Analysis of security, problems, concerns, architecture and requirements of the Internet of Things

Keyvan Karamnejadi azar
Department of Electrical Engineering,Bu Ali Sina University,hamedan,Iran
Amir Shahraieni
Department of management,payame Noor University,Tehran,Iran
Omar Farshad Jeelani
ITMO University,Russia

Abstract

Internet of Things security is a subset of cybersecurity that focuses on protecting, monitoring, and remediating threats related to the Internet of Things, or the network of connected devices that collect, store, and share data over the Internet. IoT security challenges can be very controversial because many IoT devices are not built with strong security. The security risk in IoT is greater because the sensitivity of the data that IoT devices collect and store, as well as the systems they manage, is far greater than traditional personal network security strategies. Although the Internet of Things has become one of the most practical technologies today and is used in many different industries, few people are familiar with the architecture of the Internet of Things and how it works. The Internet of Things (IoT) industry, as one of the technologies of the fourth industrial revolution, has seen great growth in recent years and is expected to experience great growth in the coming years. Many businesses are already using this technology and have invested heavily in it. Nevertheless, the challenges of the Internet of Things can always put problems in the path of the advancement of this technology, and for this reason, familiarity with these challenges will be necessary and essential for managing and planning as well as possible for the advancement of this technology. In this article, the security, problems, architecture, requirements and encryption mechanism of the Internet of Things are examined.

Keywords: Internet of Things, encryption algorithms, architecture, problems of Internet of Things.

1. Introduction

Internet of Things security and focusing on each of the seven levels, as well as data exchange between levels, requires spending a lot of time. In this article, only this important point is mentioned that security assessment should:

• Securing any device or system.
• Provide security for all processes at each level
• Secure data transfer and provide interaction between each level.

Figure 1 shows the position of security in the Internet of Things reference model. Security must govern the entire model.

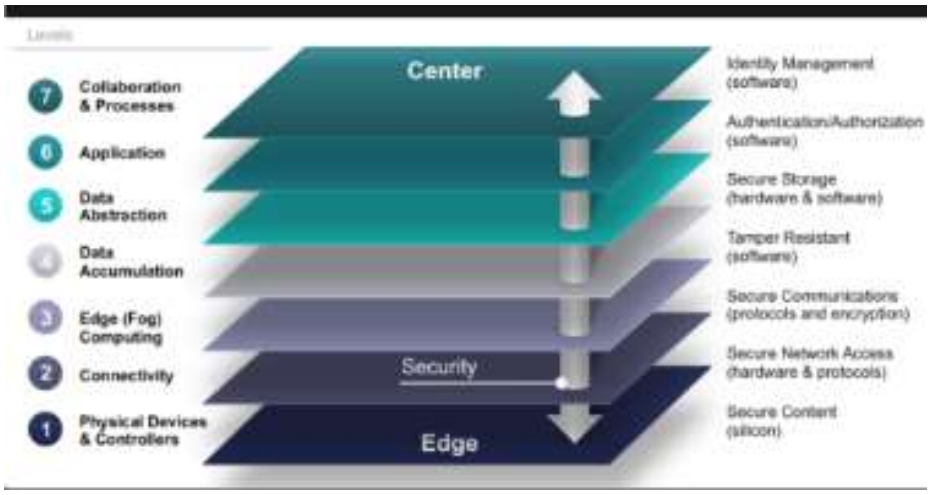

Figure 1: Security in the Internet of Things

2. An overview of security issues in the Internet of Things

In the last decade, the Internet of Things has been at the center of attention and research. Security and privacy are important issues for IoT applications and continue to face major challenges. In order to facilitate this field of emerging issues, we briefly review the IOT research method and pay attention to the security category. Using deep analysis of security architecture and its features, security requirements are presented. Based on this research, we discuss the state of research in fundamental technologies including cryptographic mechanisms, secure communications, sensor data protection, and cryptographic algorithms, and briefly outline the challenges.

