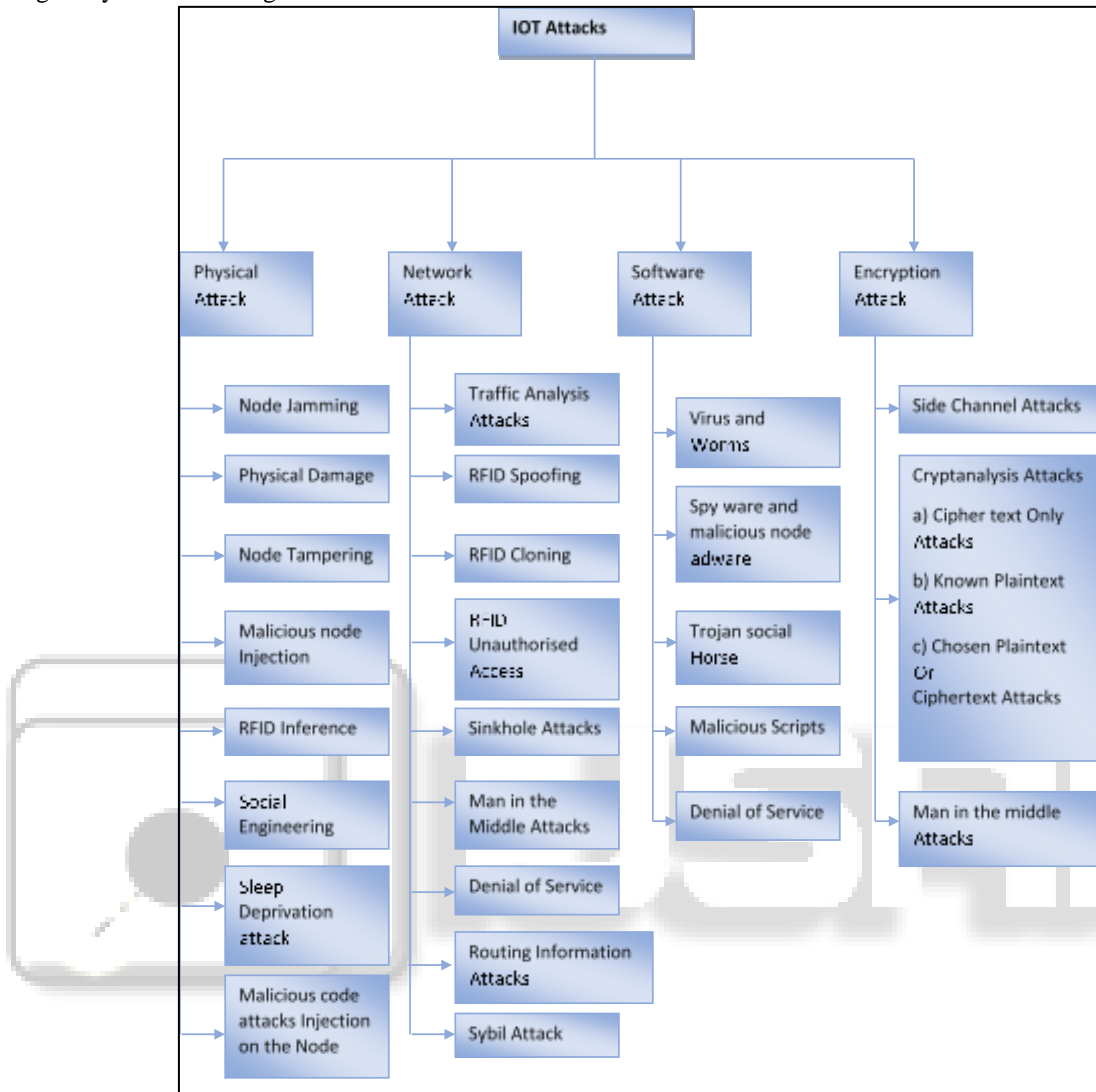


Fig. 3: IoT ATTACKS

#### A. Physical Attacks

The physical layer concentrates on the hardware devices in the IoT systems [3].

