Security Issue in Internet of Things

Ramesh Chandra Goswami and Hiren Joshi

Abstract Internet of things is a revolution after the Internet technology in the digital world. Internet of things plays a vital role in many real-life applications such as healthcare, business, education, etc. These applications are very important which are facilitating in various fields of human day-to-day activity. As the facilities are increasing security comes into the picture. Internet is not a secure channel of communications for Internet of Things technology (IoT). In this paper, we discuss the security issue of Internet of Things.

Keywords Confidentiality · Integrity · Availability · IoT architecture · Internet of Things · Data flow

1 Introduction

In 1999 Kevin Ashton at MIT uses the word Internet of Things for the first time during his presentation at Procter and Gamble. It was initially invented to promote RFID technology. Internet of Things is gaining remarkable focus among the various industries and researchers. IoT refers to a device having some basic characteristics such as unique identity, ability to connect to other devices, and it must be powered by a long-life battery [1].

The key idea behind the IoT is to make a connection between anything with anyone, anytime and anywhere. To make interactions among them various devices are used such as sensors, actuators, RFID tags, and readers [2]. The financial market of the mobile network operators in different domains and applications area is approximately 1.3 trillion dollars [3].

R. C. Goswami (✉) · H. Joshi
Department of Computer Science, Gujarat University, Ahmedabad, India
e-mail: rameshsd4@gmail.com

H. Joshi
e-mail: hdjoshi@gujaratuniversity.ac.in

N. Sharma et al. (eds.), *Data Management, Analytics and Innovation*,
Advances in Intelligent Systems and Computing 1174,
https://doi.org/10.1007/978-981-15-5616-6_33

The technology evolving in the day-to-day life is making the human world more sophisticated, therefore IoT devices make day-to-day life stress-free. IoT devices are connected to the Internet and produce large volume of data. These devices are able to collect the data and send it over the Internet for applications/software analysis so that the user sitting in any part of the globe can easily track the usage and other data received from the device. In the background of the Internet of things encryption mechanism, security of communication, protection of sensor data, and cryptographic algorithms and various types of protocols are involved [4]. In 2012, nine billion devices were interconnected and by 2020 the estimated number is about to reach 24 billion [3]. According to statistics, earlier billions of devices were generating more than two Exabyte of data per day that are not connected to the Internet [5]. IoT has a massive scope as it facilitates a unique opportunity for businesses to turn data into insights. There are a large number of factors as well as drive for the adoption of IoT such as improved sensors technology, device connections, lifestyle, and mobility.

A large number of IoT devices are receiving and sending data. The volume of this data will be something that has never been assumed earlier. In short the volume of data is increasing in such a way that it is very difficult to track and identify the suspicious traffic on the network. Lacking such incidents will make a huge loss over the network. Cyberattacks are increasing in such a way that there is not even a single day when we don’t have an attempt to crack the internet security. The risk against IoT devices and services are on the increase [6].

2 Data Flow in IoT

The sensors of the IoT collect data from their environment under measurement and turn it into useful information. Based on readings of the sensors data some action is required to be taken and that is done by actuators. Actuators basically perform certain tasks on the environment, on a system, or on a device. After that data is sent to the data center or cloud systems. When data travel from device to the cloud may introduce privacy issues and delays. Several applications require a real-time decision and cannot tolerate the delays and jitters [7]. Security is an important issue among various challenges that occur in the area of IoT. The reason behind this is the objects that are accessible from any location through the Internet, so these objects and their network remains unprotected against various intrusions. So maintaining security in the system of IoT is an important task for the researchers. The concern of data security and privacy is very important in nature if they are not taken care of properly it will affect the growth of development and deployment of IoT infrastructure [8].

2.1 Cloud and IoT

Generally the huge amount of data generated by IoT is stored in a cloud-based server. Cloud computing is a distributed environment. The user does not know where the data is stored and the risk associated with it. Basically virtual technology of the cloud computing is used for sharing the data and several virtual machines share a single resource. Till the encryption of one piece of data is not completed the data is transparent and may be easily accessed by intruders. Cloud computing is not a fully secured place. The data stored in cloud platforms have access and can analyze and process it. In this processing phase data may be leaked. So there is security risk always associated with it when data is transmitted [9].