In order to meet the security issue, IOT is facing more challenges. There are the following reasons for this:

1) IOT is developed through traditional internet, mobile network and sensor network, etc
2) Many objects are connected to this type of Internet
3) These objects communicate with each other. As a result, a new security and privacy problem arises. More attention should be paid to reliability, detection and data integration in IOT.

At this level, environmental intelligence and autonomous control are not part of the main concept of IOT. With the development of advanced methods of network and multi-agent control and cloud computing, a transition between the concepts of IOT and independent control in M2M research has been established to produce an evolution in M2M in the form of CPS. CPS generally focuses on the intelligentization of interactions, interactive programs, distributed real-time control, cross-sectional optimization, surface domain optimization, etc. As a result, some

new technologies and methods should be developed to meet more requirements in terms of reliability, security and privacy.

3. Internet of things security problems and concerns

The digital world is saturated with personal and shared data recorded by people and has raised concerns about the security and protection of information for people and governments. The problems caused by the transfer and processing of unwanted data have caused users' concerns and legal issues. With the rapid growth of IoT applications, security concepts are taken into consideration and concerns about privacy and people's inability to control their personal lives are formed. If people's daily activities are monitored and they produce information outputs, political, economic and social activities will be affected. In the event of security breaches, attacks, and malfunctions, the benefits of IoT diminish. In the near future, a large amount of information will be received and sent by connected devices and management systems. Keep in mind that information is constantly moving and moving, and with the arrival of the Internet of Things, the approach to this movement will be very different from the current state. The security of the Internet of Things will be completely different from the current trends due to the connection of all devices to each other. We must pay attention to the connection and communication points of our information transfer between all devices and clouds and networks and create safety there.

Sopho Security Center, as one of the largest security product support banks, has started predicting the security threats of 2015. According to Sopho, the exploitation of software vulnerabilities will decrease in 2015. As the number of software vulnerabilities decreases, few vulnerabilities will be heavily exploited. The Internet of Things seems to be the biggest security concern of 2015. This new technology, at its birth, has paid great attention to the issue of security. The companies Google, Samsung, Sony and other technology giants that somehow played a role in the growth of this technology have made compliance with safety one of the basic principles of work, but according to experts, the Internet of Things has passed from the "demonstration safe" stage to the "dangerous" stage at work. "It will arrive and without a doubt, the real encounter with malware writers will change the conditions in a different way.

Network and information security are measured with the components of identification, confidentiality, integrity and non-repudiation. The Internet of Things is used in the global economy and in medical services, health care, intelligent transportation and many other areas, so security requirements are of great importance in it. With the Internet of Things, it can be predicted that in the first stage, cybercriminals will attack the points of information generation and transmission, command centers, points and network entrances, and protection should be provided for these points. Heterogeneous protocols and devices, development of security services. With high error tolerance, it makes it a difficult activity. The Internet of Things is facing many challenges. In terms of scalability, IoT applications require a large number of devices, which are difficult to implement due to time, memory, and processing limitations. For example, calculating daily temperature changes within a country requires a lot of devices and requires a lot of data management. Figure 2 shows the essential security requirements for the Internet of Things. As you can see, privacy and security are required as key technical building blocks.

