Future Generation of Communication and Internet of Things (FGCIOT)

Journal homepage: http://fgciot.semnaniau.ac.ir/

Review paper

Security in the Internet of Things (IoT): A review of the status, challenges and future issues

A. Zamani, S. Ziari

Department of architecture, Semnan Branch, Islamic Azad University, Semnan, Iran

Article Info

Article History:
Received: June 27, 2023
Revised: August 10, 2023
Accepted: September 11, 2023

Keywords:
Internet Of Things (IoT), Radio FrequencyIdentification(RFID),Wireless SensorNetworks(WSN),Confidentiality, Integrity and Availability (CIA),

*Corresponding Author's Email Address:Alireza1995zamani@gmail.com, Setayeshziari5@gmail.com

Abstract

Internet of things is a modern and up-to-date technology and it has become so popular that millions of applications have been produced in this technology. Popular IoT products include smart home, smart city, smart industries, smart agriculture, etc. A wide spectrum for using the Internet of Things has led to thinking about the security of these systems. Various security measures that exist in the three-layer architecture of the Internet of Things and cover the heterogeneity and globality of this system. This article is an overview of security principles, technology and security challenges, and dealing with possible and future measures to ensure the security of the Internet of Things.

Introduction

The Internet of Things is a system of computers, computing machines, digital and mechanical devices, humans, animals and services that can share data and information to achieve a common goal in various fields. IoT has many applications such as transportation, agriculture, and health. Energy production and distribution is part of its scope.

The goal of IoT is to transform the way we live today. Building smart systems around us that perform daily tasks such as home robots, smart homes, smart cities, smart transportation, etc.

There are many application areas of IoT from personal to enterprise environment. [1] Today, programs in the personal and social sphere (social networks) enable Internet users to interact with their surroundings and users can maintain social relationships. Another application of IoT is in the field of transportation, where cars on the roads send traffic signals and create suitable transportation facilities with the purpose of safety. In companies, IoT is used in the field of industries or finance, marketing. Other mentioned applications are the field of service and facility monitoring, which includes agriculture, breeding, energy management, recycling operations, etc.

IoT applications have made great progress in recent years due to radio ID technologies and wireless sensor networks. RFID is responsible for tagging each device, so that it serves as the basic identification mechanism in the IoT. According to WSN, every "thing" i.e. people, devices, etc. becomes a wireless identifiable object and can communicate between the physical, internet and digital worlds.

In the following, after describing the framework and architecture of the three layers of IoT, issues related to various security principles and the nature of IoT devices are presented. This section also includes security issues

Doi:

related to each layer of IoT. Also, some issues have been raised about recent research and efforts to address security issues in IoT. Finally, it will be explained to the future and the directions that can be taken according to the current situation of IoT in the field of security.

A. IoT architecture

In IoT, each layer is defined by its functions and the devices used in that layer. There are different opinions about the number of IoT layers. Although, based on many studies [2] , [15] , [8] , IoT mainly operates on three layers, which are: perception, network and application layers. Each of the layers of IoT has its own inherent security problems. "Fig. 1" shows the architectural framework of three main layers according to the tools and technologies of each layer.

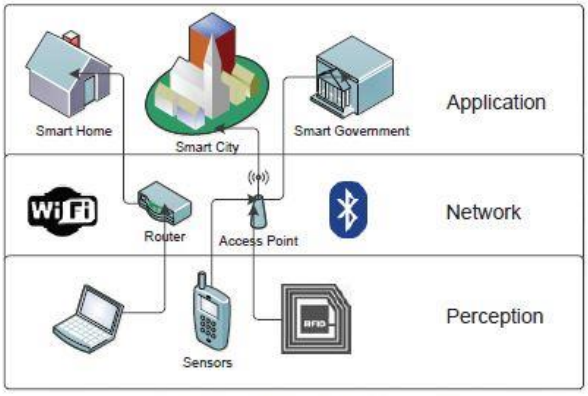

Fig 1: IoT three-layer architecture

B. Perception layer

The perception layer in the IoT architecture is also known as the "sensors" layer and its purpose is to obtain environmental data through sensors and actuators. This layer is the lowest layer in the IoT architecture that identifies, collects and processes information and then transmits it to the network layer. There are many measuring devices to collect information from objects such as actuators, RFID tags, smart sensors, wearable measuring devices, etc.

