International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

A Study on Security and Privacy in Internet of Things

Muthu Lakshmi. R[1], Mrs. T. Sathiyabama[2]
[1]III MCA, [2]Assistant Professor
Department of Computer Applications, Dr. Sns Rajalakshmi College of Arts & Science,
Coimbatore, Tamil Nadu, India

ABSTRACT

In the past decade, Internet of Things (IOT) has been attention of analysis. Security and privacy are the key problems for IOT applications, and still face some monumental challenges. So as to facilitate this rising domain, we tend to in short review the analysis progress of IoT, and listen to the protection. By suggests that of deeply analyzing the protection design and options, the protection necessities are given. On the idea of those, we tend to discuss the analysis standing of key technologies together with cryptography mechanism, communication security, protective device knowledge and scientific discipline algorithms, and in brief define the challenges.

***Keyword:** Internet of things; IOT threads; Security; Issues of security; Privacy; IoT challenges.*

INTRODUCTION

The Internet of things (IoT) is that the system of physical devices, vehicle, home appliances and different objects entrenched with physics, software, sensors, actuators, and property that modify these items to affix additionally to modify over data. each item is unambiguously acknowledgeable through its embedded ADPS however is in a position to inter-operate at intervals the present web infrastructure. Now days, web of things having huge growth within the field. the web technologies square measure primarily employed in all over.

Internet of things is meted out of communication through on web technology. web subject was 1st planned by Kevin Sir Frederick Ashton as on year 1982. During this paper we have a tendency to focuses numerous regarding advanced mode of communication between numerous fields for virtual surroundings as on IOT building the conception of device to device communication technology. The wireless communication technology through web infrastructure for the exchange of knowledge, and survey of the all security issue taking part in the web of things additionally as security issue faced by the top user. The security of the wireless communication technologies and steps takening for addressing all level of security problems with IOT.

Internet Of Thins in a security and privacy perspective, the expected pervasive introduction of sensors and devices into presently intimate areas – like the house, the car, and with wearable's and ingestible, even the body – poses explicit challenges.

IOT THREADS:

- **SECURITY THREADS IN SMART HOME**
  Smart home services can be exposed to cyber attack because service providers do not consider security at earlier stage.
- **TRESPASS**
  If the smart door is effected by codes or unauthorized part on smart home. To prevent these attack password of smart door should frequently changed, authentication, access control applied.
- **MONITORING AND PERSONAL INFORMATION LEAKAGE**
  Lot of sensors are used for monitoring , house breaking. If these sensor hacked by attacker data encryption applied between gateway and sensors.
- **DOS/DDOS**
  Attackers may access smart home network by send bulk messages. They also send malicious codes to attack devices for avoid this authentication to block an unauthorized access.
- **FALSIFICATION**
  If the smart home communicate with server the attacker may changing the packets gateway. To

secure SSL (Secure Socket Layer) technique applied.

ATTACKS IN LAYER:

HARDWARE LAYER

Hardware layer is the root of the computing system and the hardware security system is developed for mobile and desktop and cloud systems.

SECURITY FOR HARDWARE:

The hardware Trojans are exist in a chip. The hardware level Trojans malicious components or instruction sequence that when triggered, circumvent security guarantees.

HARDWARE FOR SECURITY:

Two properties are hardware security techniques.

- A hardware root of trust.
- Hardware supported software

The hardware is mainly used to store cryptographic keys.

SYSTEM SOFTWARE LAYER:

In system software layer firmware OS code and private illegal system application or program frameworks are processed.

The software can be mainly secured by these techniques.

- Process isolation
- Access control
- Information flow control
- Software updates
- Authentication

NETWORK LAYER:

The network layer is mainly used to communicate with one another. IOT network is marked by a multitude of protocols and fixed function devices.

ANALYSIS OF DIFFERENT TYPES OF ATTACKS AND POSSIBLE SOLUTIONS

The IOT facing various types of attacks including active attacks and passive attacks. Hence the security constraints must applied to prevent devices from malicious attacks. In this different types of attacks and levels of attacks is discussed.

- **Low-level attack**: If an attacker tries to attack a network and his attack is not successful.
- **Medium-level attack**: If an attacker/intruder or an eavesdropper is just listening to the medium but dont alter the integrity of data.
- **High-level attack**: If an attack is carried on a network and it alters the integrity of data or modifies the data.
- **Extremely High-level attack**: If an intruder/attacker attacks on a network by gaining unauthorized access and performing an illegal operation, making the net- work unavailable, sending bulk messages, or jamming network.

SECURITY

- **CRIME**

  The IOT will expand criminal uses of Internet by providing vastly more devices for criminals to exploit and multitudes of new protocols.

  Crime-as-a-service allows one to commit crimes from a great distance and protected by poor traceability.
- **CYBER WALFARE**

  This cyber physical system machines has ability to manipulate the physical environment that their controlled by embedded computer systems.
- **EMERGENT BEHAVIOURS**

  These side effects are happened because of feedback relationships.

SECURITY ISSUES

SECURITY ISSUE IN WIRELESS SENSOR NETWORK

The operations that are performed in WSN are

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

DOS ATTACK ON PHYSICAL LAYER

The physical layer carried out the function of selection and generation of carrier frequency. This layer is attached mainly through

- Jamming
- Node tempering

DOS ATTACK ON LINK LAYER

The link layer provides detection of data frame, MAC and error control. Some of the places where DOS attack take place in this layer are,

- Collision
- Unfairness
- Battery exhaustion

DOS ATTACK ON THE NETWORK LAYER

The main function of network layer is WSN routing. In network layer the DOS attack is happens in these layers,

- Hello food attack
- Homing
- Selective forwarding
- Sybil
- Wormhole

SECURITY ISSUES IN RFID

RFID is used for exchanging information without any manual work.

