REVIEW ON SECURITY ISSUES IN IOT

Ganesh[1], Sumedh[2],Vishal[3],Suraj[4]

BE students

Department of Electronics and Telecommunications

KC College of Engineering and Management Studies Research, Thane(E)

Abstract—Internet of Things (IoT) is an emerging and interesting platform to work on. IoT is used to connect the real world with the digital world. There is an intermediate server that is used for connectivity and transferring and storing of data. Now when data comes in action there is a need of enhanced security to keep the data safe and secured. In this paper various security issues and challenges are discussed.

Keywords—IoT Security, Privacy Issues, Authentication, Cryptography, server, safety.

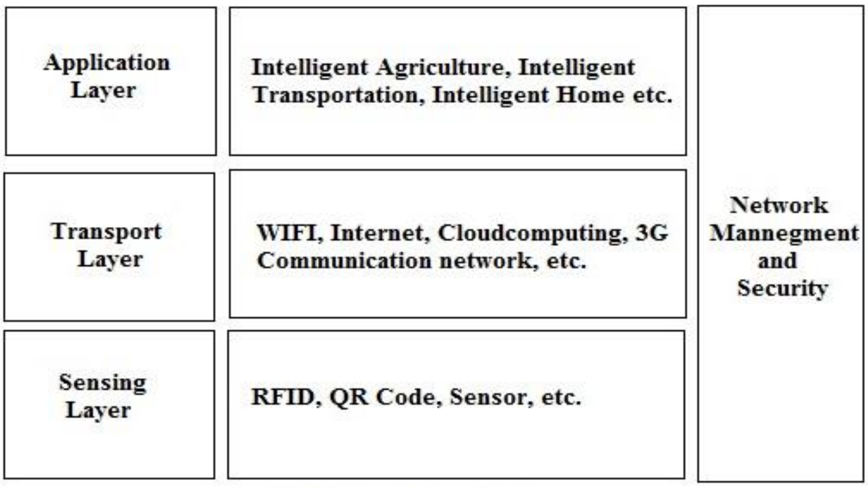
I. INTRODUCTION

With the recent spread of IoT the numbers of network connected devices are increasing rapidly. The connected devices are not limited to information devices they can be a medical equipment, vehicle, power stations and home appliances. When one of the devices is infected by malware kind of viruses, it can become starting point for the spread of infiltration that could affect to the system that should be protected. There are vulnerabilities in the communication software of devices such as PCs and surveillance cameras are targeted to enable unauthorized accesses. If one thing can prevent IoT from transforming the way we live and work, it will be a breakdown in security. While considering security of IoT there are number of issues are present that can be solved by using encryption techniques. This internet connectivity also leads to the development of Cyber-Physical Systems (CPS) to interlink the physical and cyber world. There are various technologies that come under this CPS namely IoT, advanced robotics, autonomous or near-autonomous vehicles and automation of knowledge work.

II. BASIC IOT ARCHITECTURE

The general network architecture is divided into three layers: sensing layer, transport layer and application layer

In this the layers the first layer sensing layer is also called as perception layer. This layer is responsible for collecting the information and gathering the physical parameters. Data acquisition and collaboration is the main feature of this layer. It has various sensors namely temperature and humidity sensors, GPS, RFID label, camera, etc. This layer consist of mainly two sections: field devices which possess sensing, computing and communication capabilities and field networks obtained by the interconnection of these devices. This layer aims at sensors with low power consumption and high performance. RFID technology and sensor network technologies are the key technologies employed in this layer.



IoT Network architecture

Fig.1

The second layer is Transport layer. The Transport layer concentrates on a variety of networks. It consists of the internet, 3G communication networks and the cloud computing platform. It is considered as the center of the whole network. The interface between users and IoT is achieved using the application layer. It is the upper layer in the IoT architecture which is capable of providing services to different sections or firms such as automobile, healthcare, education, logistics, agriculture, insurance, media, environmental monitoring etc. This layer makes use of data mining, cloud computing, fuzzy recognition and other intelligent computing technologies to process magnanimous data and provide effective information.

The third layer is Application layer. The Application is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, smart health, intelligent agriculture and intelligent Transportation.

III.PROTOCOLS IN IOT

Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF) and internet society are the principal technical development and standards setting bodies of Internet of Things. The protocol stack designed by them. IEEE 802.15.4.supports low energy communications at physical (PHY) and medium access control (MAC) layer.

It is the base for IoT communication protocols for the above layers. It supports a data rate of 250 kbps and the range of distance is about 10 meters.