C. Network layer

The network layer performs the function of data routing, transmission to various IoT centers and devices through the Internet. This layer is the "heart of the IoT architecture". In this layer, cloud computing platforms, internet gateways, switching and routing tools work using some recent technologies such as WiFi, LTE, Bluetooth, 5G, Zigbee, etc. It should be noted that in this layer, error detection and correction, control of messages related to routing and publishing and sharing are also done.

Network gateways act as intermediaries between different IoT nodes by collecting, filtering, and transmitting data to/from different sensors. These networks can be configured in a private, public, or hybrid model and are built to support communication requirements for latency, bandwidth, or security. The network layer in the form of a local network (LAN) can include Ethernet, WiFi and BLE, and in the form of a global network (WAN) it can include Sigfox and LoRa. In general, this layer of the IoT architecture is responsible for connecting to other smart devices, network devices, and servers, and is used to transmit and process sensor data. [21] .

D. Application layer

It is considered as the highest layer of IoT architecture, which guarantees the integrity, integrity and confidentiality of data. In fact, the application layer provides services based on the user's needs.

This layer includes the Internet of Things program, which is responsible for delivering different types of application-specific services to different users in IoT. These applications can be from various industry sectors such as manufacturing, environment, health care, food and medicine

E. LoT security issues

The usual security goals of confidentiality, integrity, and availability apply to IoT as well. But IoT has many limitations in terms of components and devices, computing resources and power, and even the nature of expansion, which causes concerns.

IoT security issues include two parts:

• General security features of IoT

• Specific security issues of each layer of IoT.

F. General security features of loT

IoT security features can be broadly divided into two categories [5]:

Technological challenges due to the heterogeneous nature and ubiquitous presence of IoT devices.

Security challenges are related to principles and capabilities that must be implemented to achieve a secure network

Security in IoT must be implemented throughout the development cycle and operationally in all IoT devices and centers [8]. There are various mechanisms to ensure security, including:

• Licensed software on all IoT devices.

• When an IoT device is powered on, it must first authenticate itself to the network before collecting or sending data.

• Firewalls in an IoT network are necessary to filter packets directed to devices because IoT devices have computations with limited memory capabilities.

• Updates and modifications to the device should be configured so as not to consume additional bandwidth.

The following security principles apply to access a secure communication framework for people, software, processes, and other things:

G. Confidentiality

It is very important to ensure that data is secure and accessible only to authorized users. In IoT, a user can be human, machine, service, internal objects (devices that are part of a network), external objects (devices that are not part of a network). For example, it is important to ensure that sensors do not reveal the collected information to neighboring nodes [23]

H. Integrity

IoT is based on the exchange of data between different devices, so it is very important to ensure the accuracy of the information. The purpose of assurance is that the information is sent by the correct sender and the data is not tampered with during the transmission process due to interference or unwanted. The integrity feature can be created by maintaining end-to-end security in IoT communications. Data traffic is also managed using firewalls and protocols, but due to the characteristic nature of low computing power in IoT nodes, it does not guarantee security at the endpoint.

I. Accessibility

The vision of IoT is to connect more and more smart devices to each other. IoT users must have access to all available data whenever needed, but data is not the only component used in IoT. To achieve IoT expectations, devices and services must also be available when needed.

J. Identity confirmation

Every object in IoT must be able to be clearly identified and authenticated by other objects. However, this process can be very challenging due to the nature of IoT because many existing issues are involved (devices, people, services, service providers, etc.) and sometimes objects may need to be first interact with each other [7]. For these reasons, an authentication mechanism is needed in every IoT interaction

K. Heterogeneity

IoT connects different entities with different capabilities, complexities and people. The devices even have different release dates and versions, use different technical interfaces and bit rates, and are designed for completely different functions.

are designed, so the protocols should be designed to work in all different devices and different conditions [2] , [8] , [7] . The purpose of IoT is to connect device to device, human to device and human to human, thus communication between heterogeneous things and networks [5] Another challenge to be considered in IoT is that the environment is always changing (dynamic), at one time a device may be connected to a completely different device than at another time, and to ensure security, the system Optimal encryption with adequate security and key protocols is required.