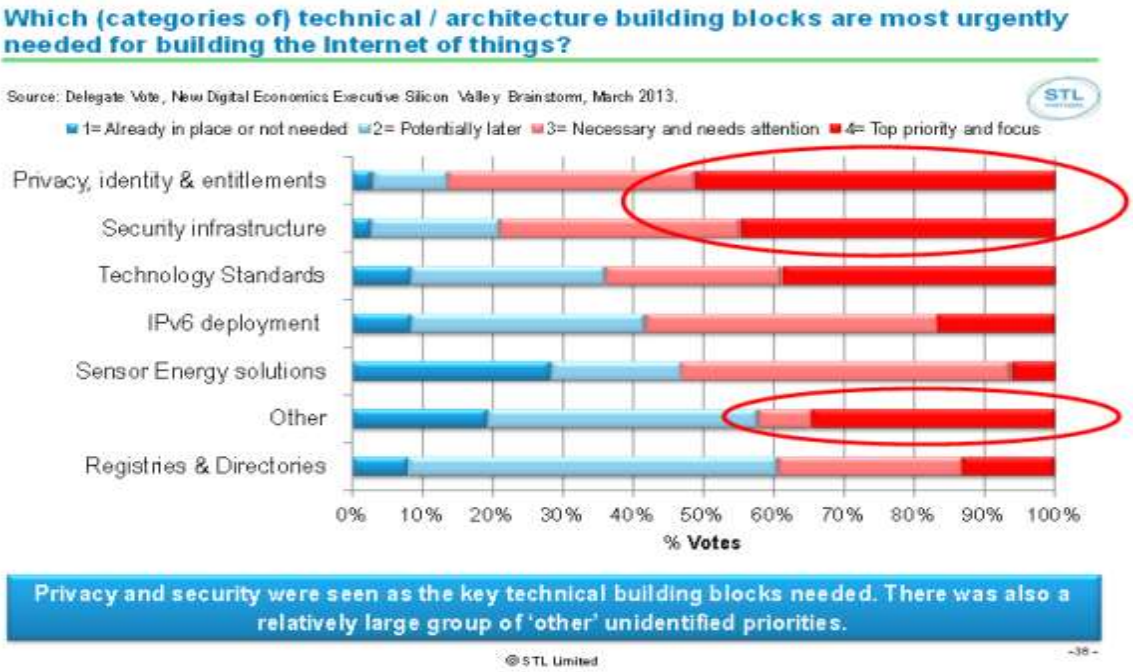

Figure 2: IoT security requirements

As an active and new research topic, IOT must solve different areas of problems, in different layers of architecture and from different aspects of information security, the following subsections analyze and summarize common challenges for the security of the Internet of Things.

A) Architectural structure

In reference 10, the IOT remains stable during the entire time period, and the security mechanism in each logical layer cannot implement the complete defense system, as a result, this is a challenge and there are many research areas to create a secure structure with A combination of control and information is required.

b) Basic management

Since core management is an important foundation of secure mechanism, this topic is always a hot research topic. This remains the most difficult aspect of cryptographic security. Currently, researchers have not found the ideal solution for this issue. A light encryption algorithm or a higher performance sensor node is still not implemented. As a result, the large-scale sensor network always remains viable. Network security issues have become more important and cause problems in the field of network environment research.

c) Security rules and regulations

Currently, security law and regulations are still not in the center of attention and there are no technological standards regarding IOT. IOT is related to national security information, trade secrets and people's privacy. As a result, our country needs a legal perspective for the development of IOT. Rules and regulations are undeniably needed. In this aspect, we have a long way to go.

d) Requirements for emerging applications

With the development of WSNs, radio frequency identification (RFID), pervasive computing technology, network telecommunication technology, and distributed real-time control theory, CPS, an emerging form of IOT, has become a reality. In this system, high security is required to guarantee system performance. As mentioned, security challenges for IoT have been met. It is also very necessary to create quasi-safe structures. Basic management in a real large-scale sensor network is always a challenging issue, and the regulations and laws of this field related to IoT are also challenging issues.

4. Attention to security in IOT

Information and network security must be met with characteristics such as identification, reliability, integration and irrefutability, etc. IOT will be applied to important areas of the national economy such as healthcare and medical care and intelligent transportation. As a result, security in the field of IOT is more important in terms of accessibility and dependability.

4.1. Secure architecture

In general, IOT can be divided into four general levels. Figure 3 shows the object level architecture.

