International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

# A REVIEW ON SECURITY OF INTERNET OF THINGS

**Dr. V. Harsha Shastri**
*Department of Computer Science, Loyola Academy Degree and P.G College, Alwal, Telangana (India)*

**ABSTRACT**: *The Internet of Things (IoT) can be defined as a global network which enables monitoring and control of the physical environment by collecting, processing and analysing the data generated by sensors or smart objects. The ability to connect, communicate with, and remotely manage an incalculable number of networked, automated devices via the Internet is becoming pervasive, from the factory floor to the hospital operating room to the residential basement. All the physical objects will be connected to the Internet and able to identify themselves to other devices. The technologies in IoT are such like RFID systems, sensor networks, and intelligence in smart objects. In the recent times, IoT has been a focus in the research area. IoT has its applications in many area including mobile, health care, security and many more. The transition from closed networks to enterprise IT networks to the public Internet is accelerating at an alarming pace—and justly raising alarms about security. In every respect of life, we are relying on the intelligent, interconnected devices but we need to protect billions of such devices from intrusions and interference or threaten public safety. e that could compromise personal privacy Security and privacy are the key issues in the IoT. There are many challenges in the field of IoT with respect to security. Deeply analysing the security architecture and features, the security requirements are given. Various key technologies such as cryptography algorithms and challenges are outlined briefly.*

***Keywords: IoT, sensor networks, privacy, cryptography***

## I. INTRODUCTION

In the area of wireless communications, the term Internet of Things (IoT) was coined by Kevin Ashton in a presentation in 1998, has gained more and more attention in acdemia and industry[2]. We embed a short range mobile transceivers into an array of gadgest and items that are used daily, a new form of communication between people and things and between things themselves was enabled. The ability to code and track objects has allowed companies to become more efficient, speed up processes, reduce error, prevent theft and incorporate comple and flexible organizational systems through IoT.

The idea of IoT is that there are variety of things or objects such as like Radio frequencty Identification RFID tags, sensors, actuators, mobile phones areound us can be addressed uniquely are able to interact with each other and cooperate with their smart componenes to reach common goals[2].

By 2020[1], it is estimated that the number of connected devices is expected to grow exponentially to 50 billion. Devices grow every day and operational technologies are becoming the connected entities across the globe. The pharse Internet of Things come from two words i.e., the first word Internet and and the second word Things. The Internet is a network of networks that consists of millions of private, public, academic and so-on linked by collection of eletronic, wireless and optical networking technologies[3]. It uses the TCP/IP protocols for communication between networks. The Things can be any object or person which exists and is distinguishable from other in the real world. The objects need not be electronic devices or techincal products but it can be like food, clothing, furniture, land marksetc. It can be borth living and non-living things.

IoT faces more severe challenges in the domain of security. The following are the reasons:

1. The IoT can be connected to the internet through the traditional internet, mobile network and sensor networks.
2. Every thing will be connected to this internet.
3. These things will coomunicate with each other.

More digitally connected devices such as mobile phones, cars and other products have potential threats through hackers, attack vectors and cyber criminals. The number of connected devices increases and their usage becomes an important part of day to day life, security, confidential and individual safety issues will arise. We need to focus on the security issues like confidentiality, authenticity, and integrity of data in Internet of Things. Many security issues are seen to take up in the Internet of Things environment for sensitive information. Security of Personal information is a major concern in the Internet of Things environment. Through cloud services available data security is provided.

## II. SECURITY IN IOT.

IoT devices normally transfer information in the network. We need to consider the properties like identification, confidentiality, integrity and undeniability. The IoT can be applied to crucial areas like medical service and health care.

### A. Secure Architecture

In general, the IoT can be divided into four levels. Fig. 1 shows the level architecture of the IoT.

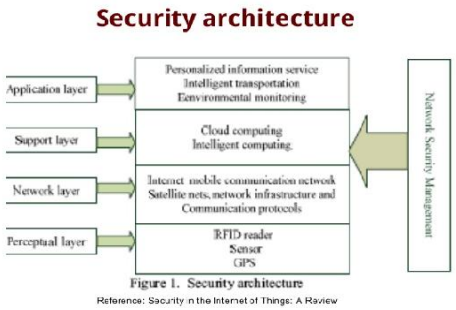


Figure 1. Security architecture
Reference: Security n the Internet of Things: A Review

The perceptual layer is known as recognition layer collects all kinds of information through physical equipment and identifies the physical world, the information about object properties, environmental condition etc and physical equipments include RFID reader, Zigbee, sensors, GPS and other equipment. The sensors is used for capturing and representine the physical world in digital world. Some

common attacks in this layer are: Node capture, malicious data, Denial of service attack, reply attack[4].