L. Specific security issues of each layer of IoT

Every layer of IoT is susceptible to security threats and attacks. These attacks can be active or passive and may originate from external sources or internal network [1] At each layer, IoT devices and services are susceptible to denial-of-service attacks that make the device, resource, or network accessible to an unauthorized user. In the following sections, a comprehensive analysis of security issues is presented with respect to each layer.

M. Perception layer

There are three layers of security in the IoT perception layer:

The first part is the strength of wireless signals. Most signals are transmitted between IoT sensor nodes using

wireless technologies, which can degrade performance with interfering waves.

The second part of security, the sensor node in IoT devices can be intercepted not only by the owner but also by attackers because IoT nodes usually work in external and outdoor environments, which leads to physical attacks on sensors and IoT devices that In it, the attacker can manipulate the hardware

The third part is the inherent nature of the network topology, which is dynamic as IoT nodes often move to different locations. The perception layer of IoT consists mostly of sensors and RFID, for this reason their storage capacity, power consumption and computing ability are very limited and expose them to all kinds of threats and attacks [1] , [9].

The confidentiality of this layer can be easily exploited by a response attack [9] which is done by forging, changing or replaying the identity information of one of the devices in the IoT. Or an attacker may perform what is known as a timing attack by analyzing the time it takes to perform the encryption and obtain the encryption key. Another attack that threatens is when the attacker takes over the node. The attack of capturing the node and obtains all the basic information and data, the attacker can add another node to the network by sending malicious data, which compromises the integrity of the data. threats in this layer. This can also lead to denial of service attacks by consuming the energy of the nodes in the system and depriving them of sleep mode and disabling energy saving methods [23]

The security issues mentioned above in the perception layer can be addressed by using encryption and authentication (to verify the true identity of the sender) and access control [9]

N. network layer

As mentioned earlier, the IoT network layer is also vulnerable to denial of service attacks. Apart from denial of service attacks, the adversary can attack confidentiality and privacy at the network layer by traffic analysis, eavesdropping and passive monitoring [1] .

These attacks are highly likely to occur due to the remote access mechanisms and data exchange of the devices. The network layer is very sensitive to man-in-the-middle attack [1] ,which can be followed by eavesdropping and if the key items of the devices are eavesdropped, the secure communication channel is completely compromised. The key exchange mechanism in IoT must have sufficient security to prevent any intruder from eavesdropping and identity theft.

Communication in IoT differs from the Internet in that it is not limited to humans in machines, however the feature of machine-to-machine communication that IoT introduces has a compatibility security issue. The heterogeneity of network components makes it difficult to use current network protocols in the same way, and efficient protection mechanisms have not yet been developed for this purpose. Attackers can also use the fact that everything is connected in order to obtain more information about users and use this information for future criminal actions [2].

Protecting the network is important in IoT, but it is equally important to protect the objects on the network. Objects must have the ability to know the state of the network and the ability to protect themselves against any attack against the network. This can be created by having good protocols as well as software that enables objects against any situations and behaviors that can be considered abnormal or that may affect their security [6]

O. IoT security measures

IoT requires security measures at all three layers. in the physical layer for data collection, in the network layer for routing and transmission, and in the application layer for maintaining confidentiality, authentication and integrity. In this section, advanced security measures that address specific IoT security features and objectives are discussed. It has been discussed.

P. Identity verification measures

In 2011, Zhao et al.proposed a mutual authentication scheme for IoT between operating systems and terminal nodes. This scheme was based on hashing and feature extraction to avoid any collision attack. This scheme actually provides a suitable solution for authentication in IoT. Although this scheme improves security while reducing the amount of information sent, it only works in theory and there is no practical evidence to support it.

Another method for ID authentication in IoT sensor nodes is presented by Wen et al. [9]. In this method, one-time encryption is based on the request-response mechanism. This dynamic variable code is implemented using a pre-shared matrix between communication parties, and the parties can use random coordinates as

key coordinates. The key coordinate is what is actually transferred between the two parties, not the key itself. In this case, the key, that is, the password, is generated from a coordinate, and all messages are sent by encrypting the key along with the key coordinate, device ID, and time stamp. This encryption can be used when IoT security is not critical because the key is reproducible for different coordinates. Security can be optimized for specific IoT if the original coordinates are changed regularly.