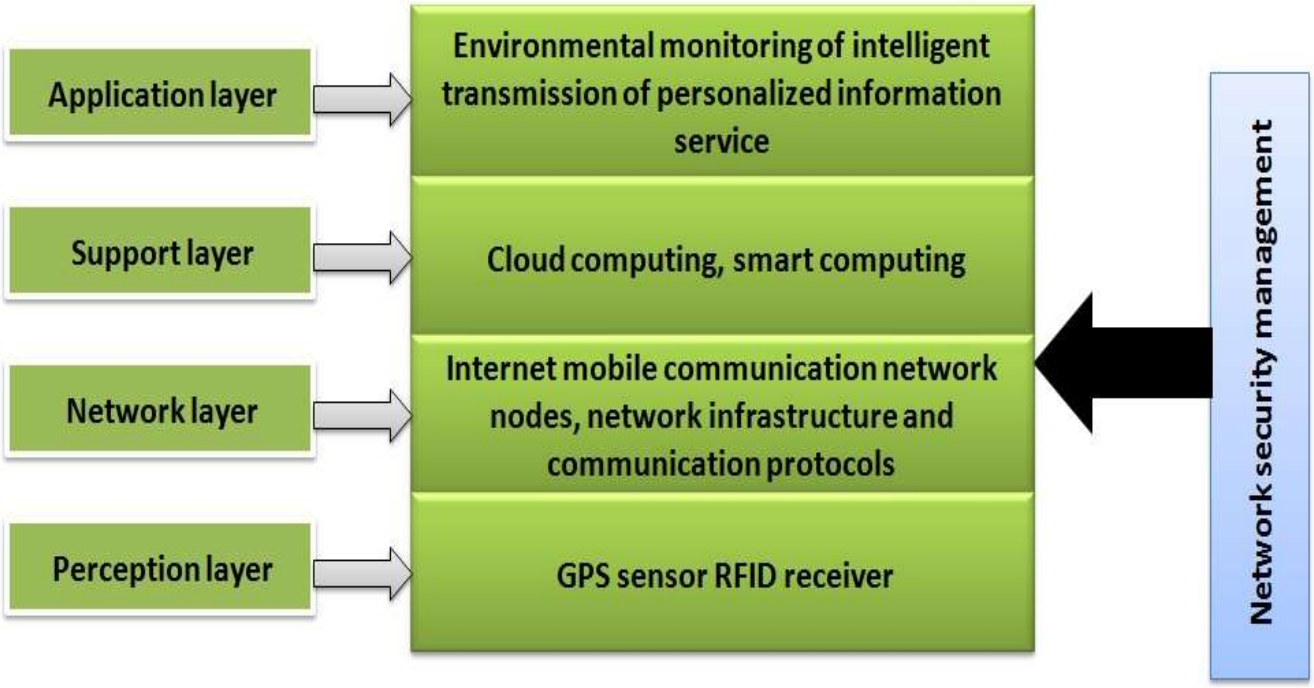

Figure 3: Architecture of objects

The most basic foundation is the perception layer or detection layer, which collects all the information through physical equipment and identifies the physical world, this information includes the characteristics of objects, environmental conditions, etc., and the physical equipment includes the RFID reader. , all types of sensors, GPS and other equipment. The basic component in this layer is the sensors to receive and express the real world in the digital world.

The second layer is the network layer. The network layer is responsible for sending information from the perception layer, primary processing of information, classification and submission. In this layer, sending information is based on several basic networks, which include the Internet, mobile telecommunication network, satellite nodes, wireless network, network structure, and telecommunication protocols are also necessary for the exchange of information between equipment.

The third level is the support layer. The support layer sets up a reliable support platform for the application layer, in this support platform, all the computing power is organized through the connection network and cloud computing. This layer plays the role of an application composition layer. The application and management layer plays a fundamental role at any top level. Then, we will analyze the security features.

4.2. Secure architecture in the Internet of Things

One of the mechanisms for creating security in the Internet of Things is the use of appropriate architecture. IoT architecture has four levels. Figure 4 shows the four levels of IoT, on the left and on the right of the security requirements of each layer, to get to know the architectural layers

of this technology and the mechanisms of each layer. The discussion about the functioning of these 4 layers and their security system requires a separate topic that is not included in this article.