Layer	Protocol
Application	CoAP
Network/Routing	IPv6, RPL
Adaptation	6LoWPAN
MAC and PHY	IEEE802.15.4

IoT Protocols

Fig.2

IEEE 802.15.4e addendum supports time synchronized multi hop communication at MAC layer. IEEE 802.15.4 uses at most 102 bytes for data transmission. IPv6 is having more address space than IEEE 802.15.4. So the IPv6packets are made to transmit over IEEE 802.15.4. This led to the development of IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN). It helps in packet fragmentation and reassembly. Routing Protocol for Low power and Lossy Networks (RPL) are used for routing over 6LoWPAN. Communications at application layer is supported by a protocol called as Constrained Application Protocol.

IV.SECURITY ISSUES IN THE IOT

The security requirements of IoT mainly focus on the Confidentiality, integrity, authentication, no repudiation, Availability, resilience, privacy, anonymity, liability and trust. Availability and resilience are to be given importance if the network is prone to internet originated attacks like Denial of Service (DOS). Direct sequence spread spectrum (DSSS), and Chirp spread spectrum (CCS) modulation methods are used to achieve reliability in the PHYSICAL layer. IEEE 802.15.4 security is achieved at the MAC layer with the help of efficient symmetric cryptography. In order to encrypt data, symmetric block ciphers are used in both hardware and software. Encryption and decryption techniques help in achieving confidentiality. Data integrity is achieved through message integrity codes (MIC). Availability is ensured by using Intrusion Detection System (IDS) and firewalls. Integrity-protected timestamps, sequence numbers, etc. are used for replay protection. The security issues are described by considering the different layers of IoT. In sensing layer, the RFID and wireless sensor network security threats are the major problem makers. The RFID security threats mainly include copying an identical RFID label (also known as replication attack), leakage of location information of RFID tags and users, channel blocking attack in which attacker occupies the channel long time, forgery attack, impersonation attack in which attacker fake as a legitimate reader and tampering attack where the information is modified after listening to it and then sends to the other node. Fake node and malicious data, DOS, timing attack and side channel attack are other security threats. External attack and link layer security, Witch attack, HELLO flooding attack, wormhole and sewage pool, Selective forwarding attack, broadcast authentication and flooding etc are some of the possible attacks in the wireless sensor networks. In network layer, traditional Security Problems like illegal access networks, eavesdropping information, confidentiality damage, integrity damage, DoS attack, Man-in-the middle attack, virus invasion, exploit attacks, etc. may occur. Security, interoperability, and coordination of network are affected as a result of heterogeneity of the networks.

This leads to compatibility problem which forms another security threat to network layer. Privacy disclosure is another problem in this layer. DOS attack, DDOS attack, impersonation attack, middleman attacks, cross heterogeneous network attacks etc. are the common issues in the transport layer. When considering the application layer, the major issues occurs while selecting the same database content according to the different access, providing user privacy information protection, solving the leakage of information tracking problem, taking the computer forensics, destroying the computer data, protecting electronic products and software intellectual property etc. Physical methods or code mechanisms or a combination of both the methods are used for providing the RFID security. Data encryption, blocker tag, tag frequency modification, jamming, kill order policy, etc. are the commonly used physical methods whereas the code mechanisms include the design of protocols for RFID node security. Hash Lock protocol, LCAP, Hash Chain and re-encryption protocol are the RFID security protocols. Methods like key distribution policies, intrusion detection mechanisms, security routing protocols, etc. are also employed to achieve the security. Specific authentication cohesive mechanism, the end-to-end authentication and key agreement mechanism, PKI (Public Key Infrastructure), WPKI for wireless, Security routing, Intrusion detection, etc. are used to tackle the security problems in the network layer. It also describes about the security measures in application layer. Symmetric key cryptosystem, public key cryptosystem and certification transfer technology are used to achieve authentication and key agreement in the heterogeneous network. Fingerprint technology, digital watermarking, anonymous authentication, threshold cryptography, etc. are employed to attain the security of private information. The necessary security services in IoT are confidentiality, data integrity, source integrity or authentication, availability and replay protection. Encryption/decryption techniques help in achieving confidentiality. Data integrity is achieved through message integrity codes (MIC). Availability is ensured by using IDS and firewalls. Integrity protected timestamps, sequence numbers, etc. are used for replay protection. Datagram transport layer security (DTLS) and IPSec are the security protocols used to attain security in the transport layer and network layer respectively. Malicious activities in the network can be detected using IDS and unauthorized access can be blocked by the use of firewalls. We have to provide security to communication, networks and data in the IoT.