Establishing the right access controls is as important to security as authentication, and these two functions go hand in hand to achieve a secure IoT. To address these features, Lu and Partners presented a controllability-based identity identifier and access capability for IoT, in this research they tried to fill the gap of a unified protocol with authentication and access control capability to achieve mutual authentication in IoT. The proposed model uses a public key approach and is limited to IoT devices plus existing access technologies such as Bluetooth, 4G, WiMax and Wi-Fi. By using a time stamp in the authentication message between the devices, which is referred to as the verification code. Message action prevents man-in-the-middle attacks. This plan works in three stages; First, a secret key is generated based on elliptic curve cryptography-Diffie-Hellman algorithm (N. Koblitz, 1987), then identity creation is done by one-way and mutual authentication protocols, and finally access control is implemented. The shared secret key is formed by combining the public key and a private parameter, and due to the use of elliptic curve encryption, it has a small size and low computational overhead**.**

Most of the devices involved in the IoT perception layer are RFID and sensors, such devices are computationally very limited, making it difficult to use any cryptographic algorithm to ensure network security. However, researchers presented a lightweight authentication protocol to secure RFID tags. In insecure RFID, an attacker can gain access to the network by hitting the victim's tag key joint and program it with another tag, such attacks can be prevented by using an authentication protocol. This protocol ensures mutual authentication between RFID readers and tagged items without introducing a large overhead on these devices.

Q. Creating trust

Since IoT devices can be migrated from one owner to another, trust must be established between both owners to enable smooth relocation of devices within an IoT subnet with respect to access control and permissions. be provided By creating an access control framework, Xie and Wang [3] presented the concept of mutual trust for inter-system security in IoT. This trust is created from the stage of creation, operation and transmission of IoT. The creation key and password are created in every new device that is entered into the network and created by a key right system. This key is applied by the manufacturer of the device, and the token of this key is applied by the manufacturer or the current owner; It is identified and combined. This mechanism ensures that permissions can be changed by the device itself. If the device is assigned to a new owner or is to be activated in another department of the same company, these tokens can be changed by the owners, provided that the old password is provided. , to replace previous permissions and access control. This mechanism is like changing the old key when buying a new house [22]

R. Unified architecture

The lack of global policies and standards to control the design and implementation of algorithms in IoT makes it difficult to control security. For IoT architecture, it is important to have a unified architecture that has an internal autonomy or centralized unit to overcome the heterogeneity of different devices, software and protocols. The work presented in proposed a definition for IoT integration and based on that, defined the access control model. The presented model takes into account flexibility and scalability, which are the main characteristics of IoT systems, and such an effort in another research [17] was done to propose a framework called secure intermediate gateway for critical infrastructures. This method is an abstraction of IoT because it is relevant for any type of distributed infrastructure that is completely different in nature and functionality. The secure intermediate gateway can discover all distributed information from different nodes and can exchange all messages and information through the unauthenticated network of the Internet.

Having policies and standards is not enough to ensure security, mechanisms to implement such policies are also required. Neisse et al.'s research in has addressed this issue by integrating a security tool called Security Kit with the MQ Telemetry transport protocol.

S. Awareness of security

Another important security measure for the success and growth of the IoT framework is awareness among

human users who are part of the IoT network. In the authors have explained the consequences of IoT insecurity using real numbers that the devices in IoT with Use the default password that has been made available to the public. The recorded results were very interesting and showed that many of these devices were actually available. People should be aware of the lack of awareness and do not use the minimum security such as the default password in the product, not changing the password makes IoT more harmful and harmful. In fact, if one of its devices is not secure, hackers can attack. against the entire network.

T. The current state of research

IoT security is determined by many factors and security principles discussed earlier, and the challenges facing IoT security have been the focus of many researchers. In this section, the analysis of some related works is presented and the contribution of this paper is given.

