SECURITY ON IOT: A REVIEW

Ritesh Kumar Thakur and Rajesh Kumar Tiwari

ABSTRACT

Now a days, we see that the Things are connected with internet by using Internet of Things (IoT) and became very useful in different area like Health, Homes, Agriculture, Transporting and so on. The internet of things (IoT) refers to the interconnection via the internet of computing devices embedded in everyday object enabling them to send and receive data. Security and Privacy are the key issue for the IoT application and still face some huge challenges. The data collected from the lot sensors contain the large amount of private information which needs to be preserved.

***Index Terms**—Internet of things; security; privacy; confidentiality; challenges; sensor; Availability; Authentication; Heterogeneity; Key Management*

Reference to this paper should be made as follows:

***Ritesh Kumar Thakur, Rajesh Kumar Tiwari (2020), '**SECURITY ON IOT: A REVIEW", Int. J. of Electronics Engineering and Applications, Vol. 8, No.2, July-Dec 2020, pp-40-48, DOI-10.30696/IJEEA.VIII.II.2020.40.48.*

Biographical notes:

***Ritesh Kumar Thakur** working as a Asst. Professor in Jamshedpur Women's College, Jamshedpur, Jharkhand, India.*

***Rajesh Kumar Tiwari** completed M. Tech (CSE) and PhD in the field of data security form Birla Institute of Technology, Ranchi in the year 2010. Currently, he is working as Professor and Dean of Academic Affairs at RVS College of Engineering and Technology, Jamshedpur, Jharkhand, India. His research is focused on data security, cloud computing, database management system, and Machine Learning.*

INTRODUCTION

The word, Internet of Things (IoT) was first proposed in 1998 and denotes to inimitably recognizable object, things and their simulated representation in an internet. The main component of IoT is sensor, equipment, data processing, feedback and cloud are involved in any IoT application. Additional component are privacy and security. The IoT ranges the internet with the help of mobile network, Bluetooth sensor network and so on.

All Things are connected with the internet and they communicate with each other. For this communication, privacy and security problem will arise. so there is a need for research in the area of authenticity, integrity, confidentiality of data called in the IoT. Nowadays, the IoT as a buzzword is widely known, subsequent industry applications related to the IoT will arise, for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications [1].

At this stage, the ambient intelligence and autonomous control are not part of the original concept of IoT. With the development of advanced network techniques, distributed multi-agent control and cloud computing, there is a shift integrating the concepts of IoT and autonomous control in M2M research to produce an evolution of M2M in the form of cyber-physical System. Cyber-Physical System mainly focuses on intelligent zing interaction, interactive applications, distributed real-time control, cross layer optimization, cross-do main optimization, etc. Therefore, some new technologies and methodologies should be developed to meet the higher requirements in terms of reliability, security and privacy [2].

2. RELATIONSHIP TO M2M AND THE INTERNET OF EVERYTHING

Machine to machine(M2M) involves direct communication between devices without human intervention. This communication can be over any channel, whether wired or wireless, and the number of technologies, standards, and protocols for communication is large and growing. Communication may occur through a network, including cellular networks (GSM, 3G, 4G), or directly between devices (without going through a base station, intermediary, or access point) in a point-to-point manner, each having a different attack surface. Some of the key communication technologies include Wi-Fi, RFID, Dedicated Short Range Communication (DSRC), Bluetooth, Bluetooth Low Energy (more recently referred to as Bluetooth Smart), NFC, and Zigbee [13].

3. SECURITY ATTENTION ON IOT:

The security of information and network should be equipped with these properties such as identification, confidentiality, integrity and undeniability. Different from internet, the IoT will be applied to the crucial areas of national economy, e.g., medical service and health care, and intelligent transportation, thus security needs in the IoT will be higher in availability and dependability.

- **SECURITY ARCHITECTURE**

In Security architecture of IoT there has four layer through which security manages.

