Security Issues in the Internet of Things (IoT): A Comprehensive Study

Mirza Abdur Razzaq
Department of Computer Science
Shah Abdul Latif University
Khairpur, Pakistan

Muhammad Ali Qureshi
Department of Telecommunication Engineering
University College of Engineering and Technology
The Islamia University of Bahawalpur, Pakistan

Sajid Habib Gill
Department of Computer Science
NCBA & E Rahim Yar Khan Campus
Rahim Yar Khan, Pakistan

Saleem Ullah
Department of Computer Science & IT
Khwaja Fareed University of Engineering and IT
Rahim Yar Khan, Pakistan

***Abstract*—Wireless communication networks are highly prone to security threats. The major applications of wireless communication networks are in military, business, healthcare, retail, and transportations. These systems use wired, cellular, or adhoc networks. Wireless sensor networks, actuator networks, and vehicular networks have received a great attention in society and industry. In recent years, the Internet of Things (IoT) has received considerable research attention. The IoT is considered as future of the internet. In future, IoT will play a vital role and will change our living styles, standards, as well as business models. The usage of IoT in different applications is expected to rise rapidly in the coming years. The IoT allows billions of devices, peoples, and services to connect with others and exchange information. Due to the increased usage of IoT devices, the IoT networks are prone to various security attacks. The deployment of efficient security and privacy protocols in IoT networks is extremely needed to ensure confidentiality, authentication, access control, and integrity, among others. In this paper, an extensive comprehensive study on security and privacy issues in IoT networks is provided.**

***Keywords*—Internet of Things (IoT); security issues in IoT; security; privacy**

I. Introduction

Internet of Things (IoT) has attracted considerable attention during the past few years. The concept of IoT was firstly proposed by Kevin Ashton in 1999. Due to rapid advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency IDentification (RFID), and cloud computing, communications among IoT devices has become more convenient than it was before. IoT devices are capable of co-operating with one another. The World of IoT includes a huge variety of devices that include smart phones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices. The IoT devices are based on cost-effective sensors and wireless communication systems to communicate with each other and transfer meaningful information to the centralized system. The information from IoT devices is further processed in the centralized system and delivered to the intended destinations. With the rapid growth of communication and internet technology, our daily routines are more concentrated on a fictional space of virtual world [1]. People can work, shop, chat (keep pets and plants in the virtual world provided by the network), whereas humans live in the real world. Therefore, it is very difficult to replace all the human activities with the fully automated living. There is a bounding limit of fictional space that restricts the future development of internet for better services. The IoT has successfully integrated the fictional space and the real world on the same platform. The major targets of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others [2]. Nowadays the adoption rate of the IoT devices is very high, more and more devices are connected via the internet. According to appraisal [3], there are 30 billion connected things with approximate 200 billion connections that will generate revenue of approximately 700 billion euros by the year 2020. Now in China, there are nine billion devices that are expected to reach 24 billion by the year 2020. In future, the IoT will completely change our living styles and business models. It will permit people and devices to communicate anytime, anyplace, with any device under ideal conditions using any network and any service [4]. The main goal of IoT is to create Superior world for human beings in future. Fig. 1 shows the concept of IoT with their capabilities.

Unfortunately, the majority of these devices and applications are not designed to handle the security and privacy attacks and it increases a lot of security and privacy issues in the IoT networks such as confidentiality, authentication, data integrity, access control, secrecy, etc. [5]. On every day, the IoT devices are targeted by attackers and intruders. An appraisal discloses that 70% of the IoT devices are very easy to attack. Therefore, an efficient mechanism is extremely needed to secure the devices connected to the internet against hackers and intruders.

The rest of the paper is organized as: Section II discusses IoT applications while Section III provides a brief overview of security requirements followed by security threats in IoT are discussed in Section IV. Section V provides analysis of different attacks and their possible solutions and finally the paper is concluded in Section VI.