The network layer is responsible for reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization. The transmission of information is based on various networks like internet, mobile communication netowrk, satellite nets, wireless network, network infrastructure and communication protocols. These are essential to the information exchange between devices. This layer is responsible for routing and transfer information through the wireless technology such as wi-fi, bluetooth and infrared[7]. Some security problems are DoS attack, Man-in-the-middle attack, illegal access network, eavesdropping, confidentiality and integrity damage.

The support layer will set up a reliable support platform for the application layer. On this support platform all kind of intelligent computing powers will be organized through cloud and grid computing.

The application layer is the topmost and terminal level. They provide personalized services according to the need of the users. Users can access the IoT through this layer interface using television, PC or mobile device. Application layer has some security problems such as data security, cloud platform security, data protection and recovery etc. To solve the security problems of this layer, authentication and privacy protection are needed. Particularly, password management is very important for data security [1].

### B. Security features

At perceptual layer, the nodes are short of computer power and storage capacity. The freqeuency hopping communication cannot be applied and public key encryption algorithm is difficult to apply for security protection. We can also have other external attacks like denial of service that can bring new security probkems. The sensor data still need the protection for integirity, authenticity and confidentiality.

At the network layer we can have the man-in-the middle attack aand counterfeit attacks. Junk mail and computer virus alo pose a serious potential threat. These problems can create a large number of data when they are sent creating congestion.

We need to do a lot of data processing and decision at the network layer. Intelligent processing is limited for malicious information, so it is a challenge to improve the ability to recognize the malicious information.

In the application layer, there are different security needs for different application environment. Data sharing is that one of the characteristics of application layer which creates problems of data privacy, access control and disclosure of information[4,10].

### C. Security Requirements

According to the above analysis, we can summarize the security requirements for each level in the following as shown in fig 2:

a) Perceptual layer: Authentication is needed to prevent illegal node from accessing; data encryption is needed to protect the confidentiality of information when transmitted between the nodes; data encryption key is important well in advance.
b) Network layer: Authentication is a kind of mechanism to prevent a node from illegal access; confidentiality and integrity are of equal importance. Distributed denial of service attack is severe in IoT. Prevention of DDOS attack is solved in this layer.
c) Support layer: This layer needs a lot of application security architecture such as cloud computing and secure multiparty computation. We need a stronger security technology and antivirus.
d) Application layer: To solve the security problems we need authentication, key agreement across heterogenous network, privacy protection, and password management.

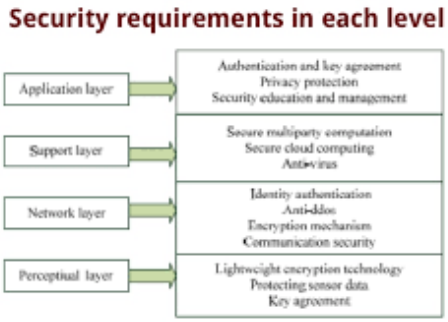


Fig 2: Security requirement in each level

## III. REVIEW OF LITERATURE

Chen Qiang et.al [5] discussed various security issues such as RFID tag security, wireless security, transmission security, privacy protection and information security. Researches on network security was investigated and a new security method for IoT was provided. A massive amount of IoT data needs to be processed and reliability of data and secuirty was highlighted.

Qi Jing et. al [6] analysed the security problems in IoT. The comparative analysis of secuirty issues in IoT and traditional network is performed. Security issues of RFID technology, WSN technology, RSN technology were discussed and the corresponding solutions were offered. The features of the given solutions were analyzed using the technology involved. Finally, an overall security architecture for IoT system was given.

Gupreet Singh Matharu et al. [7] described the general layer architecture and briefed several challenges in IoT such as robustness in connectivity, interoperability and standardization, naming and identity management, safety and security of objects, data confidentiality and encryption. Security issues related to all the four layers of the IoT architecture were discussed, analyzed and determined. Finally, the strategies for solving security issues were suggested.

Mahmud Hossain et al. [8] explored security challenges and open problems in IoT. The need for a systematic study of the security challenges in IoT was propounded. A detailed

analysis of IoT security challenges was done to bridge the gap in the existing scenario. A series of open problems in IoT security and privacy was provided. An overview of IoT architecture and interoperability between interconnected networks, the critical security problems and the mitigation methods in IoT were presented. Five major components of IoT ecosystem viz. IoT devices, coordinator, sensor bridge, IoT services and controller were examined to understand IoT security issues.