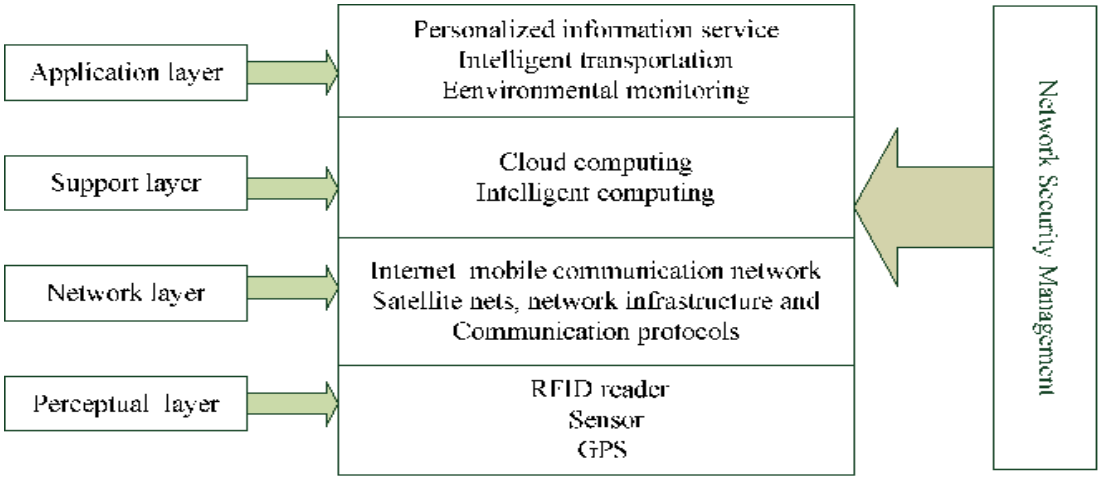


Figure 1. Security architecture

- Perceptual Layer: This layer is the basic layer is also called as a recognition layer,which gather all types of information with the help of physical equipment and identifies the external world. The information from them includes the properties of the object or the things, environmental condition and different physical equipment include RFID reader, GPS, all kinds of sensors and other equipment. There are different component involved, the key component in this layer is the sensor that are used for capturing and representing the physical world.
- Network Layer: The second layer in the security architecture is network layer. This layer collect data from the previous layer. This is responsible for the dependable broadcast of data and information from previous layer, initially handling of the data collected through the sensor cataloguing and polymerization. In this layer, the data broadcast is trusted on numerous basic network which could be one of the mobile communication networks, wireless network, satellite nets etc.
- Support Layer: This is third layer in the security architecture. In this layer will set up a dependable platform for the application layer. The Grid and cloud computing are mostly used for all kind of intelligent computing power. It supports layer helps merging application layer upward network and network layer downward.
- Application layer: This is the topmost layer in security architecture. this layer delivers the personalized services based on the user needs. application layer helps user to access the internet of thing (IoT)through the interface using personal computer, mobile equipment, television etc.

B. SECURITY FEATURES OF IOT

- The security challenges of IoT can be broadly divided into two classes; Technological and Security objection [5]. The technological challenges come due to the different and pervasive nature of IoT devices, while the security provocation is related to the ethics and usefulness that should be implemented to attain a secure network. Security should be included in IoT throughout the growth and running lifecycle of all IoT devices and

hubs [6].Given below are the security principles that should be followed to achieve a secure interaction framework for the people, software, processes, and things in an IoT.

- Confidentiality- It is important to ensure that data is secure and only available to approved users. Integrity. The IoT is based on interchanging data and information between many various types of devices, which is why it is important to confirm accuracy of the data; that data is being comes from the right sender as well as to make sure that the data is not modified with during the process of transmitting due to intended or unintended interference.

- Availability. The vision of IoT is to join as many smart devices as possible. The users of the IoT should have all the data visible whenever they need it. However, data is not the only modules that is used in the IoT; devices and services must also be approachable and accessible when needed in a timely fashion in order to achieve the predictions of IoT.

- Authentication-Each object in the IoT must be clever to clearly identify and authenticate other objects. However, this process can be testing because of the nature of the IoT; many entities are mixed up (devices, people, services, service providers and processing units). In addition, sometimes objects may need to communicate with other objects for the first time [7][11]. Because of all this, a method to mutually authenticate entities in every communication in the IoT is required.

- Lightweight Solutions-All of the security intentions considered earlier is not peculiar to IoT, although it may add special characteristics and constraints to each of them. However, in general confidentiality, integrity, availability and authentication are treated as basic intention in every computer or network security.

- Heterogeneity- The IoT aims at connecting device to device, human to device, and human to human, thus it implements connection between different things and networks [5]. One more challenge that must be considered in IoT is that the environment is always changing (dynamics), at one time a device might be linked to a completely distinctive set of devices than in another time. And to ensure security optimal cryptography system is needed with an adequate key management and security protocols [18].