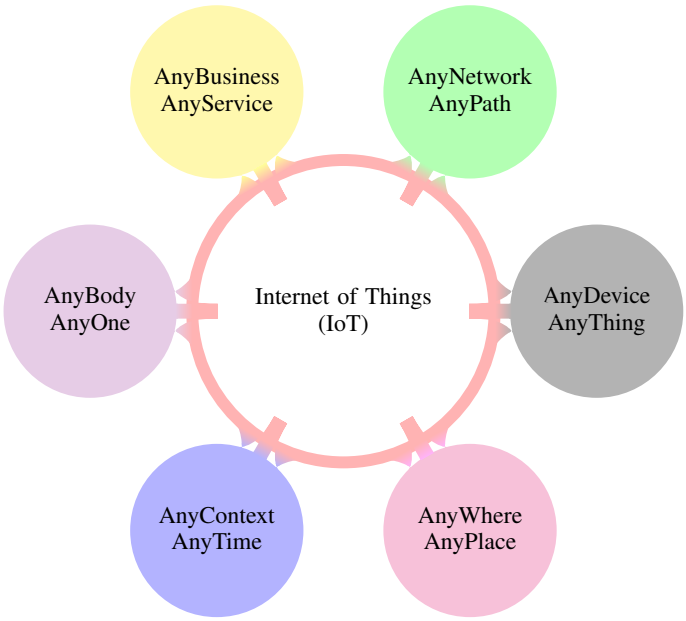

Fig. 1. Definition of IoT.

II. IoT Applications

The main objectives of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others [2]. The applications of IoT in industries, medical field, and in home automation are discussed in the following section.

A. IoT in Industries

The IoT has provided a fair opportunity to build significant industrial systems and applications [6], in an intelligent IoT transportation system, the authorized person can monitor the existing location and movement of a vehicle. The authorized person can also predict its future location and road traffic. In earlier stage, the term IoT was used to identify unique objects with RFID. Latterly, the researchers relate the term IoT with sensors, Global Positioning System (GPS) devices, mobile devices, and actuators. The acceptance and services of new IoT technologies mainly depend upon the privacy of data and security of information. The IoT permits many things to be connected, tracked and monitored so meaningful information and private data collected automatically. In IoT environment, the privacy protection is a more critical issue as compared to traditional networks because numbers of attacks on IoT are very high.

B. IoT in Personal Medical Devices

The IoT devices are also widely used in healthcare systems for monitoring and assessment of patients [7]. To monitor the medical condition of a patient, Personal Medical Devices (PMDs) are either planted in patients body or it may attach to patients body externally. PMDs are small electronic devices that are becoming very common and popular. The market value of these devices is projected to be around 17 billion dollars by 2019 [8]. These devices use a wireless interface to perform communication with a base station that is further used to read status of the device, medical reports, and change parameters of the device, or update status on the device. Wireless interface causes a lot of security and privacy threats for the patient. The wireless interface of such devices is very easy to cyber-attacks that may jeopardize the patients security, privacy, and safety. In the case of health care, the primary goal is to ensure the security of network in order to prevent the privacy of patient from malicious attacks. When attackers attack mobile devices, they have their predefined goals. Usually, their aim is to steal the information, attack on devices to utilize their resources, or may shut down some applications that are monitoring patients condition.

There are many types of attacks on medical devices that include eavesdropping in which privacy of the patient is leaked, integrity error in which the message is being altered, and availability issues which include battery draining attacks. Some cyber security threats related to security, privacy, and safety of medical data of patient are discussed as follows:

1) PMDs are critical to any task that uses battery power. Hence these devices must support a limited encryption. If the device is a part of different networks then confidentiality, availability, privacy, and integrity will be at high risk.
2) As PMDs have no authentication mechanism for wireless communication. So the information stored in the device may be easily accessed by unauthorized persons.
3) Absence of secure authentication also uncovers the devices to many other security threats that may leads to malicious attacks. A hostile may launch Denial of Service (DoS) attacks.
4) The data of patient is sent over transmission medium which may be altered by unauthorized parties, as a result privacy of a patient may loss.

C. IoT in Smart Home

The IoT smart home services are increasing day by day [9], digital devices can effectively communicate with each other using Internet Protocol (IP) addresses. All smart home devices are connected to the internet in a smart home environment. As the number of devices increases in the smart home environment, the chances of malicious attacks also increase. If smart home devices are operated independently the chances of malicious attacks also decreases. Presently smart home devices can be accessed through the internet everywhere at any time. So, it increases the chances of malicious attacks on these devices.