- 1) Node Tampering: It physically alerts the node which is been compromised and also can obtain sensitive information like encryption key [1].
- 2) RF Interference on RFIDs: It performs Denial of service attack by sending signal through noise over radio frequency signals. It is used for RFID' s communication.
- 3) Node Jamming in WSNs: In this attack the attacker can disturb the wireless communication by using jammer. It causes denial of service attacks.
- 4) Malicious Node Injection: In this, the new malicious node between two or more nodes was injected physically by the attacker. Then the data has been modified and passes the wrong information to other nodes [1]. Multiple nodes are been used by the attacker to perform malicious node injection attacks [7]. To prevent this attack, monitoring verification scheme can be used.

- 5) Physical Damage: The components of IoT system are harmed by the attacker and results in the attack called Denial of service.
- 6) Social Engineering: In this attack, the attacker physically manipulates and interacts with the user of IoT system.
- 7) Sleep Deprivation Attack: The attackers aim is to use more power and that results in shutting down of nodes[3].
- 8) Malicious Code Injection: It physically introduces a malicious code into IoT system. The attacker gets full control of IoT system.

#### B. Network Attacks

This attack is based on network of IoT system. The adversary can perform the attack on system by damaging node.

- 1) Traffic Analysis Attacks: In this attack, the attacker intercepts and examines messages to provide network information.

- 2) **RFID Spoofing:** It spoofs RFID signals and then it captures information that is been transmitted from RFID tag. It gives wrong information that seems to correct.
- 3) **RFID Cloning:** The data is been copied from pre-existing RFID tag to other RFID tag[3]. The original ID is not been copied. By using cloud node the attacker can control the data passing or can insert the wrong data.
- 4) **RFID Unauthorized Access:** The adversary can observe, alter or remove information on the nodes, if there is an incorrect authentication.
- 5) **Sinkhole Attack:** the node inside the network has been compromised by the adversary and performs the attack by using this node[1]. The node which is been compromised sends a fake routing information to its neighbor node. It also alters the data and drop the packets.
- 6) **Man in the Middle Attacks:** by using the internet the attacker intercepts the communication between two nodes.
- 7) **Denial of Service:** In this type of attack the attacker floods the network with huge traffic, so that services are not available to the users [1].
- 8) **Routing Information Attacks:** By spoofing, modifying or sending routing information, the attacker can make the network complex which results in allowing or dropping packets and forwarding wrong data.
- 9) **Sybil Attack:** The malicious node takes the identities of multiple nodes. e.g. voting system- in wireless sensor network, single node can vote many times.

#### C. Software Attacks

The attacks like virus, worm, spyware, adware etc are been performed by the attacker to steal data and to deny the services.

- 1) **Phishing Attacks:** The private information like username, passwords by email spoofing and using fake websites are been obtained by attacker [3].
- 2) **Virus, Worms, Trojan horse, Spyware and Aware:** It can damage the system by using malicious code. The worm has the ability to replicate itself without any human action.
- 3) **Malicious Scripts:** The attacker can gain access to the system by injecting malicious script.
- 4) **Denial of Service:** The user is been blocked by the attacker from the application layer [1].

#### D. Encryption Attacks

Encryption depends on destroying encryption method and to obtain the private key.

- 1) **Side-channel Attacks:** The side channel information is used by the attacker that is emitted by encrypting devices. It is neither a plaintext nor the cipher text. There are different types of side-channel such as Simple and Differential Power Analysis, timing attacks and Differential Fault Analysis [3].
- 2) **Cryptanalysis Attacks:** The encryption key is been obtained by either using plaintext or cipher text.
  - a) **Cipher text Only Attacks:** The attacker can access cipher text [3].
  - b) **Known Plaintext Attack:** The plaintext for some part of cipher text is known to the attacker. The aim is to decrypt the remaining text.
  - c) **Chosen Plaintext Attack:** The attacker need to choose what plaintext is encrypted and to find the encryption key.
  - d) **Chosen Cipher text Attack:** Using the plaintext of chosen cipher text the attacker can find the encryption key.

- 3) **Man in the Middle Attacks:** The attacker intercepts the communication when two users are interchanging the key and then the attacker obtains the key [1].

#### IV. CONCLUSION & FUTURE WORK

As network architecture is been used by the internet of things which is similar to our traditional network that is used for communication between various devices. In the development of IoT, many kinds of attacks are been introduced to breach the security of IoT devices. Many solutions are invented by researchers to avoid the happening of such attacks. By implementing all these techniques it is used to consume computation and also battery power of such devices which is not been acceptable for IoT devices and technologies [10]. By analyzing all these we need a mechanism for security which is used for handling the huge security problems. It should be light weight and it should be robust for IoT technology. Several attacks are been discussed above. Some attacks are difficult to detect or to prevent and should find a secure and efficient solution.