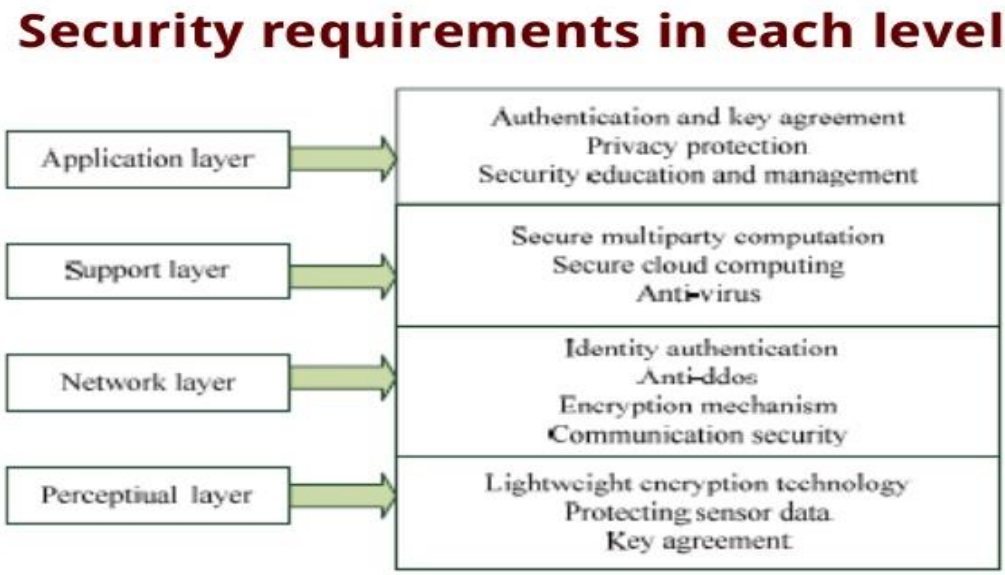
- Policies-There must be policies and standards to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to accomplish such plan is needed to assure that every entity is implementing the standards. Service Level Agreements (SLO) must be clearly identified in every service involved. The enforcement of such guidelines will recommend trust by human users in the IoT model which will hereafter result in its growth and scalability.

- Key Management Systems- In IoT, the devices and IoT sensors need to interchange some encryption materials to achieve confidentiality of the data. For this intention, there needs to be a lightweight key management system for all structures that can enable trust

between different things, and can deliver keys by consuming devices' minimum capacity [12].

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.



- Perceptual Layer: At first node authentication is necessary to prevent illegal node access; secondly to protect the confidentiality of information transmission between the nodes, data encryption is absolute necessity; and before the data encryption key agreement is an important process in advance; the stronger are the safety measures, the more is consumption of resources, to solve this problem, lightweight encryption technology becomes important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol. At the same time the integrity and authenticity of sensor data is becoming research focus, we will discuss this question more in-depth in the next section.

- Network Layer: In this layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, and it is the premise of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrality mechanism. Besides distributed denial of service attack (DDoS) is a common attack method in the network and is particularly severe in the internet of thing, so to prevent the DDOS attack for the vulnerable node is another problem to be solved in this layer.

- Support Layer: Support layer needs a lot of the application security architecture such as cloud computing and secure multiparty computation, almost all of the strong encryption algorithm and encryption protocol, stronger system security technology and anti-virus.

- Application Layer: To solve the security problem of application layer, we need two aspects. One is the authentication and key agreement across the heterogeneous network, the other is user's privacy protection. In addition, education and management are very important to information security, especially password management [3,4].

4. RESEARCH ASSPECTS

A. Encryption Mechanism: In the IoT network layer and application layer connect so closely, so we should choose between by-hop and end-to-end encryption. If we adopt by-hop encryption, we can only encrypt the links which need be protected, because in the network layer we can apply it to all business, which make different applications safely implemented. In this way, security mechanism is transparent to the business applications, which gives the end users convenience. Currently, IoT is developing in its primary phase, and the research of safety mechanism is in the blank in the practice, so we have a long way for the research of this domain.

