International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Review on Vulnerabilities of IoT Security

Dr. E. J. Thomson Fedrik[1], A. Vinitha[2], B. Vanitha[2]

[1]Associate Professor, [2]MCA Student
[1,2]Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

How to cite this paper*:* Dr. E. J. Thomson Fedrik | A. Vinitha | B. Vanitha "Review on Vulnerabilities of IoT Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1117-1119, URL: https://www.ijtsrd.com/papers/ijtsrd24020.pdf

IJTSRD24020

ABSTRACT

IoT is referred as Internet of objects and wireless sensor networks and RFID are enabled in the fields of education, health, agriculture and entertainment. The IoT is the development production of the computer science and communication technology. The vulnerable nature of IoT is related to the security and privacy issues. The user may face as the consequence of the spread of IoT technology. The survey is focused on security loopholes arising out of the information exchange technologies used in IoT. Data analytics utilizes IoT and Big Data and it faces security challenges to protect their important data. In 2020, the wide amount of data could be generated by using the technologies of IoT and Big Data. The purpose of this survey is to analyze the vulnerable security issues and risk involved in each layer of the IoT as per to our knowledge the first survey with some goals.

Keywords: *RFID, WSN, Security and privacy*

1. INTRODUCTION

The IoT is the combination of physical objects with sensors, actuators and controllers with connectivity to the public world via the internet. The term “IoT” was first coined in 1998 and it is defined as, “the internet of things allows people and things to be connected anytime, anyplace with anything and anyone ideally using any path or network and any service”. Due to technological development there is increase in number of interconnected sensing and computing devices.

The information that can be accessed through the IoT devices are susceptible to the hackers to evaluate the security loopholes of the IoT devices. IoT is collecting data from various sources and making them useful. Big Data can be defined as collection of data with sizes beyond the ability of commonly used software tools to capture and analyze within a stipulated time. Business organization uses Big Data to compete in market and outperform and use data driven technologies to innovate, compete and capture value. Big Data organization to make better decision to compete. The BI techniques include Big Data analytics which extracts the information using data mining. Recent techniques such as data mining, predictive analysis, statistical analysis are performed in organizations.

There is no technology and protocol to support the IoT and it deals with,
- Motivation for IoT security.
- Security issues in IoT architecture.
- IoT applications and security issues and attacks in various layers.

2. LITERATURE REVIEW

Vinay Sachidananda et al, 2017 did the research on the IoT with the help of Testbed framework through the holistic approach constituting the initial groundwork in security analysis for IoT devices, have demonstrated the vulnerability level of IoT devices. Tuhin Borgohain, Uday Kumar and Sugata Sanyal, 2015 focused on the security loopholes arising out the information exchange technologies used in IoT. They used the cryptographic and stenographic security measures to exchange the information. Azamuddin, 2017 did the research on the development production of computer science and technology of IoT. The embedded security of IoT is maintained using the cryptographic algorithm such as Elliptic-Curve-Cryptography (ECC) used for melting the requirements of execution speed. Santhosh Krishna.B.V, Gnanasekaran.T, 2017 did the research on IoT that deals with motivation of IoT security, security issues in IoT architecture and IoT applications, and security issues and attacks in various layers. The techniques used are TLS, SSL and DNS. Alex Roney Mathew and Aayad Al Hajj, 2017 focused on security challenges to protect their important data. The authentication is based on Generic Bootstrapping Architecture (GBA) and key agreement used for device identification. Here Secure key storage, authentication methods used together for secure communication.

3. REVIEW ON IoT SECURITY

In the current scenario, security in technology plays a major role in IoT. There are number of protocols and technologies that are available to address most of the security issues for wireless networks, but still there are many security issues in each layer. The whole communication infrastructure of the IoT is flawed from the security standpoint and is susceptible to loss of privacy for the end users. The security issues of each layer are described below.

3.1. SECURITY ISSUES IN IoT ARCHITECTURE:

- Application layer
- Middleware layer
- Network layer
- Perception layer

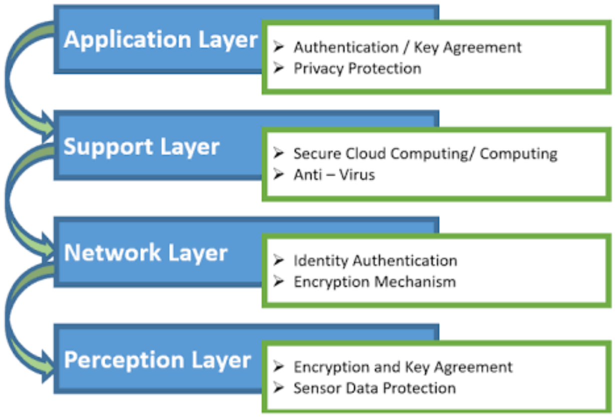

Figure1. IoT architecture for security issues

3.1.1. PERCEPTION LAYER:

This layer is a sensor network and RFID security policy and it is the lowest layer where information can be passed across IoT network. The issues in sensor network are physical capture of sensor nodes, integrity and congestion attacks, eavesdropping and node replication networks. The issues in RFID networks are tampering attacks, leakage of information. Issues of this layer are unauthorized access, theft, wiretapping and replay attacks.

3.1.2. NETWORK LAYER:

This layer is also known as information transmission security policy. This is used to transfer of information across the network and it is implemented on communication framework. Issues created by this layer are to maintain authenticity, confidentiality, integrity, data availability.

3.1.3. MIDDLEWARE LAYER:

This layer is also known as information processing security policy and is used to process information and provide interface between network and application layer. Issues of this layer are privacy, security and reliability.