Jorge Granjal et al. [9] discussed various security issues in IoT and also surveyed existing protocols. Existing protocols were analyzed to offer security in communications between IoT devices. Several existing protocols were explored to enable security in physical (PHY), Medium Access Control (MAC) layers low-energy communications, network layer, routing, and application layer with CoAP. Possible ways to offer novel security mechanisms were provided based on security requirements.

Raja Benabdessalem et al. [10] explored different methods to address security and privacy issues. The security requirements viz. confidentiality, authentication, integrity, authorization, non-repudiation and availability in IoT were analyzed to ensure privacy, data protection and security. Discussion on various kinds of threats such as eavesdropping and denial-of-service attacks was made. Several cryptographic algorithms were scrutinized to ensure secure data communication between IoT devices.

Sye Loong Keoh et al. [12] focused on communication security for IoT, specifically the standard security protocols. Four modes namely NoSec, PreShared Key, Raw Public Key and Certificate based on the configuration of IoT device were described. Deployment of DTLS which is considered as the main security suite for IoT was done to provide security functionalities to the IoT devices.

## IV. CRUCIAL TECHNOLOGIES IN IOT

A detail research on encryption mechanism, communication security, protecting sensor data and cryptographic algorithms is provided.

### *A.* Encryption mechanism

In traditional network layer we adopt the by-hop encryption mechanism, in this way the information is encrypted in the transmission process, but the plain text needs to be maintained at each node through encryption and decryption process. Meanwhile in the traditional application layer encryption mechanism is end-to-end encryption, that is, the information only is explicit for the sender and the receiver, and in the transmission process and forwarding nodes it will be always encrypted.

### *B.* Communication Security

At first in communication protocols there are some solutions being established, these solutions can provide integrity, authenticity and confidentiality for communication. TLS/SSL is designed to encrypt the link in the transport layer, and IPSec is designed to protect security of the network layer, they can provide integrity, authenticity, and confidentiality in the each layer.

Communication security is often weak because the IoT devices have less processing power. Meanwhile in the IoT, the core network is always current or next generation Internet, most of the information will be transferred through internet.

### *C.* Protecting Sensor data

The integrity and authenticity of sensor data is of prime focus, confidentiality of sensor data is a lower demand because when an attacker can just place its own sensor physically near, he can sense the same values. So at the sensor itself the confidentiality need is relatively low.

Another major concern is the privacy. We should adopt the mechanisms to protect the privacy of human and objects in the physical world.

### *D.* Cryptographic algorithms

Several cryptographic algorithms are applied to internet security protocols as shown in the table 1.

TABLE 1. A SUITE OF CRYPTOGRAPHIC ALGORITHMS

| Algorithm | Purpose |
|---|---|
| Advanced encryption standard (AES) | Confidentiality |
| Rivest shamir adelman (RSA)/ Elliptic curve cryptography (ECC) | Digital signatures key transport |
| Diffie-hellman (DH) | Key agreement |
| SHA-1/SHA-256 | Integrality |

Usually, the symmetric encryption algorithm is used to encrypt the data for confidentiality such as Advanced Encryption Standard (AES) block cipher; the asymmetric algorithm is often used to digital signatures and key transport, the algorithm used is the Rivest Shamir Adelman (RSA). The diffie- hellman key exchange algorithm is used for key agreement. SHA-1 and SHA-256 will be used for key integrity.

To implement these cryptographic algorithms available resources are necessary such as processor speed and memory.

## V. KEY TECHNOLOGIES IN IOT

### *A.* Identification, sensing and communication technologies

Identification methods are electronic product code(EPC) and ubiquitous code (uCode). In IoT, object's address refers to the address within the communication network that includes IPv6 and IPv4. RFID technology is the main factor in the embedded communication technology. It can be used to monitor objects in real time. Sensing refers to gathering of the data from IoT objects within the same network and sending it to the database or cloud.

Objects can interact with the physical environment either passively or actively (performing sensing operations or performing actions) [14]. The IoT sensors can be smart sensors, actuators or wearable sensing devices [13]. IoT communication technologies connect heterogeneous objects together to deliver specific smart services. The communication protocols used by IoT are Bluetooth, Wi-Fi etc.