A smart home consists of four parts: service platform, smart devices, home gateway, and home network as shown in Fig. 2. In the smart home, many devices are connected and smartly shares information using a home network. Consequently, there exists a home gateway that controls the flow of information among smart devices connected to the external network. Service platform uses the services of service provider that deliver different services to the home network.

III. Security Requirements

In IoT, all the devices and people are connected with each other to provide services at any time and at any place. Most

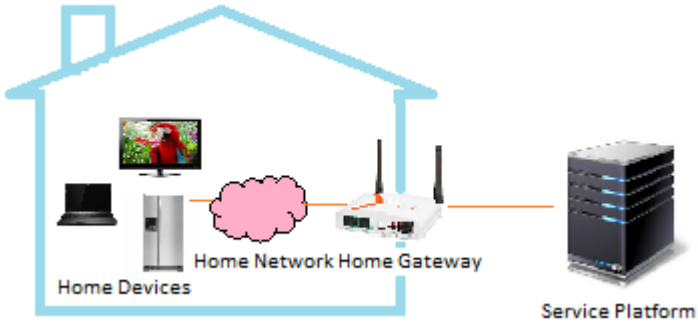

Fig. 2. Elements of a smart home in IoTs.

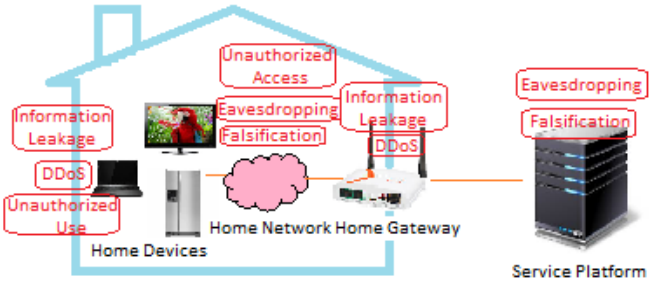

Fig. 3. Threats in smart home in IoTs.

of the devices connected to the internet are not equipped with efficient security mechanisms and are vulnerable to various privacy and security issues e.g., confidentiality, integrity, and authenticity, etc. For the IoT, some security requirements must be fulfilled to prevent the network from malicious attacks [7], [10], [11]. Here, some of the most required capabilities of a secure network are briefly discussed.

- **Resilience to attacks:** The system should be capable enough to recover itself in case if it crashes during data transmission. For an example, a server working in a multiuser environment, it must be intelligent and strong enough to protect itself from intruders or an eavesdropper. In the case, if it is down it would recover itself without intimation the users of its down status.
- **Data Authentication:** The data and the associated information must be authenticated. An authentication mechanism is used to allow data transmission from only authentic devices.
- **Access control:** Only authorized persons are provided access control. The system administrator must control access to the users by managing their usernames and passwords and by defining their access rights so that different users can access only relevant portion of the database or programs.
- **Client privacy:** The data and information should be in safe hands. Personal data should only be accessed by authorized person to maintain the client privacy. It means that no irrelevant authenticated user from the system or any other type of client cannot have access to the private information of the client.

IV. IoT Security, Privacy, Threats and Challenges

The era of IoT has changed our living styles [12]. Although the IoT provides huge benefits, it is prone to various security threats in our daily life. The majority of the security threats are related to leakage of information and loss of services. In IoT, the security threats straightforwardly are affecting the physical security risk. The IoT consists of different devices and platform with different credentials, where every system needs the security requirement depending upon its characteristics. The privacy of a user is also most important part because a lot of personal information is being shared among various types of devices [13], [14]. Hence a secure mechanism is needed to protect the personal information.

Moreover, for IoT services, there are multiple types of devices that perform communication using different networks. It means there are a lot of security issues on user privacy and network layer. User privacy can also be uncovered from different routes. Some security threats in the IoT are as follows:

1) **E2E Data life cycle protection:** To ensure the security of data in IoT environment, end-to-end data protection is provided in a complete network. Data is collected from different devices connected to each other and instantly shared with other devices. Thus, it requires a framework to protect the data, confidentiality of data and to manage information privacy in full data life cycle.
2) **Secure thing planning:** The interconnection and communication among the devices in the IoT vary according to the situation. Therefore, the devices must be capable of maintaining security level. For example, when local devices and sensors used in the home-based network to communicate with each other safely, their communication with external devices should also work on same security policy.
3) **Visible/usable security and privacy:** Most of the security and privacy concerns are invoke by misconfiguration of users. It is very difficult and unrealistic for users to execute such privacy policies and complex security mechanism. It is needed to select security and privacy policies that may apply automatically.

