An overview of the structure and security in the Internet of Things

First Author Azadeh Pasandideh
Affiliation : Master of Computer Science, Azad University, Tehran Science and Research Unit

Abstract
Success and achieving widespread use for any technology requires gaining users' trust by providing adequate security and guaranteeing privacy. The Internet of Things (IoT) is an emerging paradigm that focuses on the internal connection of objects or devices with each other or users.
The Internet of Things technology needs a change in the legal framework. Issues related to maintaining security in the Internet of Things are an integral part of the IOT architecture. Without IoT security protocols and standards, the existence of any hardware is considered useless. Because only with their existence, data transfer is possible by hardware and useful information can be extracted from the transferred data by the end user. . Compared to other articles in this field, this article has a more comprehensive coverage and extensively examines the domains of the Internet of Things, including the structure and security protocols.

Keywords: Internet of Things, Security, IOT.

Introduction

In recent years, the world has faced rapid technological progress, each of which has a significant impact on daily life. The emergence of technologies such as smartphones; tablets; Laptops and personal computers have increased mutual communication over time and in the distance dimension. Contemporary technology goes beyond strengthening communication between humans and currently to achieve a common goal of communication between humans and objects and in in fact, it facilitates the communication of objects with each other; This definition is called Internet of Things (IoT). [1]

The Internet of Things was created in the period of 2008 and 2009. According to the research conducted in this field, it is predicted that the number of connected devices will reach 50 billion in 2020. The main goal of this increase in the number and types of IoT objects is to generate useful information about the surrounding environment to make them smarter.

It is done through the collection and analysis of past, present and future data. The data allows the optimal decision to be made about us and our environments in real time.[2] which causes concerns about There is a risk of privacy loss. To the extent that many researchers of this research field believe that the growth and development of the Internet of Things depends on providing security and solving this concern. [3] The Internet of Things (IoT) is supposed to be one of the Important technological developments are time to change, provided that we can use their full potential. IoT is a global infrastructure for the information society and provides advanced services by connecting (physical and virtual) objects based on the interaction of existing information and communication technologies. [2]

The emergence of the Internet of Things (IoT) has accelerated the pace of economic development in all sectors. However, it has also brought significant challenges to traditional human resource management, revealing an increasing number of problems and making it impossible to meet the needs of contemporary organizational management. The Internet of Things has brought many conveniences to human society, but it has also led to security problems in communication networks. To ensure the security of these networks, it is necessary to integrate data-driven technologies to solve this problem. Despite the significant and widespread applications of IoT, its deployment in mission-critical areas presents great challenges with fundamental security and privacy concerns. gives for example, a successful security breach in a smart healthcare system can lead to the loss of patient lives and significant financial consequences. Similarly, in the context of smart transportation systems, a breach of rules can lead to financial losses and human casualties. [4]

Definition and concept of IOT

Various definitions of IoT have been created at present. The important differences between the emerging definitions depend on the desired perspective to examine IoT. According to the definitions that are often mentioned about IoT, "IoT" considers global infrastructures for the information society and advanced services. It implements through the communication (physical and virtual) of objects based on communication technologies and compatible information that is evolving and existing. [5]

The phrase "Internet of things" refers to a convention in the world that "everything" can be uniquely identified and addressed through some kind of communication device, and objects can be located, used, preserved and maintained for various purposes. and inspected.

"Objects" are valuable resources, either as material value or in the form of service they provide. Resources need to be managed through their lifecycle, and access to resources needs to be controlled and audited. The identity of resources and their clients (where applicable) must be managed, protected and maintained by an identity management system, and There should be mechanisms in place to authenticate identities, control access to resources, and protect the use of information to protect privacy.[6,7]

Architecture and structure of the Internet of Things

The Internet has evolved tremendously in recent years and has connected billions of objects worldwide. These objects have different sizes, capabilities, processing and computing power, and have different applications. Currently, it can be said that the traditional Internet has been integrated into the smart Internet of the future, which is called the Internet of Things (IOT). IoT connects real-world objects and embeds intelligence into the system to intelligently process object-specific information and make useful autonomous decisions. Therefore, the Internet of Things can give rise to many useful applications and services that we have never imagined before.[8]