1. **UNAUTHORIZED TAG DISABLING**
   Render a RFID tag to malfunction and misbehave under the scan of a tag reader.
2. **UNAUTHORIZED TAG CLONING**
   The capturing of the identification information. Ones the identification information of tag is compromised then replication of the tag is possible.
3. **UNAUTHORIZED TAG TRACKING**
   A tag can be traced through reader they can read information. . There is no confidentiality.
4. **REPLAY ATTACKS**
   In this the attacker uses a tag's response to rouge readers. In replay attacks the communication between the reader and tag is interrupted.

PRIVACY:

In this we discuss the privacy impacts of internet of things, we discuss the privacy impacts of society of these data streams enables by IOT and grant challenges arise from them.

- Location data
- Audio data
- Video data
- Digital identity
- Vehicles
- Other personal data
- Ubiquitous sensing

PRIVACY CONCERNS OF IOT

Privacy can be protected in the device in storage during communication. The privacy of users and their data protection has been concerned by their secure communication.

PRIVACY IN DEVICE

The information may be leaked out in the case of unauthorized manipulation or handling of hardware or software in these devices. In order to provide privacy, protecting the personal information incase device is theft. This can be achieved by WSN by using multi routing random walk in wireless device.

PRIVACY DURING COMMUNICATION

In this encryption technology is used to achieve confidentiality during communication and pseudonyms can be replaced by encryption.

PRIVACY IN STORAGE

To achieve the real identity with the storage of data psudonymization and anonumization could be used.

PRIVACY IN PROCESSING

- It is mainly processed on two things. Personal data must be rarely collected in the intended purpose.
- Without the data owner knowledge personal data should not be accessed by third parties.
- User permission and their awareness are the requirements of data processing.

IOT CHALLENGES:

The most important challenges are

- Data privacy
- Data security
- Insurance concerns
- Lack of common standard
- Technical concerns
- Security concerns

DATA PRIVACY

Some manufacturers of smart TVs collect data about their customers to analyze their viewing habits so the data collected by the smart TVs may have a challenge for data privacy during transmission.

DATA SECURITY

Data security is also a great challenge. While transmitting data seamlessly, it is important to hide from observing devices on the internet.

INSURANCE CONCERNS:

The insurance companies in- stalling IoT devices on vehicles collect data about health and driving status in order to take decisions about insurance.

LACK OF COMMON STANDARD

Since there are many standards for IoT devices and IoT manufacturing industries. Therefore, it is a big challenge to distinguish between permit- ted and non-permitted devices connected to the internet.

A GRANT CHALLENGES OF IOT

- **A SCIENTIFIC OR TECHNICAL CHALLENGES**

  The main challenges is calculate of data transmission rates predict significant engineering. The general estimation science to approximate how difficult is to identify an individual form of data.

  The common criteria have defined set of privacy qualities for privacy preserving identity management.

- **ANONIMITY**

  An individual use of resource without disclosing identity.

- **PSEUDONYMITY**

  An individual use resource without identity but remain accountable for use.

- **UNLINK ABILITY**

  An individual make multiple user of resource without others being able to link these together.

- **UNOBSERVABILITY**

  An individual may use a resource without others, especially third parties able to observe that the resource being used.

CONCLUSION

IoT is a scheme of connected physical objects that square measure accessible through the web.

This paper is focus on security vulnerabilities and therefore the challenges featured in IOT. the safety necessities are mentioned during this paper. take into account the importance of IOT security. Its important to put in security mechanism in IOT devices and communication networks. Finally, during this paper chiefly focus regarding security problems and their challenges and conjointly secure IOT devices by victimization security necessities. This paper mentioned regarding a way to secure the IOT layers like hardware, Software, Network, Application Layers. Consistent with this paper security mechanism for these layers's doing seem to be developed and in future the safety for these systems ought to developed. During this paper the author focuss regarding the privacy of data in IOT, the economical info management and their method. The most issue of web of issue is security.

REFERENCES

1. N. Papernot, "Towards the Sci- ence of Security and Privacy in Machine Learning," Com- puting Research Repository, vol. abs/1611.03814, 2016; arxiv.org /abs/1611.03814.
2. 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.
3. M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.
4. Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg, "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology;
5. Burmester, Mike, and Breno De Medeiros. "RFID security: attacks, countermeasures and challenges." The 5th RFID Academic Convocation, the RFID Journal Conference. 2007.
6. J. Sen, "A Survey on Wireless Sensor network Security", International Journal of Communications Network and Information Security, vol. 1, no. 2, (2009) August, pp. 59-82.
7. N. Davies et al., "Privacy Mediators: Helping IoT Cross the Chasm," Proc. 17th Int'l Workshop Hot Topics in Mobile Computing (Hot Mobile 16), 2016, pp. 39–44.
8. A. Cardenas et al., "Challenges for Securing Cyber Physical Systems," Proc. Workshop Future Directions in Cyber-Physical Systems Security, Dept. Homeland Security, 2009; chess.eecs.berkeley.edu/pubs/601.html.
9. Mirza Abdur Razzaq "Security Issues in the Internet of Things (IoT): A Comprehensive Study" Department of Computer Science Shah Abdul Latif University Khairpur, Pakistan.
10. J. Sathish Kumar "A Survey on Internet of Things: Security and Privacy Issues "Department of Computer Engineering, SVNIT.