A. Security Threats in Smart Home

Smart home services can be exposed to cyber-attacks because majority of the service provider do not consider security parameters at early stages. The possible security threats in a smart home are eavesdropping, Distributed Denial of Service (DDoS) attacks and leakage of information, etc. Smart home networks are threatened by unauthorized access. The possible security threats to smart home are discussed as follows (see Fig. 3).

1) Trespass: If the smart door lock is effected by malicious codes or it is accessed by an unauthorized party, the attacker can trespass on smart home without smashing the doorway as shown in Fig. 4. The result of this effect could be in the form of loss of life or property. To get rid of such attacks, passwords should be changed frequently that must contain at

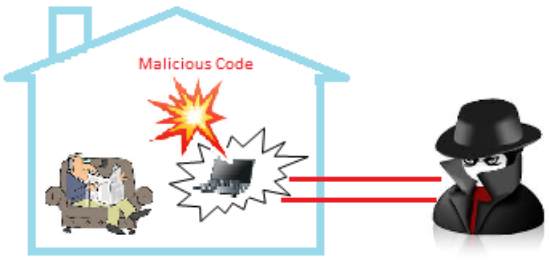

Fig. 4. An example of Trespass attack, hacking a door lock.

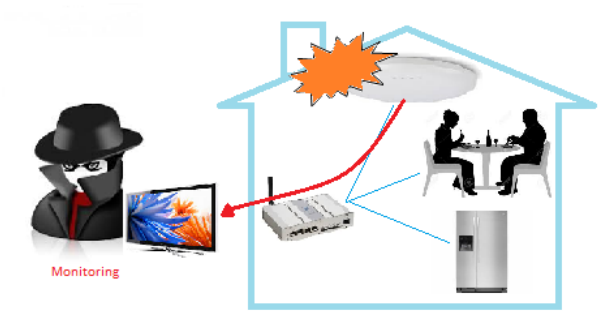

Fig. 5. An example of monitoring personal information.

least ten characters because it is very difficult for attackers to break the long password. Similarly, authentication mechanism and access control may also be applied.

2) Monitoring and personal information leakage: Safety is one of the important purposes of a smart home. Hence there are a lot of sensors that are used for fire monitoring, baby monitoring, and housebreaking, etc. If these sensors are hacked by an intruder then he can monitor the home and access personal information as shown in Fig. 5. To avoid from this attack, data encryption must be applied between gateway and sensors or user authentication for the detection of unauthorized parties may be applied.

3) DoS/DDoS: Attackers may access the smart home network and send bulk messages to smart devices such as Clear To Send (CTS) / Request To Send (RTS). They can also attack targeted device by using malicious codes in order to perform DoS attacks on other devices that are connected in a smart home as shown in Fig. 6. As a result, smart devices are unable to perform proper functionalities because of draining resources due to such attacks. For avoidance from this attack, it is very important to apply authentication to block and detect unauthorized access.

4) Falsification: When the devices in smart home perform communication with the application server, the attacker may collect the packets by changing routing table in the gateway as shown in Fig. 7. Although the SSL (secure socket layer) technique is applied, an attacker can bypass the forged certificate. In this way, the attacker can misinterpret the contents of data or may leak the confidentiality of data. To secure the smart home network from this attack, SSL technique with proper authentication mechanism should be applied. It is also important to block unauthorized devices that may try to access smart home network.