2.2 Challenges of Security

Some important security challenges are as follows:

i. Confidentiality

The confidentiality protects system data and information from unauthorized exposure.

ii. Integrity

Integrity protects data from threats such as those that may modify data. It confirms the reliability which means the data is not altered. It ensures its functionality by encryption and hashing algorithms [10]. In the IoT environment integrity also needs to be ensured.

iii. Availability

Information is available when needed to authorize users, i.e., an availability service is one that protects a system to ensure its availability. It is an important security threat. Denial of service (DOS) is a serious threat to availability [10].

iv. Authentication

Authentication provides access control for IoT systems by checking the user's credentials with the real users or data that is available in the server which allows integration of various IoT devices [11] (Fig. 1).

Confidentiality, Integrity, and Availability are issues in IoT which is impacting the business as well as humans. There are various components which are interacting and communicating with each other on the untrusted network. All the interaction which is happening among various devices must be secured by ensuring data, providing service, and restricting data.

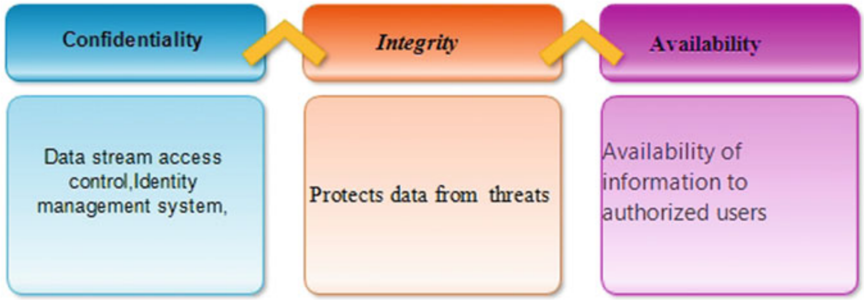
Confidentiality
Integrity
Availability
Data stream access control,Identity management system,
Protects data from threats
Availability of information to authorized users

Fig. 1 Confidentiality, integrity, and availability

Basically there are two types of security challenges faced by IoT devices which are Software Challenges and Hardware Challenges [12].

2.2.1 Software Challenges

i. The software that is installed in IoT devices is lacking security, i.e., they are not designed in such a way that can provide proper security.
ii. As the number of devices is increasing, the security risk is also increasing so the device should be designed in such a way that can update in runtime to make more secure.

2.2.2 Hardware Challenges

i. Due to limited memory and then low processing power the majority of IoT devices are not able to process complex security algorithms which therefore stop the execution of recent security applications on IoT devices.
ii. The life of the battery installed in IoT devices is also a challenge for security.

3 Architecture of IoT

There is lack of uniformity in IoT architecture. Different researcher communities propose different architecture. There are two views; one is three-layered architecture and the other is five-layered architecture. But the fundamental IoT model has three-layered architecture. This three-layer architecture was proposed in the early stage of development which is shown in Fig. 2. These three layers are perception layer, network layer, and application layer. Each layer has different functionality, hence each layer has different security issues [13]. The IoT layers are as follows:

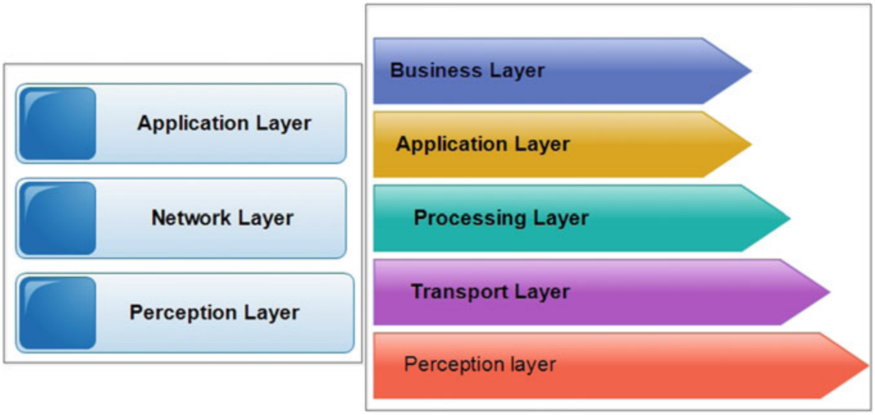

Fig. 2 Three-layered and five-layered architecture of IoT

i. Perception Layer

This is the lowest layer. It is also called the sensors layer or physical layer, which contains sensors for sensing and gathering information about the environment. The functionality of the perception layer is to identify, gather, process data, and then send to the network layer. In majority of cases it uses GPS, sensor, and Radio Frequency Identification (RFID).

ii. Network Layer

The network layer is mainly responsible for connection of smart object, devices, and various servers. Another important functionality of this layer is transmitting and processing of the data collected by sensors. In other words we can say that network layer is basically working routing of the data. It uses different technology such as Bluetooth, WIFI, and ZigBee.

iii. Application Layer

The application layer is basically responsible to deliver corresponding service to end users. This layer is directly involved to achieve the idea of IoT by facilitating smart environment applications such as smart city, smart transportation, smart homes, etc. The summarized functionality of each layer is shown in Table 1.