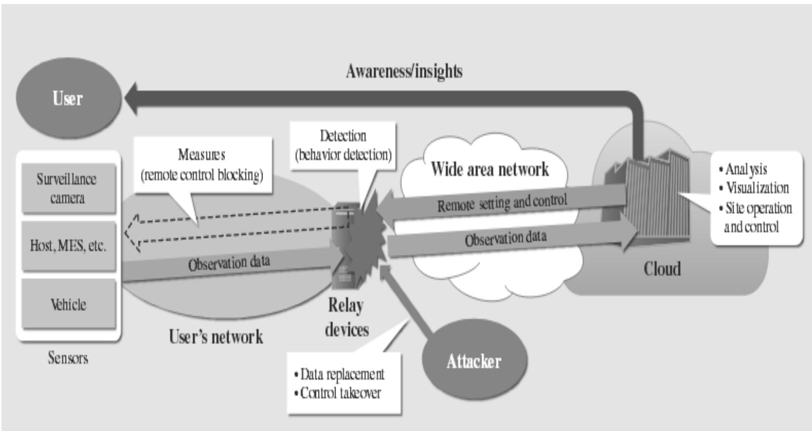


Fig.3

V. SECURITY CHALLENGES

1. Interoperability: Relevant security solutions should not prevent the functionality of interconnected heterogeneous devices in IoT network system.
2. Resource constraints: In IoT architecture, most of nodes lack of storage capacity, power and CPU. They generally use low-bandwidth communication channels. Hence, it is unable to apply some security techniques such as frequency hopping communication and public key encryption algorithm. Setup of security system is very difficult under these circumstances.
3. Data volumes: Although some IoT applications use brief and infrequent communication channels, there are considerable number of IoT system such as sensor-based, logistics and large scale system that have potentials to entail huge volume of data on central network or servers.
4. Privacy protection: Since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well.
5. Privacy protection: Since a great number of RFID systems are short of suitable authentication mechanism, anyone can tracks tags and find the identity of the objects carrying them. Intruders can not only read the data, but can also modify or even delete data as well.
6. Scalability: The IoT network consists of a large number of nodes. The proposed security mechanism on IoT should be scalable.
7. Autonomic control: Traditional computers need users to configure and adapt them to different application domains and different communication environments. However, objects in IoT network should establish connections spontaneously, and organize/configure themselves for adapting to the platform they are operating in. This kind of control also involves some techniques and mechanisms such as self-configuring, self-optimizing, self-management, self-healing and self-protecting.

VI. CONCLUSION

The network architecture and protocols of IOT are discussed in this paper. The security threats in different layers are studied. The issues are different in different layers. In-order to achieve security, different measures like encryption and decryption, key mechanisms, Security protocols, end to end authentication, etc. are performed. A study on the existing research works has been done.

REFERENCES

[1] Eleonora Borgia, “The Internet of Things vision: Key features, applications and open issues”, Institute of Informatics and Telematics (IIT), Italian National Research Council (CNR), Italy.

[2] Xu Xingmei, Zhou Jing,Wang He, “Research on the Basic Characteristics, the Key Technologies, the Network Architectureand Security Problems of the Internet of Things”, 2013 3rd International Conference on Computer Science and Network Technology.

[3] Jorge Granjal , Edmundo Monteiro , Jorge Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues”, IEEE Communications Surveys & Tutorials.

[4] “The Internet of Things: Challenges & Security Issues”, Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary, 2014 IEEE

[5] D Cavalcanti, S Das, J Wang, K Challapali, “Cognitive radio based wireless sensor networks”, in Proceedings of 17th International Conference on Computer Communications and Networks, vol. 1. St. Thomas, U.S. Virgin Islands, pp. 1–6, 2008.

[6] Kai Zhao, Lina Ge, “A Survey on the Internet of Things Security”, 2013 Ninth International Conference on Computational Intelligence and Security.

[7] Md. AlimulHaque Md. FaizanuddinN. K. Singh, “A Study of Cognitive Wireless Sensor Networks: Taxonomy of Attacks and Countermeasures”, World Applied Programming, Vol (2), Issue (11), November 2012. 477-484
[8] Shahid Raza, “Lightweight security solutions for the internet of things”, 2013, School of Innovation, Design and Engineering, Swedish Institute of Computer Science.
[9] Teemu Savolainen, Jonne Soininen, Bilhanan Silverajan, “IPv6 addressing strategies for IOT”, IEEE Sensors Journal, Vol. 13, No.10, October 2013.
[10] “Datagram Transport Layer Security Version 1.2”, RFC6347, September 2012.
[11] PavanPongle, GurunathChavan, “A Survey: Attacks on RPL and 6LoWPAN in IOT”, International Conference on Pervasive Computing (ICPC), 2015 IEEE.Kasinathan, et al. "Denial-of-Service detection in 6LoWPAN based internet of things", WiMob, 2013 IEEE 9th International Conference.