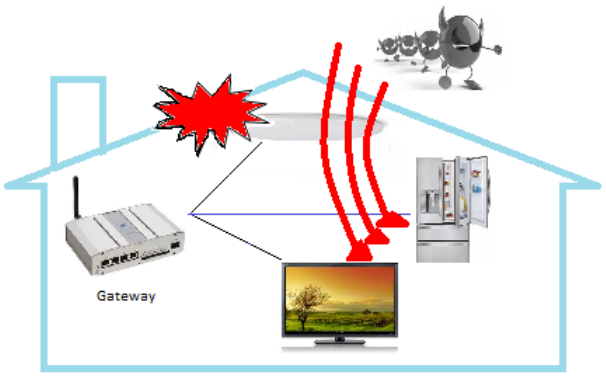

Fig. 6. An example of DDoS attack.

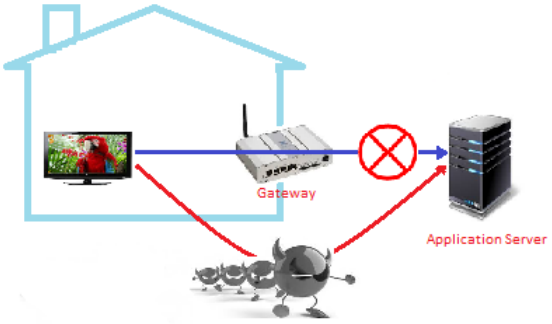

Fig. 7. An example of falsification.

The IoT is a concept that depicts future where the physical objects connected to internet communicate with each other and identify themselves for other devices [15]. The IoT system consists of smart objects, smartphones, tablets and intelligent devices etc. as shown in Fig. 8. Such systems use RFID, Quick Response (QR) codes or wireless technology to perform communication between different devices.

The IoT helped to build connections from human to human, human to physical objects, and physical object to other physical objects. As per appraisal from IDC, there will be 30 billion internet connected devices by 2020. This rapid growth of internet data needs more valuable and secure network.

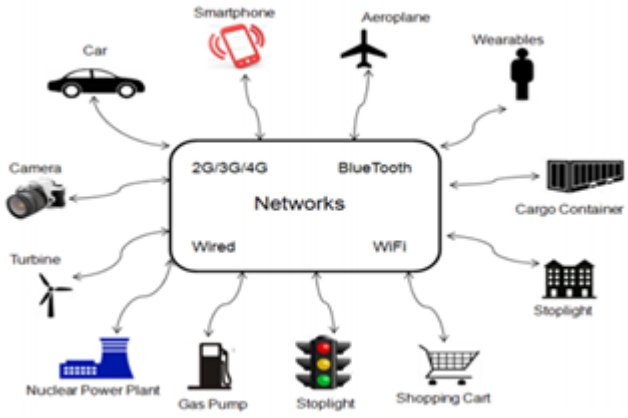

Fig. 8. Example of IoT system [16].

B. IoT Challenges

The security concern is the biggest challenge in IoT. The application data of IoT could be industrial, enterprise, consumer or personal. This application data should be secured and must remain confidential against theft and tampering. For example, the IoT applications may store the results of a patients health or shopping store. The IoT improve the communication between devices but still, there are issues related to the scalability, availability and response time. Security is a concern where the data is securely transmitted over the internet. While transporting the data across international border, safety measure act may be applied by government regulation such as Health Insurance Portability and Accountability (HIPA) act. Among different security challenges, the most important challenges relevant to IoT are discussed.

1) ***Data Privacy****:* Some manufacturers of smart TVs collect data about their customers to analyze their viewing habits so the data collected by the smart TVs may have a challenge for data privacy during transmission.

2) ***Data Security****:* Data security is also a great challenge. While transmitting data seamlessly, it is important to hide from observing devices on the internet.

3) ***Insurance Concerns****:* The insurance companies installing IoT devices on vehicles collect data about health and driving status in order to take decisions about insurance.

4) ***Lack of Common Standard****:* Since there are many standards for IoT devices and IoT manufacturing industries. Therefore, it is a big challenge to distinguish between permitted and non-permitted devices connected to the internet.

5) ***Technical Concerns****:* Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence there is a need to increase network capacity, therefore, it is also a challenge to store the huge amount of data for analysis and further final storage.

6) ***Security Attacks and System Vulnerabilities****:* There has been a lot of work done in the scenario of IoT security up till now. The related work can be divided into system security, application security, and network security [17].

a) System Security: System security mainly focuses on overall IoT system to identify different security challenges, to design different security frameworks and to provide proper security guidelines in order to maintain the security of a network.

b) Application security: Application Security works for IoT application to handle security issues according to scenario requirements.

c) Network security: Network security deals with securing the IoT communication network for communication of different IoT devices.