In the survey article provided by Roman et al. [6] , a detailed introduction to IoT and security issues that require standards is stated. However, no countermeasures are provided for the given security challenges. This was followed by a survey analysis in [7] where countermeasures were presented for all security challenges; Zhao and colleagues in [2] tried to describe the security issues in each layer with specific security measures, but in the end no solution except encryption in the perception layer in the paper as the optimal data solution. can't In [1] analysis and security threats, challenges and requirements are described in detail, but advanced countermeasures are presented only for one security feature of access control. In [23] , IoT security is only considered in terms of security principles such as confidentiality, integrity, and availability, and the authors proposed two-step authorization using biometrics, which is not applicable to machine-to-machine communication. In [18] shows open challenges to achieve centralized autonomy in IoT devices by having a management center that verifies identity in IoT. Slow, there is**.**

Conclusion

The IoT framework is susceptible to attacks at every layer, hence there are many security challenges and requirements that

must be addressed. The current state of research in IoT is mainly focused on authentication and access control protocols, but with the rapid development of technology, it is necessary to include new network protocols on IPv6 and 5G platforms. The major developments that are observed in IoT and are mainly ongoing are on a small scale, that is, within companies, some industries, etc., and also the IoT framework is different from one company to another, which needs to be modified. Companies and systems have various security concerns, and to take advantage of the high potential of IoT, steps must be taken to change the way life and future are changed. But, the most important concern in realizing fully intelligent frameworks is security. If security such as privacy, confidentiality, authentication, access control, trust management, global policies and standards are fully utilized, we can see everything being revolutionized by IoT in the near future.

There is a need for new identifiers, changes in wireless devices, new software and hardware, as well as technology to solve currently open IoT research challenges, such as standards for heterogeneous devices, implementing key management, and establishing identity systems. and trust management centers that can still be suitable research subjects.

Author Contributions

A. Zamani and S. Ziari designed the experiments. S. Ziari collected the data. S. Ziari carried out the data analysis. A. Zamani and S. Ziari interpreted the results and wrote the manuscript.

Acknowledgment

The author gratefully acknowledges the M. Abomhara . M. Farooq , M. Waseem , A. Khairi, and S. Mazhar their work on the original version of this document.

Conflict of Interest

The author declares that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancy have been completely observed by the authors.

References

[1] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *Int'l Conference on Privacy and Security in Mobile Systems (PRISMS),* 1-8, 2014.

[2] K. Zhao and L. Ge, "A survey on the internet of things security," in *Int'l Conf. on Computational Intelligence and Security (CIS),* 663-667, 2013.

[3] Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in *Applied Mechanics and Materials*, 1430-1432, 2014.

[4] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P.Agrawal, "Choices for Interaction with Things on Internet and Underlying Issues," *Ad Hoc Networks,* 2015.

Books:

[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *J. of Cyber Security and Mobility,* vol. 1, 309-348, 2013.

[6] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer,* vol. 44, 51-58, 2011.

[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.

Papers Presented at Conferences (Unpublished):

[8] 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.

[9] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in *Int'l Conference on Cloud Computing and Intelligent Systems (CCIS),* 1062-1066, 2012.

[10] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in *Int'l Conference on Modelling, Identification and Control (ICMIC),* 563-566, 2011.

[11] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in *Int'l Symposium on Next-Generation Electronics (ISNE),* 1-2, 2014.

[12] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capabilitybased access control delegation model on the federated IoT network," in *Int'l Symposium on Wireless Personal Multimedia Communications (WPMC),* 604-608, 2012.

[13] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in *Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 165-172, 2014.

[14] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen,"Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," in *Joint Intelligence and Security Informatics Conference (JISIC),* 232-235, 2014.

Papers from Conference Proceedings (Published):

[15] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (sIoT)–when social networks meet the internet of things: Concept,architecture and network characterization," *Computer Networks,* vol. 56,3594-3608, 2012.

[16] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,*vol. 48, 203-209, 1987.

[17] M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny,*et al.*, "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," *Int'l Journal of Critical Infrastructure Protection,* vol. 5, 86-97, 2012..

[18] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security,privacy and trust in Internet of Things: The road ahead," *Computer Networks,* vol. 76, 146-164, 2015.

[19] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *Wireless Communications,* vol. 21,106-112, 2014.

[20] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *Communications Magazine,* vol. 53, 28-35, 2015.

[21] Pallavi Sethi and Smruti R. Sarangi,"Internet of Things: Architectures, Protocols, and Applications",Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035

[22] B. Sasikala, M. Rajanarajana, Dr. B. Geethavani, “Internet of Things: A Survey on Security Issues Analysis and ountermeasures”, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 5 May 2017, Page No. 21435-21442

[23] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *Perception,* vol. 111, 2015.