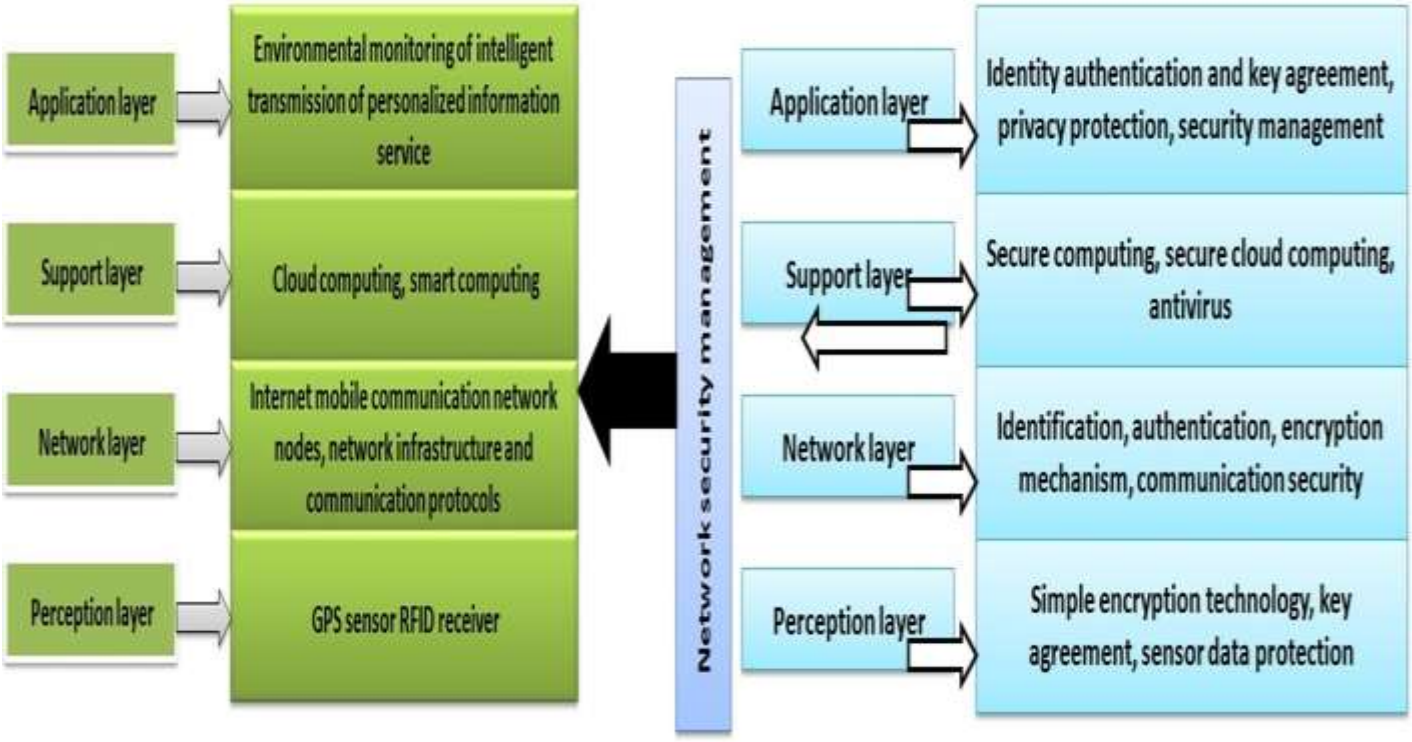

Figure 4: IoT security architecture and security requirements in each layer

4.3. Security features

a) Perception layer: Perception nodes are generally smaller than computing power and storage capacity because they are simple and consume less power. As a result, they are not able to apply the desired telecommunication frequency and general encryption algorithm for secure protection. And therefore, creating a secure protection system is very difficult. Meanwhile, attacks from external networks such as network inaccessibility also create new security issues. On the other hand, sensor data still needs protection for integration, detection and reliability.

b) Network layer: Although the central network has full security protection, but human attacks and fake attacks still exist, in addition, spam emails and computer viruses cannot be ignored, a large amount of data transmission causes congestion. to be As a result, the security mechanism at this level is very important in IOT.

c) Support layer: The task of performing heavy data processing and intelligent decision making of network behavior is in charge of this layer, intelligent processing is limited for fake information, because there is a challenge to improve the ability to detect unwanted and fake information.

d) Application layer: At this level, security is different for different application environments, and data sharing is one of the characteristics of the application layer, which causes problems in data privacy, access control, and information disclosure.

