Internet of Things (IoT): Security Perspective

Sunilkumar Malge, Pallavi Singh

ASM Institute of Management & Computer Studies (IMCOST), Thane, Maharashtra, India

***How to cite this paper*:** Sunilkumar Malge | Pallavi Singh "Internet of Things (IoT): Security Perspective" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1041-1043, URL: https://www.ijtsrd.com/papers/ijtsrd24010.pdf

IJTSRD24010

ABSTRACT

In the past decade, internet of things (IoT) has been a focus of research. It makes more intelligent to core element of modern world such as hospitals, cities, organizations, and buildings. Usually, IoT has four major components including sensing, information processing, applications and services, heterogeneous access and additional components e.g. Security and privacy. In this paper, we are presenting security perspective from the perspective of layers that comprises IoT. In this we focus on the overview of IoT security perspective.

Keywords: *Internet of Things, Security, Privacy, Confidentiality, Cryptography Algorithms, Security Attacks*

I. INTRODUCTION

Internet of Things (IoT) enables various devices to interact with each other via Internet. This ensures the devices to be smart and send the information to a centralized system, which will then monitor and take actions according to the task given to it.IoT can be used in many domains such healthcare, transportation, entertainment, power grids and smart buildings. IoT is expected to act as a catalyst for the future technological innovations and its use is expected to rise exponentially over the coming years.

According to security perspective, the IoT will be faced with more severe challenges. E.g. (1) The IoT extends the 'internet' through the traditional internet, sensor network and mobile network and so on, (2) every 'thing' will be connected to this 'internet', and (3) these 'things' will communicate with each other. Therefore, the new security and privacy problems will arise.Here; we pay more attention to the research issues for confidentiality, integrity, and authenticity of data in the IOT.

II. Core Layers of IoT

In general, the IoT can be divided into four key levels.

1. Perception Layer:

The most basic level is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical equipment and identifies the physical world, the information includes object properties, environmental condition etc.; and physical equipment include RFID reader, all kinds of sensors, GPS and other equipments.The key component in this layer is sensors for capturing and representing the physical world in the digital world.

2. Network Layer:

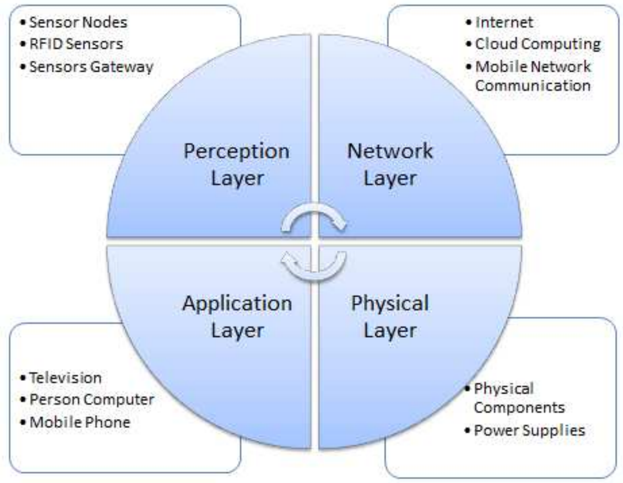
The second level layer is Network layer. Network layer is responsible for the reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization. In this layer the information transmission is relied on several basic networks, which are the internet, mobile communication network, wireless network, satellite nets, network infrastructure and communication protocols are also essential to the information exchange between devices.

3. Physical Layer:

The third level layer is physical layer. Physical 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 network grid and cloud computing. It plays the role of combining application layer upward and network layer downward.

4. Application Layer:

The application layer is the topmost and terminal level. Application layer provides the personalized services according to the needs of the users. Users can access to the internet of thing through the application layer interface using of personal computer, mobile equipment and television so on.



III. Security in IoT:

A. Security Features

1. Perceptual Layer:

Usually perceptual nodes are less of storage capacity and computer power as they are simple as well as with less power. So, it is not able to apply frequency hopping communication and public key encryption algorithm to security protection. As it is very difficult to set up security protection system. Meanwhile attacks from the external network such as deny of service also will bring new security problems. Apart from this sensor data still need the protection for confidentiality, integrity, authenticity.

2. Network Layer:

Although the core network has complete ability of protection security, but Man-in-the-Middle Attack and counterfeit attack still exist, Along this , congestion can be caused huge number of data sending. Therefore security mechanism in this level is very important to the IoT.

3. Support Layer:

Do the mass data processing and intelligent decision of network behavior in this layer, intelligent processing is limited for malicious information, so it is a challenge to improve the ability to recognize the malicious information.

4. Application Layer:

In this level different security applied for different application environment. The major characteristic of Application layer is data sharing which harms data privacy, access control and disclosure of information.

B. Security Requirements:

1. 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.

2. Network Layer:

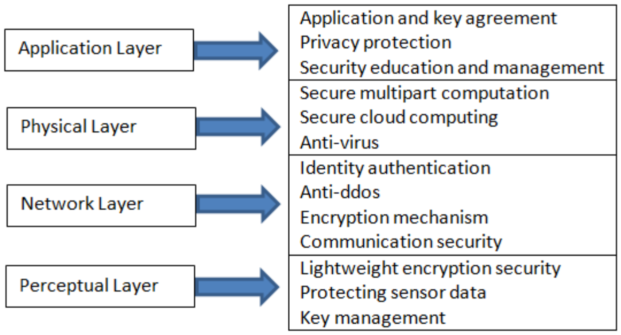
In this layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, and it is the premise of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrity 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.

3. 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.

4. 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. In summary security technology in the IoT is very important and full of challenges. In other hands laws and regulations issues are also significant, we will discuss this problem in the following.



IV. Technology used for security purpose in IoT

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. In the meantime this brings the features of the by-hop full play, such as low latency, high efficiency, low cost, and so on. However, because of the decryption operation in the transmission node, using by-hop encryption each node can get the plaintext message, so by-hop encryption needs high credibility of the transmission nodes.

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.

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. 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, 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.

D. Cryptographic Algorithms:

So far there is a well-known and widely trusted suite of cryptographic algorithms applied to internet security protocols such as table. 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. To implement these cryptographic algorithms available resources are necessary such as processor speed and memory. So how to apply these cryptographic techniques to the IoT is not clear, we have to make more effort to further research to ensure that algorithms can be successfully implemented using of constrained memory and low-speed processor in the IoT.

Algorithms	**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

V. Conclusion

In the last few years, 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 layer. Then, we discussed the research status in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm. At last we summarize several challenges. All in all the development of the IoT will bring more serious security problems, which are always the focus and the primary task of the research.

VI. References

[1] https://www.researchgate.net/publication/301281714_Security_in_Internet_of_Things_Challenges_Solutions_and_Future_Directions

[2] https://www.researchgate.net/publication/254029342_Security_in_the_Internet_of_Things_A_Review

[3] https://www.researchgate.net/publication/328261954_Study_on_Security_issues_in_Internet_of_Things