In five-layered architecture the perception, transport, processing, application, and business are mentioned. The two-layer perception and application are similar as in three-layered and functionality of the other three layers are as follows. Three- and five-layered architecture of the IoT are shown in Fig. 2.

iv. Transport layer

This layer transfers data that is collected from the sensor to the processing layer and vice versa through networks like Bluetooth, RFID, and NFC.

Table 1 Layer-wise functionality

SN	IoT layers	Functionality
1	Perception layer	Collect Process the data from the physical world
2	Network layer	Transmission Routing of packets
3	Application layer	Data processing Service providing

v. Processing layer

The basic functionality of this layer to is to store, analyze, and process data that is coming from the transport layer.

vi. Business layer

The business layer manages the complete IoT system such as applications, business and profit and also privacy of the users.

3.1 Layer-Wise Security Issue

It is well known that IoT is the integration of heterogeneous networks so it is difficult to achieve a trusted connection between different nodes in IoT. Data protection is a major challenge in IoT networks. Layer-wise security issue is as follows.

i. Perception layer

Dynamic nature of IoT increases the risk of different attacks. Basically these layers have sensors with RFID which has some security problem such as man-in-middle attacks, cloning attacks, and conflict collisions for RFID.

ii. Network Layer

IoT communication takes place between machines which are not following the standard protocols of security for communications and on the other side exchange sensitive information among each other. Attackers are able to access data related to different users from their IoT devices and it may possible they can use these data for malicious activity [14]. Noted attacks in these layers are wormhole attack, Sybil, and clone ID attack.

Table 2 Layer-wise security issue

SN	IoT layers	Security issue
1	Perception layer	Man-in-middle attacks Cloning attacks
2	Network layer	Wormhole attack Sybil attack Clone ID attack
3	Application layer	DoS DDoS

iii. Application layer

Many security issues arise because there is no standardization in the rules that look at interaction and application development process. It is very difficult to authenticate and secure data privacy when different applications have different authentication mechanisms. In this layer various attacks are DoS, DDoS, etc. At the time of designing application various factors should be considered such as different user interaction with the application and the, volume of data that will be generated [15].

The layer-wise security attacks are shown in Table 2.

4 IoT Applications

IoT applications are projected to equip billions of objects that are used in daily routine with connectivity and some level of intelligence. These major application areas are basically as follows:

i. Health Care

IoT has an important role in the health care sector. By using IoT the quality of service is increasing day by day and it also reducing the cost. In health care IoT can be used to monitor health services, monitor health inventory, and by providing various health e-services to needful peoples. Different functions of the human body such as glucose level, electrocardiogram, blood pressure, body temperature, and heart rate can be monitored by different sensors. The wearable body sensor is designed in such a way that it continuously tracks the activity of the patient which plays a deciding role in this direction. The use of smartphones is increasing day by day and these smartphones also have the functionality to control the latest electronic device. A typical smartphone is able to diagnose diseases such as cystic fibrosis, asthma, and can also detect some symptoms of the respiratory system [16].

ii. Smart grid

It is an electricity network which is based on digital technology to fulfill the demand of electricity to consumers. This uses bidirectional communication. It also provides monitoring, analysis, control, and communication for enhancing efficiency, reducing the consumption of energy, cost and enhancing the transparency, and reliability of the energy system. Modern grid is capable to store, communicate, and is able to take decisions while traditional grid can only distribute the electric power [17].

iii. Agriculture

Smart agriculture system can be classified in two ways first by plant monitoring and second by land monitoring. Plants can be measured by various sensors that can measure melanin, fertilizer, etc. On the other hand land monitoring can be done by sensors which can monitor temperature, moisture, humidity, etc. Basically in agriculture the purpose of this technology is to enhance the quality and to minimize the cost whereas WSN assists the farmers statistically which helps them for better and up to date decisions [18, 19].

iv. Smart Home applications

A smart home means a home with smart devices. Devices such as TV, laptop, AC, lights are smart which means that these devices take care of choices, feelings, and behaviors of humans. For example, intensity of light will change based on the intensity of sunlight. AC will adjust room temperature according to the temperature of the house.

v. Transport

Population is increasing day by day which impacts the public as well as private transport. IoT is playing a significant role in transport. Smart Parking, Traffic Congestion, Smart Roads are some implementations of IoT in the transportation sector.