4.4. Security requirements

According to the above analysis, we can show the security requirements for each level as below and according to Figure 5.

a) Perception layer: At first, node confirmation is necessary to prevent illegal node access. Second, data encryption is absolutely required to protect the reliability of data transmission between nodes. And prior to data encryption, basic agreement is an important process. The stronger the secure measurements are, the less resources will be consumed. In order to solve this

problem, light encryption technologies have become important, which include light encryption algorithms and light encryption protocols. At this time, integration and detection of sensor data has become a research topic, so we talk about this in detail in the next section.

b) Network layer: In this layer, it is difficult to apply existing telecommunication security mechanisms. Identification of characteristics is a mechanism to prevent illegal nodes and it is a form of secure mechanism, reliability and integrity are of equal importance, as a result, it is necessary to record data in a reliable and correct manner. Distributed Denial of Service (DDOS) attacks are a common network attack method and are specifically used in many Internet of Things applications. As a result, in order to prevent DDoS attacks for vulnerable nodes, it is another problem to be solved in this layer.

c) Support layer: The support layer requires a lot of secure architecture, such as cloud computing and secure multi-part computing, almost all strong cryptographic algorithms and cryptographic protocols are stronger than security systems and antiviruses.

d) Application layer: In order to solve the security problem in the application layer, we need two aspects. One is detection and the other is basic agreement in the heterogeneous network, the other is the protection of people's privacy. In addition, learning and management are very important in information security, especially password management.