In general, at the moment, a standard architecture for the Internet of Things has not been designed and built, and for this reason, explaining the architecture of the Internet of Things can be a bit difficult and problematic. If we want to talk about this issue in general, we can say that the architecture of IoT is completely dependent on the way its components and parts work and implement. However, there is a basic process in this field that the Internet of Things is built on. This layer, which is also known as the data center or the cloud center, is actually connected with the end

users and manages the data. But based on TCP / IP and TMN models. Similarly, a 6-layer architecture is proposed based on a hierarchical network structure. As a result, it is typically separated into six layers:

- **Coding layer**: The coding layer of the Internet of Things that identifies the desired object is its core. In this layer, each object is given a unique identifier, which simplifies identification between objects. [9]
- **Perceptual Layer**: The Perceptual Layer is also known as the "Device Layer". The lowest layer consists of smart objects integrated with sensors. Sensors enable the interconnection of the physical and digital worlds and enable the collection and processing of information in real time. There are different types of sensors for different purposes. Sensors have the capacity to measure such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity, etc. In some cases, they may also have a degree of memory that allows them to record a certain number of measurements. . A sensor can measure a physical property and convert it into a signal that can be understood by an instrument. Sensors are grouped based on their unique purpose such as environmental sensors, body sensors, home appliance sensors and automotive telematics sensors etc. Most sensors need to be connected to sensor gates.[10]
- **Network layer**: The network layer can also be called "transport layer". This layer securely transmits information from the sensor devices to the information processing system. The network layer is like the neural network and brain of LOT, whose main task is to transmit and process information. The network layer includes a convergence network of the communication network and the Internet, network management center, information center and intelligent processing center, etc. [11]
- **Middleware layer**: Devices on the Internet of Things implement different types of services. Each device connects and communicates with only those other devices that run the same type of service. This layer is responsible for managing the service and has a link to the database and receives information from the Network layer and stores it in the database. It stores information from the network layer. In the database section, it performs information processing and calculations everywhere and automatically makes decisions based on the results.[8]
- **Application Layer**: Based on the processed data, this layer enables IoT applications for various industries. As the applications support IoT development, this layer is useful for the massive deployment of IoT networks.
- **Business Layer**: All IoT related studies are managed by this layer which also oversees IoT applications and services. It provides several business models for efficient tactics.[12]

Information communication network security

When conducting information communication network security management, the first priority is to ensure data security. Therefore, the use of big data technology can not only provide data support for management, but also improve It. information security problems in the Internet of Things from the perspective of application, the Internet of Things can be divided into the understanding layer, the network layer, the application layer, and the Internet of Things layer. However, network information security problems also arise one after another. When the Internet of Things acquires data in the sensor layer, the information transfer is mainly completed through wireless networks. However, the security of wireless networks in public places is low and criminals can easily use them to carry out illegal operations.

Operations on user equipment In IoT applications, many devices are characterized by sensor technology and operated remotely by it. Computers These devices are basically installed in an unattended location, so attackers can easily access these devices. find and destroy them.

In addition, they break the sensor communication protocol and perform illegal operations. The sensor itself has very simple operation and limited energy storage and lacks security protection. In addition, the variety of communication networks covered by the Internet of Things is so rich that it cannot provide a unified security defense system, so the security of the sensor ontology is very low.[4,14]

Core network security

When the Internet of Things is acquiring information, it produces many nodes that can understand, acquire and monitor information. Currently, the Internet's security performance is relatively high. However, there are many nodes in the Internet of Things. When data is transmitted across many nodes simultaneously, it is easy to create network congestion. One of the main security problems of IoT is the arrangement and connection of the Internet of Things in a crosswise manner. During operation, the topology is constantly changing, which makes it difficult for the application equipment to easily control the input and output. In the Internet of Things environment, if the viruses spread on the Internet pass through the barriers of the relevant security protection technologies, they are likely to maliciously manipulate the authorization management of the Internet of Things, thereby violating the privacy of users and stealing other people's funds. .