As IoT uses network architecture that was based on traditional network that are used for communication between different devices[19]. There is a huge need for refinement of existing network architecture or to create a new architecture, which is light weight and secure that is possible for solving performance and security and related issues. The future work is the refinement of all the layers in security.

#### REFERENCES

- [1] Jyoti Deogirakar, Amarsinh Vidhate, " Security Attacks in IoT: A Survey" , Dept.of Computer Engineering R.A.I.T Navi Mumbai, India,2017.
- [2] Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri, " IoT Security Framework for Smart Water System" , ECE Department The University of Arizona Tucson, ,2017.
- [3] Ibrahim R. Waz, Mohamed Ali Sobh, Ayman M. Bahaa-Eldin, " Internet of things(IoT) security platforms" , Ministry of communication cairo, 2017.
- [4] Israr Ahmed, Saleel A.P, Babak Beheshti, Zahoor Ali Khan, Imtiaz Ahmad, " Security in the Internet of Things (IoT)" , Oct., 25 – 26 2017.
- [5] Yogeesh Seralathan, Tae (Tom) Oh, Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong, Young Ho Kim, and Jeong Noyo Kim, " IoT Security Vulnerability: A Case Study of a Web Camera" , February 2018.
- [6] Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai," Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study" , February 2018.

- [7] Hui Suo, Jiafu Wan, Caifeng Zoua, Jianqi Liu, “ Security in the Internet of Things: A Review” , 2012.
- [8] Arbia Riahi Sfar, Enrico Natalizi, Yacine Challal, Zied Chtourou, “ A roadmap for security challenges in the Internet of Things” , VRIT Lab - Military Academy, Nabeul, Tunisia
- [9] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibib “ Internet of things Security: A Survey” , Faculty of Computer Science and information Technology, University of Malaya.
- [10] Mayuri A. Bhabad, Sudhir T. Bagade, “ Internet of Things: Architecture, Security Issues and Countermeasures” , P.G. Scholar Dept. of Computer Science and Technology Usha Mittal Institute of Technology, SNDT Women’ s University, Volume 125 – No.14, September 2015.
- [11] Taha M. Alfaqih, Jalal Al-Muhtadi,” Internet of Things Security based on Devices Architecture” , Information System Department King Saud University Riyadh, Saudi Arabia, Volume 133 – No.15, January 2016.
- [12] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, “ Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues” , Volume 17, NO. 3, 2015.
- [13] Mangal Sain, Young Jin Kang, Hoon Jae Lee,” Survey on Security in Internet of things: state of the art and challenges” , Department of Computer Engineering, Dongseo University, South Korea, February 2017.
- [14] Saad Albishi, Ben Soh, Azmat Ullah, Fahad Algarni, “ Challenges and Solutions for Applications and Technologies in the Internet of Things “ , Department of Computer Science and Computer Engineering, La Trobe University, La Trobe Business School, La Trobe University, Australia , Bisha University, Saudi Arabia.
- [15] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, “ Internet of Things: A survey on the security of IoT frameworks” , Department of Computer Science, KU Leuven University, Department of Computer Science, University of Auckland, New Zealand.
- [16] Ala Al-Fuqaha, Mohammed Aledhari, & quot;Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications & quot;, vol. 17, no. 4, fourth quarter 2015.
- [17] Alma Oracevic, Selma Dilek, Suat Ozdemir, & quot; Security in Internet of Things: A Survey&quot;,2017.
- [18] Radek Krejci Ond`rej Hujnak Marek Svepeš, & quot; Security Survey of the IoT Wireless Protocols&quot;,2017.
- [19] Ankush B. Pawar Dr. Shashikant Ghumbre, & quot; A Survey on IOT Applications, Security challenges and counter measures&quot;,2016.
- [20] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li\_, and Hongbin Zhao, & quot;A Survey on Security and Privacy Issues in Internet-of- Things&quot;, 2016.
- [21] Alma Oracevic, Selma Dilek, Suat Ozdemir, & quot;Security in Internet of Things: A Survey&quot;.,2017.