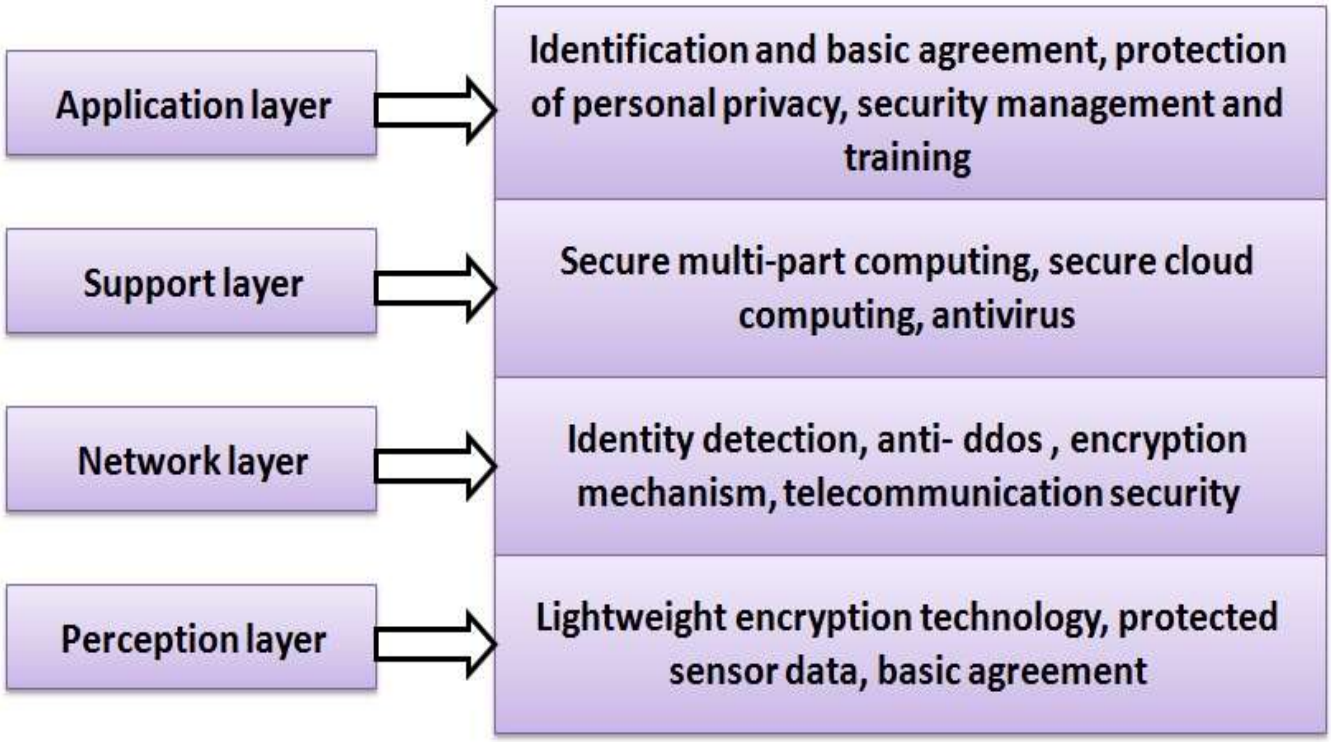

Figure 5: Security requirements at each level

5. Basic technologies research mode

Now, we turn our attention to the state of research for secure requirements in Section 2, and provide further details on the cryptographic mechanism, communication security, sensor data protection, and cryptographic algorithm in the following subsections.

5.1. Encryption Mechanism

In the traditional network layer, we use the step-by-step encryption method, in this method, the information is encrypted in the transmission process, but it is necessary that the original message is preserved in each node through the encryption and decryption operation. In addition, in the layer of traditional applications, the encryption mechanism is end-to-end encryption, so that the

information is clear only to senders and receivers, and encryption is always done in the process of sending and forwarding nodes. In IOT, the network layer and the application layer are very closely connected to each other, so end-to-end and close connection methods must be used, we can protect only the links that need protection, because At the network layer, we can apply it to all businesses, which creates a secure implementation of various applications. In this way, the security mechanism in business applications is clear, which makes the end user comfortable. In this way, this mode creates features in the by-hop mode such as low delay, high efficiency, low cost, etc. However, due to the decryption operation in the sending node, using the by-hop method in each node can lead to the original encrypted message, which results in high reliability in the sending nodes. By using end-to-end encryption, we can choose different security rules based on the type of business, as a result, it can provide high-level security protection in business security requirements. However, end-to-end encryption cannot encrypt the destination address because each node determines how to send the message based on the destination address, the results of which cannot be hidden from the source and destination in the sent message and prevent unwanted attacks Create**.**

According to the above analysis, we can conclude that: when the security requirement in some business is not very high, we can adopt by-hop encryption protection: when our business needs high security, then encryption End to end is the first choice. As a result, according to different requirements, we can use alternative encryption mechanisms. At present, IOT is developing in its early phase, and research in security mechanism is an overlooked point in this field, therefore, we have a long way to go for our research in this field.

5.2. Telecommunication security

Initially, in telecommunication protocols, some solutions have been developed, these solutions can provide integrity, detection and reliability for TLS/SSL or IPSec communications. TLS/SSl is designed to encrypt the link at the transport layer. This can provide integrity, detectability and reliability at each layer. And the need for security is also caused by this case, but unfortunately it has not been widely used.

Communication security mechanisms are also rarely implemented in today's applications. Since small IoT devices have little processing power, this leads to often poor secure communication. Meanwhile, in IOT, the central network is always current with the next generation Internet, often information is sent through the Internet. As a result, DDoS still exists and is a huge problem. These restrictions and DdoS attacks cause the loss of accessibility in telecommunication networks. When organized or large-scale DDoS attacks occur, the recovery methods of these problems become significant, as a result, it is necessary to pay more attention to research on prevention and recovery mechanisms of risks.

5.3. Sensor data protection

Similar to what was discussed in Section 2, the integrity and accuracy of sensor data has become a research issue and the reliability of sensor data is a lower demand because when an attacker can physically place his own sensor in close proximity to the original sensor. , can receive similar values. As a result, there is relatively little reliability required in the sensor itself.