The key technologies of data-based network information security include data acquisition and data persistence, which in the process of data-based security is the first step of obtaining data that can be classified into internal data and external data according to the data source. divided When acquiring data, since the content of the original data is relatively diverse, it is necessary to filter the data and remove some redundant information to facilitate subsequent operations. After filtering and processing, the operational status of information systems can be mastered in relation to related information at a point in time, thus achieving the goal of data-based network security. In the data persistence stage, the persistence of data meets the actual needs. Gains depth by analyzing the relationship. In the process of data persistence, relational databases are usually used to store data, and the storage is complex. The main reason is the variety of primary data and the large proportion of unstructured data in this data.[15,16]

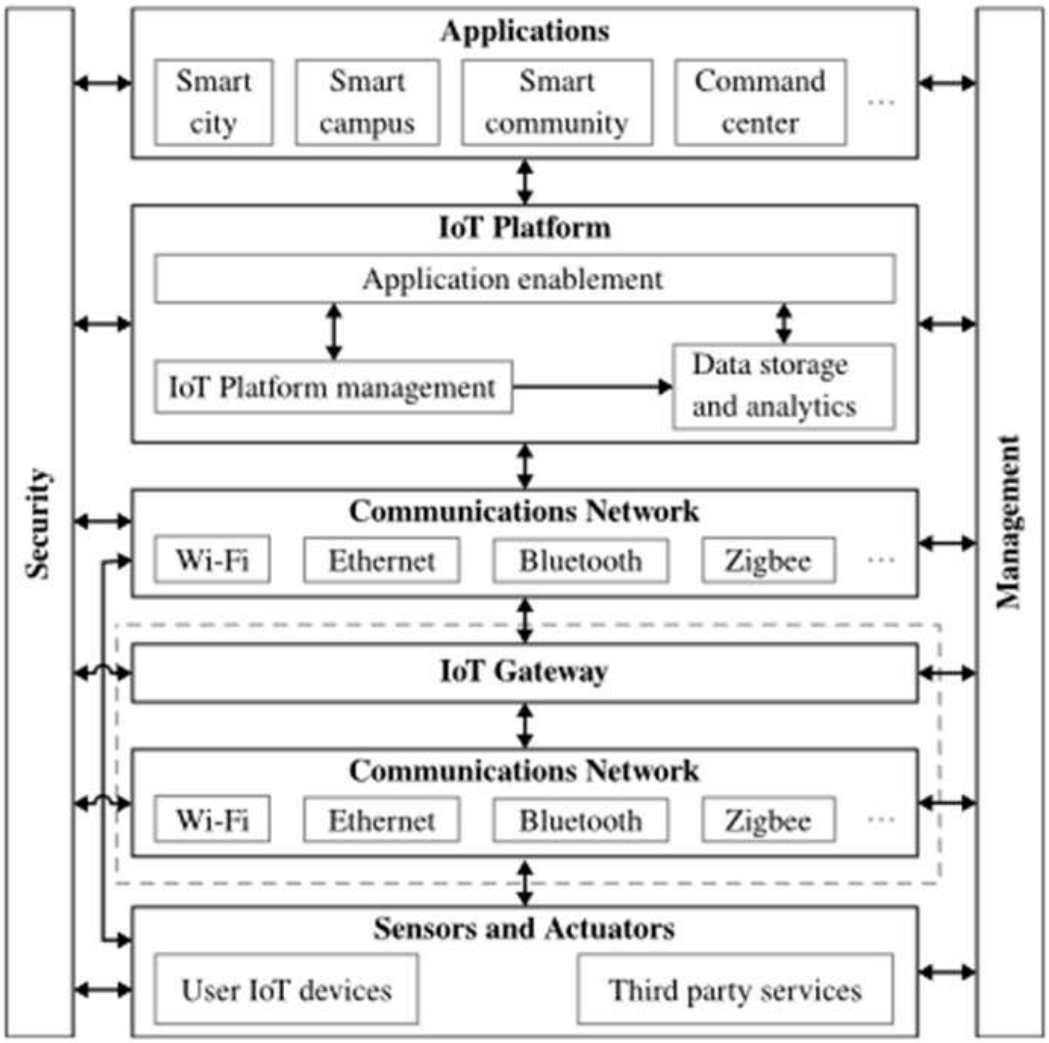

Figure (1) IoT architecture [13]