B. Communication Security: At first in communication protocols there are some solutions being established, these solutions can provide integrity, authenticity, and confidentiality for communication, for example: TLS/SSL or IPSec. 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. And the needs of privacy also have been come up with but unfortunately are not in wide use. Then communication security mechanisms are also seldom applied nowadays. Because in the IoT small devices are less processing power, this leads that communication security is often weak. Meanwhile in the IoT, the core network is always the current or next-generation Internet, most of the information will be transmitted through the Internet. So DDoS still exists and is a very severe problem. These botnets and DDoS attacks will destroy the availability of communication. When lager-scale or organized DDoS attacks happen, how to do the disaster recovery is highly significant, so we need pay more attention to researching better preventive measures and disaster recovery mechanisms [8].

C. Protecting Sensor Data : The integrity and authenticity of sensor data is becoming research focus, and 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 [8]. The other main research target in sensors is privacy, and privacy is also a major problem. We should adopt the mechanisms to protect the privacy of humans and objects in the physical world. Most times people are often unaware of sensors in their life, so we need to set up regulations to preserve the privacy of people. In the literature [9], several guidelines are given to solve this problem in the design phase: at first users must know that they are being sensed, the second users must be able to choose whether they are being sensed or not, the third users must be able to remain

anonymous. When the user has no realization of these guidelines, that regulations must be made [8].

D. Cryptographic Algorithms : So far there is a well-known and widely trusted suite of cryptographic algorithms applied to internet security protocols .Usually the symmetric encryption algorithm is used to encrypt data for confidentiality such as the advanced encryption standard (AES) block cipher; the asymmetric algorithm is often used to digital signatures and key transport , frequently-used algorithm is the rivest shamir adelman (RSA); the diffie-hellman (DH) asymmetric key agreement algorithm is used to key agreement; and the SHA-1 and SHA-256 secure hash algorithms will be applied for integrality. Another significant asymmetric algorithm is known as elliptic curve cryptography (ECC), ECC can provide equal safety by use of shorter length key, the adoption of ECC has been slowed and maybe be encouraged recently [10]. To implement these cryptographic algorithms available resources are necessary such as processor speed and memory.

5. MAJOR FUNCTIONALITIES

The security related solution may be embedded when it comes to IoT. There have 10 major functionalities which can help to solution of the security problem on IoT

- The microcomputer unit in the IoT System carries the firmware and can be advanced to deliver improved services or for a security patch to overcome the threat.
- Access limitation and usage of public network during the pairing stage need secured channel. A message channel like wifi, Zigbee, Bluetooth, and near field communication are usually involved in this stage.
- Binding helps to configure the things after the pairing Wifi, SSID and password helps to connect to the internet .An appropriate protocol is followed while binding the user and the thing.
- In case of a local or private network the controller can link to a Port and during this process user authentication is must before further action.
- Only after authentication the controller can direct command for things control that are present in the system.
- Sometimes if the controller is on the publicly available internet and not on private network ,then cloud services are used for authentication.
- And if the controller is not on local network then the control of things also happens through cloud service only.
- During this remort authentication process cloud has to relay the authentication along with the control message between different thing present in the IoT system and the controller.
- Big data analytics on the data can be processed in the cloud.
- Abnormal behavior can be notified to the user and this include too many attempts

6. CONCLUSION

Authentication and identification in IoT systems is fundamental for security and privacy. Obviously, systems based upon biometric identification, possibly combined with a token, may prove advantageous compared to existing systems, but care must be taken to ensure that the system is secure yet frictionless. this emerging domain for the IoT has been attracting the significant interest, and will continue for the years to come. In spite of rapid evolution, we are still facing new difficulties and severe challenges. In this literature, we concisely reviewed security in the IoT, and analyzed security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application laye

REFERENCES

[1] J. F. Wan, H. H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, 2011, 5(11): 1891-1908.

[2] M. Chen, J. F. Wan, and F. Li, "Machine-to-machine communications: architectures, standards, and applications," KSII Transactions on Internet and Information Systems, to appear, January 2012.

[3] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[4] C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac)

[6] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

[7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

[8] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.

[9] M. Langheinrich, "Privacy by design-principles of privacy-aware ubiquitous systems," In Proc. of Ubicomp, pp. 273-291, Oct. 2001.

[10] T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[11] X. Li et al., "A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things," vol. 5, no. 3, pp. 1606–1615, 2018

[12] K. W. Kim, Y. H. Han, and S. G. Min, "An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks," Sensors (Switzerland), vol. 17, no. 10, pp. 1–14, 2017.

[13] B. L. Parne, S. Member, S. Gupta, and S. Member, "SEGB : Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE / LTE-A Network," vol. 6, 2018.