3.1.4. APPLICATION LAYER:

This layer is also known as information application security policy. Privacy is the major issue of this layer. The unauthorized persons could collect the information by hacking using this layer.

3.2. SECURITY ISSUES IN WIRELESS SENSOR NETWORK (WSN):

A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. A wireless sensor network is an important element in IoT paradigm. Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors. WSN based on IoT has received remarkable attention in many areas, such as military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire and flood detection.

The oppressive operations that can be performed in a wireless sensor network can be categorized under three categories:

- Attacks on secrecy and authentication.
- Silent attacks on service integrity.
- Attacks on network availability.

3.3. SECURITY ISSUES IN RADIO FREQUENCY IDENTIFICATION (RFID):

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or person wirelessly using radio waves in the form of a serial number. RFID technology plays an important role in IoT for solving identification issues of objects around us in a cost effective manner. RFID used in information tags and they use radio frequency waves for interacting and exchange information without any requirement for alignment in the same line of sight or physical contact. This uses Automatic Identification and Data Capture (AIDC).

- Active tag- This houses a battery internally, which facilitates the interaction of its unique EPC with its surrounding EPCs remotely from a limited distance.
- Passive tag- The information relay of EPC occurs only by activation by a transceiver from a predefined range of the tag.

This is mainly used as RFID tags for automated exchange of information without any manual involvement. The most common attacks are

- **Attack on Authenticity-** This attack render a RFID tag to malfunction and misbehave under the scan of a tag reader, its EPC giving misinformation against the unique numerical combination identity assigned to it.
- **Attack on Integrity-** The capturing of the identification information through the manipulation of the tags by rogue readers.
- **Attack on Confidentiality-** A tag can be traced through rogue readers, which may result in giving up of sensitive information.
- **Attack on Availability-** The communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag.

3.4. SECURITY ISSUES IN PHYSICAL LAYER:

This layer performs the function of selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data. This layer is mainly attacked through

- **Jamming-** This occupies the communication channel between nodes thus preventing them from communicating with each other.
- **Node tampering-** Physical tampering of the node to extract sensitive information.

3.5. SECURITY ISSUES IN DATA LINK LAYER:

This layer of WSN multiplexes the various data streams, provides detection of data frame, MAC and error control. This layer is mainly attacked through

- **Collision-** Collision occurs when two nodes simultaneously transmit packet of data on the same channel.
- **Unfairness-** Repeated collision based attack.
- **Battery Exhaustion-** This occur unusually high traffic in a channel making its accessibility very limited to the nodes.

3.6. SECURITY ISSUES IN NETWORK LAYER:

The function of this layer is routing. This layer is mainly attacked through

- **Spoofing-** This causes replaying and misdirection of traffic.
- **Hello flood attack-** This causes high traffic in channels by congesting the channel with an unusually high number of useless messages.
- **Homing-** A Search is made in traffic for cluster heads and key managers which has the capability to shut down the entire network.
- **Sybil-** The attacker replicates a single node and represent it with multiple identities to other nodes.
- **Wormhole-** Relocation of bits of data from its original position in the network.

3.7. SECURITY ISSUES IN TRANSPORT LAYER:

This layer provides reliability of data transmission and avoids congestion resulting from high traffic in the routers. This layer is mainly attacked through

- **Flooding-** Refers to deliberate congestion channels through relay of unnecessary messages and high traffic.
- **De-synchronization-** Fake messages are created at one or both endpoints requesting retransmission for correction of non-existent error.

3.8. SECURITY ISSUES IN APPLICATION LAYER:

This layer is responsible for traffic management. This also acts as the provider of software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries.

3.9. SECURITY CHALLENGES WITHIN IoT AND BIG DATA:

IoT is main target of security attacks is whole communication process is performed between IoT devices. The components involved are IoT device itself and gateway. If gateway is damaged then whole communication process gets affected. Interference caused due to jamming of physical channel between nodes. Signal interception caused due to traffic flow, unauthenticated access, insecure network resources. Intrusion occurs due to insecure user interfaces, software. Exploitation occurs when attackers act as authenticated users to access the data. Communication process can be hijacked the sensors and devices for communication by attackers. Gateway plays an important role in communication. IoT can replace damaged devices and install new devices. Authentication and authorization can be achieved by end-to-end encryption. End nodes can be hacked by attackers. Biometric information can be used to authenticate and authorize the communication.

4. CONCLUSION

This paper presents a survey on vulnerable issues in IoT security. Tremendous changes occurs in business utilizing big data by analyzing and targeting marketing specifications. Business organizations should concentrate on security and secure communications through IoT security techniques. Security becomes very vulnerable in our current scenario hence there is an need to secure our information by using any of the Cryptographic and Stenographic security measures in the information exchange process and use of the efficient methods for communication will result in more secure and robust IoT information.

5. REFERENCES

[1] Alex Roney Mathew and Aayad Al Hajj " Secure Communications on IoT and Big Data",2017.

[2] Azamuddin "Survey on IoT Security", 2017.

[3] Santhosh Krishna.B.V, Gnanasekaran.T "A Systematic Study of Security Issues In Internet of Things", 2017.

[4] Tuhin Borgohain, Sugata Sanyal "Survey of Security and Privacy Issues of Internet of Things", 2015.

[5] Vinay Sachiananda, Shachar Siboni, Asaf Shabtai, Jinghui Toh, Suhas Bhairav, Yuval Elovivi "Let the cat out of the bag: A Holistic Approach Towards Security Analysis of the Internet of Things", 2017.