5 Security Issue in IoT

The CIA features Confidentiality, Integrity, and Availability which are basic principles for majority of security and also true for IoT. In IoT network also having limitations due to which security is treated as a big challenge. A resource-constrained device cannot implement a foolproof security framework. Other things are lack of globally accepted standardization and protocols heterogeneity which are also issues. Every layer of IoT has some security issue. Majority of smart objects have several features which makes them different from the general computers for which different security mechanisms are developed. These smart objects have limited computation capacity such as microcontroller of smart object are not able to run asymmetric decryption algorithm within the required time limit. Because of these reasons security mechanism of IoT devices should be based on efficient encryption, decryption mechanism like symmetric encryption, and real environment where smart objects are operating is also different than that of general-purpose computers.

Apart from the computation constraint there is one more important thing that is power constraint of smart objects which leads to the security issue. For the purpose of maintaining low power smart objects keep their radios off. The attackers make radio on of the smart objects by sending false data to these devices and depleting its battery which breaches the availability property [18, 19].

6 Conclusion

The primary focus of this paper is to draw attention to major security issues of IoT devices. Due to poor security mechanism of IoT devices, it become a soft target for attack. Apart from this basic security, requirements are also discussed. In IoT devices and communication networks, it is also necessary to mount security mechanism. It is a common suggestion to protect the device from threat that do not use the default passwords and also false features of devices which are not in use. Doing such small steps will increase the security. IoT devices which are on wireless sensor networks are often physically exposed to the world which may create a problem. Similarly if we talk about network then at every level of the IoT network, security is required. Every endpoint on the network must be part of the overall strategy of security.

References

1. Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communication Surveys & Tutorials, 17*(4).
2. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the internet of things. *Digital Communications and Networks*, (4), 118–137.
3. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
4. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. In *International Conference on Computer Science and Electronics Engineering* (No. 3, pp. 648–651). IEEE.
5. Fog Computing. (2016). *The internet of things: Extend the cloud to where the things are.* Cisco Systems.
6. Abomhara, M., & Køien, G. M. (2015). *Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks.* Norway: Department of Information and Communication Technology, University of Agder.
7. Rauf, A., Shaikh, R. A., & Shah, A. (2018). Security and privacy for IoT and fog computing paradigm. In *15th Learning and Technology Conference (L&T)* (pp. 96–101). IEEE.
8. Wang, H., et al. (2015). Special issue on security, privacy and trust in network-based big data. *International Journal of Geographical Information Science, 318*(C), 48–50.
9. Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The internet of things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274.

10. Padmavathi, D. G., & Shanmugapriya, M. D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security, 4*(1), 1–9.
11. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Al-varenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications, 84*(January), 25–37.
12. Jain, A., & Singh, T. (2020). Security challenges and solutions of IoT ecosystem. In *Information and communication technology for sustainable development* (pp. 259–270). Singapore: Springer.
13. Mohammadi, M., Aledhari, M., Al-Fuqaha, A., Guizani, M., & Ayyash, M. (2015). *Internet of things: A survey on enabling*. IEEE.
14. Zhao, K., & Geo, L. (2013). A survey on the internet of things security. In *International Conference on Computational Intelligence and Security* (CIS) (pp. 663–667).
15. Huang, X., Craig, P., & Lin, H. Y. (2013). SecIoT: A security framework for the internet of things. *Security and Communication Networks, 9*, 3083–3094.
16. Sivagami, S., Revathy, D., & Nithyabharathi, L. (2016). Smart health care system implemented using IoT. *International Journal of Contemporary Research in Computer Science and Technology, 2.*
17. Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of smart grid technologies. *Renewable and Sustainable Energy Reviews,* 710–725.
18. Fang, S., Da Xu, L., Zhu, Y., Ahati, J., Pei, H., Yan, J., et al. (2014). An integrated system for regional environmental monitoring and management based on internet of things. *IEEE Transactions on Industrial Informatics, 10,* 1596–1605.
19. Kodali, R. K., Rawat, N., & Boppana, L. (2014). WSN sensors for precision agriculture. In *Region 10 Symposium* (pp. 651–656). IEEE.