Another research topic in sensors is privacy, and privacy is also an important issue. It is necessary to provide a mechanism to protect the privacy of people and people in the real world. Most of the time, people are often unaware of the sensors in their lives, so there is a need to establish regulations to ensure people's safety.

5.4. Cryptographic algorithms

Suitable and reliable and well-known cryptographic algorithms are presented in Internet security protocols according to Table 1.

Table 1: Encryption algorithms

purpose	Algorithm
Reliability	Advanced encryption standard
Digital signature	Rivestshamiradelman (RSA) or elliptic curve cryptography

transfer	
Basic matching	Diffie-hellman (DH)
completeness	SHA-1/SHA-256

Generally, symmetric encryption algorithm is used to encrypt data for reliability such as Advanced Encryption Standard (AES); Asymmetric algorithm is also used in digital signature and important transmission applications. ECC implementation is also reduced and may be welcomed in recent applications.
In order to apply these encryption algorithms, available resources such as processor speed and memory are required. As a result, it is not clear how these cryptographic methods can be applied in IOT, more research efforts are needed to confirm that the algorithms can be well used in IOT with limited memory and low speed processors. , to be implemented.

6. Conclusion

In the past few years, this emerging field for IoT has attracted considerable attention. Due to the rapid evolution of this matter, we are still facing new and different challenges in this field. In this chapter, we examined security in the Internet of Things and reviewed the security characteristics and requirements in four layers, including the perception layer, the network layer, the support layer, and the application layer. Then, we describe the research states in this area of cryptographic mechanism, telecommunication security, sensor data preservation and cryptographic algorithm. And we briefly stated several challenges. All in all, the development of IOT provides serious security issues that are always in the center of attention and research topics.

References

1. Mohammadiyeh, Seyyed Ali and Khorram, Ttoosa and Beshkani, Mohammad Kazem,2022,Investigating intelligent dialogue factors in e-commerce projects,The 17th International Conference on Information Technology, Computers and Telecommunications,https://civilica.com/doc/1588764
2. Madanchi F., Maghroor H., O'Neal T.,"A Systematic Review of the Internet of Things Contribution to Obtain Supply Chain Integration", Proceedings of the 9th North American Conference on Industrial Engineering and Operations Management (IEOM), Washington D.C., USA June 4-6, 2024.
3. Beshkani, Mohammad Kazem, 2023, review of the architecture, protocols and components of the Internet of Things structure, the fifth national conference on new achievements in electrical, computer and industrial engineering, Esfarayn, https://civilica.com/doc/2005596.
4. Ebrahimi, Nahid and Beshkhani, Mohammad Kazem, 2019, Investigating the impact of Internet of Things on transportation in big cities, https://civilica.com/doc/1242181.
5. Reihanian, Iman and Paknezhad Panahi, Sima and Beshkani, Mohammad Kazem,2021,Examining the opportunities and challenges of the Internet of Things,The 17th International Conference on Information Technology, Computers and Telecommunications,https://civilica.com/doc/1588766.
6. Hilley Sarah, Badly advised: US Government data mining program may be pulled due to privacy concerns, Computer Fraud & Security, Volume 2007, Issue 10, Pages 8-10, November 2017.
7. Tsai, C., Lai, C., & Vasilakos, V. (2019). Future internet of things: Open issues and challenges. ACM/Springer Wireless Networks,. doi:10.1007/s11276-014-0731-0.
8. Hachem, S., Teixeira, T., & Issarny, V. (2018). Ontologies for the internet of things (pp. 1–6). New York: ACM.
9. Patel, K.K.; Patel, S.M.; Scholar, P. Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. **2016**, 6, 6122–6131.
10. Strategy analytics: internet of things now numbers 22 billion devices but where is the revenue?, strategy analytics online newsroom." https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where, (accessed Feb. 23, 2020).
11. Patel K. K., Patel S. M., and Scholar P., Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges, *International journal of engineering science and computing*. (2016) .
12. Vermesan O. and Friess P., Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 2017, River publishers, Denmark.