In the next section, the security concerns regarding IoT are discussed. The security attacks are categorized into four broad classes.

V. Analysis of Different Types of Attacks and Possible Solutions

The IoT is facing various types of attacks including active attacks and passive attacks that may easily disturb the functionality and abolish the benefits of its services. In a passive attack, an intruder just senses the node or may steal the information but it never attacks physically. However, the active attacks disturb the performance physically. These active attacks are classified into two further categories that are internal attacks and external attacks. Such vulnerable attacks can prevent the devices to communicate smartly. Hence the security constraints must be applied to prevent devices from malicious attacks. Different types of attack, nature/behavior of attack and threat level of attacks are discussed in this section. Different levels of attacks are categorized into four types according to their behavior and propose possible solutions to threats/attacks.

1) **Low-level attack:** If an attacker tries to attack a network and his attack is not successful.
2) **Medium-level attack:** If an attacker/intruder or an eavesdropper is just listening to the medium but dont alter the integrity of data.
3) **High-level attack:** If an attack is carried on a network and it alters the integrity of data or modifies the data.
4) **Extremely High-level attack:** If an intruder/attacker attacks on a network by gaining unauthorized access and performing an illegal operation, making the network unavailable, sending bulk messages, or jamming network.

The Table I presents different types of attacks, their threat levels, their nature/behavior, and possible solution to handle these attacks.

VI. Conclusion

The main emphasis of this paper was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. In this survey, twelve different types of attacks are categorized as low-level attacks, medium-level attacks, high-level attacks, and extremely high-level attacks along with their nature/behavior as well as suggested solutions to encounter these attacks are discussed.

Considering the importance of security in IoT applications, it is really important to install security mechanism in IoT devices and communication networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networks.

TABLE I. A SUMMARY OF DIFFERENT TYPES OF ATTACKS AND THEIR THREAT LEVELS, THEIR NATURE AND SUGGESTED SOLUTIONS

Type	Threat level	Behavior	Suggested Solution
Passive	Low	Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data.	Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques.
Man in the Middle	Low to Medium	Alteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data.	Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
Eavesdropping	Low to Medium	The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked.	Apply encryption on all the devices that perform communication.
Gathering	Medium to High	Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered.	Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks.
Active	High	Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker.	Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person.
Imitation	High	It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data.	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack.
Privacy	High	Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy.	Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature.
Interruption	High	Affects availability of data. This makes the network unavailable.	Applying authorization, only authorized users are allowed to access specific information to perform certain operation.
Routing diversion	High	Only the route is diverted showing the huge traffic and the response time increased.	Ensure connectivity based approach so no route will be diverted.
Blocking	Extremely High	It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network.	Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks.
Fabrication	Extremely High	Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information.	Data authenticity can be applied to ensure that no information is changed during the transmission of data.
DoS	Extremely High	Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices.	Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.

REFERENCES

[1] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.

[2] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), International Conference on*. IEEE, 2014, pp. 1–8.

[3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct 2010.

[5] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015, pp. 21–28.

[6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[7] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in *Communications (ICC), IEEE International Conference on*. IEEE, 2012, pp. 6121–6125.

[8] A. Mohan, "Cyber security for personal medical devices internet of things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*. IEEE, 2014, pp. 372–374.

[9] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in iot environment," in *Computer Science and its Applications*. Springer, 2015, pp. 691–696.

[10] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23–30, 2010.

[11] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)," in *International Conference on Network Security and Applications*. Springer, 2010, pp. 420–429.

[12] Y. H. Hwang, "Iot security & privacy: threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*. ACM, 2015, pp. 1–1.

[13] M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative analysis and implementation of efficientdigital image watermarking schemes," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 4, p. 558, 2012.

[14] M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, "Digital image security: Fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 5, 2017.

[15] S. Singh and N. Singh, "Internet of things (iot): Security challenges, business opportunities & reference architecture for e-commerce," in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*. IEEE, 2015, pp. 1577–1581.

[16] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The Internet Society (ISOC)*, pp. 1–50, 2015.

[17] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.