Conclusions

According to the content presented in this article, it can be seen that the Internet of Things (IoT) is expanding rapidly and reaches various domains, including personal health care, environmental monitoring, home automation, smart mobility, and industry. As a result, IoT devices are more and more deployed in various public and private environments and gradually become common objects of daily life. Hence, it is obvious that in such a scenario, cyber security becomes critical to prevent threats such as leakage of sensitive information, denial of service (DoS) attacks, unauthorized network access, etc. Unfortunately, many low-end commercial IoT products typically do not support strong security mechanisms and can therefore be a target or even a tool for a number of security attacks.

References

[1] Bordbar,M,Rahmani,M,Zakariyan,A.(1402). Examining the structure and protocols of the Internet of Things . Journal of Science andEngineering Elites

[2] Seitz,L, Selander,G, Gehrmann,CH.(2013). Authorization Framework for the Internet-of-Things. IEEE. ttps://doi.org/10.1109/WoWMoM.2013.6583465

[3] Pallavi Sethi and Smruti R. Sarangi(2017). Internet of Things: Architectures, Protocols, and Applications, Journal of Electrical and Computer Engineering. https://doi.org/10.1155/2017/9324035

[4] Niu ,X.(2024). Exploration on human resource management and prediction model of data-driven information security in Internet of Things. . Journal homepage: Heliyon, https://doi.org/10.1016/j.heliyon.2024.e29582

[5] Yadollahzadeh-Tabari ,M ,Mataji,Z.(2021). Detecting Sinkhole Attack in RPL-based Internet of Things RoutingProtocol, Journal of Artificial Intelligence and Data Mining. Journal homepage: http://jad.shahroodut.ac.ir

[6] Fongen,F.(2012). Identity Management and Integrity Protection in the Internet of Things. IEEE. https://doi.org/10.1109/EST.2012.15

[7] Samani,A, H.H,Ghenniwa , A , Wahaishi .(2015) Privacy in Internet of Things: A Model and Protection Framework, Elsevier. https://doi.org/10.1016/j.procs.2015.05.046

[8] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges. In 2012 10th International Conference on Frontiers of Information Technology (FIT): Proceedings (pp. 257-260). Institute of Electrical and Electronics Engineers Inc.https://doi.org/10.1109/FIT.2012.53

[9] Ibrar,Y, Ejaz A, Ibrahim Abaker Targio ,H, Abdelmuttlib , Ibrahim ,A.A, Abdullah ,G, Muhammad ,I, Guizani,M.(2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges, http://dx.doi.org/10.1109/MWC.2017.1600421

[10] Patel, K.K. and Patel, S.M. (2016) Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, 6, 6122-6131.

[11] Wu,M, Lu,T.L, Ling,F.L, Sun,,L , Du,H.Y.(2010). Research on the architecture of Internet of Things, 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE).http://dx.doi.org/10.1109/ICACTE.2010.5579493

[12] Md. Mahbubur ,R.(2022). A Review on Internet of Things-IoT-Architecture, Technologies, Future Applications & Challenges. Journal homepage: ijsab.com/ijsb.80-92.http://doi.org/10.5281/zenodo.7066810

[13] Bolaño,T.D, Campos,O, Barral,V, Escudero C.J, García-Naya,J.A.(2022). An overview of IoT architectures, technologies, and existing open-source projects. Internet ofThings, ,https://doi.org/10.1016/j.iot.2022.100626.

[14] Kokila ,M , Reddy ,S. K.(2025).Authentication, access control and scalability models in Internet of Things Security–A review, Cyber Security and Applications, 2025, p. 100057, https://doi.org/10.1016/j.csa.2024.100057.

[15] C. Maniveena, R. Kalaiselvi, A survey on IoT security and privacy, AIP conference proceedings, AIP Publishing, 202

[16] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Commun. Surv. Tutorials 22 (3) (2020) 1646–1685.