### *B.* Middleware

In IoT, a middle ware is a software layer or a set of sub layers interposed between the technological and the application levels. Embedded middleware are modules and operating

environments which support different communication protocols [11]. It is responsible for providing services to the customers, besides ensuring interoperability, scalability and abstraction. Also, it authenticates the user to provide more secure environment along with efficient delivery of services [7].

### *C.* ZigBee

ZigBee is a wireless network protocol formulated by ZigBee Alliance. It is a two-way wireless access technology of close distance, low power consumption, low data rate, low complexity and low-cost. It is mainly suitable for automatic control and remote monitoring. ZigBee is highly reliable wireless data transmission network, which is similar to CDMA and GSM networks. ZigBee data transmission module is similar to the mobile network base station. ZigBee technology constitutes wireless data transmission network platform up to 65000 wireless data transmission modules [15]. ZigBee is widely used in home automation, digital agriculture, industrial controls, and medical monitoring.

### *D.* Cloud Computing

Cloud computing is the integrated product of traditional computer technology and network technology, such as grid computing, distributed computing, parallel computing and utility computing etc. [15]. In Internet of Things, there is a large scale, massive amount of data need to be processed. So the data processing capacity is in high demand. The data collected by IoT devices are stored in the cloud environment. Integrated IoT and cloud computing applications enable the creation of smart environments such as smart cities, smart home etc.

## VI. CONCLUSION

In the last few years, IoT is an emerging domain and is of significant interest. There are several challenges and issues in this area. The layers in IoT are discussed clearly. We have analysed the characteristics and security requirement of all the layers including support, network, perceptual and application layer.

## VII. ACKNOWLEDGMENT

The author would like to acknowledge that the paper would be incomplete with out the guidance supported by the Black Buck company. The effort did not go into vain had it not been the members of the department who motivated in writing the article.

## VIII. REFERENCES

[1] Hui Suoa, Jiafu Wana and Caifeng Zoua, Jianqi Liua, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, 2012, pp. 649-651.
[2] D.Giusto, A.Lera, G.Morabito and L.Atzori, editors, The Internet of Things, Springer 2010.
[3] E.Nagai, K.Moon, F.Riggins and C.Yi, RFID research: An academic literature review (1995-2005) and future research directions, International Journal of Production Economics, 112:510-520,2008.
[4] Kai Zhao and Lina Ge, "A Survey on the Internet of Things Security", IEEE, International Conference on Computational Intelligence and Security, 2013, pp. 663-667.
[5] Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, "Research on Security Issues on the Internet of Things", International Journal of Future Generation Communication and Networking, 2013, pp.1-9.
[6] Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qui, "Security of the Internet of Things: perspectives and challenges", Springer, Wireless Networks, vol. 20, Iss.8, pp. 2481–2501.
[7] Gurpreet Singh Matharu,Priyanka Upadhyay and Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues", IEEE, International Conference on Emerging Technologies (ICET), 2014, pp.54-59
[8] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", IEEE World Congress on Services, 2015, pp. 21-28.
[9] Jorge Granjal, Edmundo Monteiro and Jorge Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communication Surveys and Tutorials, 2015, vol.17, no.3, pp. 1294 – 1312.
[10] Raja Benabdessalem, Mohamed Hamdi and Tai-Hoon Kim, "A Survey on Security Models, Techniques and Tools for the Internet of Things", International Conference on Advanced Software Engineering & Its Applications, 2014, pg. 44-48.
[11] Xu Xiaohui, "Study on Security Problems and Key Technologies of the Internet of Things" International Conference on computational and Information Sciences, 2013, pp. 407-410.
[12] Sye Loong Keoh, Sandeep S.Kumar and Hannes Tschofenig, "Securing the Internet of Things: A Standardization Perspective", IEEE Internet of Things Journal, 2014, pp.265-275.
[13] Ala Al-Fuqaha, Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications", IEEE Communications Surveys & Tutorials, 2015, vol.17, Iss. 4, pp. 2347-2376.
[14] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: Vision, Applications and Research Challenges", Elsevier Ad Hoc Networks, 2012, pp.1497-1516.
[15] Wang Rui1, Wang Jingu and Wang Na, "Analysis of key technologies in the Internet of things", International Conference on Material, Mechanical and Manufacturing Engineering (IC3ME), 2015, pp. 938-941
[16] Xian-Yi Chen, Zhi-Gang and Jin, "Research on Key Technology and Applications for Internet of Things", Elsevier International Conference on Medical Physics and Biomedical Engineering, 2012, pp.561-566.