Direct Research Journal of Engineering and Information Technology
Vol. 12 (1), Pp. 1-10, March 2024
ISSN: 2354-4155
DOI: https://doi.org/10.26765/DRJEIT19928475
Article Number: DRJEIT19928475

Internet of Thing (IoT) Privacy and Security Issues

Umosor, Egiegbai Wilson*, Idewoh, Omotomhe Grace, and Akhuewu, Divine Emoata

Department of Computer Science, School of Information and Communication Technology, Auchi Polytechnic, Auchi Edo State, Nigeria.
Corresponding Author E-mail: umosorwilson@gmail.com

Received 8 February 2024; Accepted 16 March 2024; Published 21 March 2024

ABSTRACT: The Internet of Things (IoT) is a network that connects various devices to the Internet using specific protocols, allowing for the exchange of information and communication to enable smart functionalities such as recognition, positioning, tracing, monitoring, and administration. This paper provides a brief overview of IoT, its enabling technologies, architecture, characteristics, security threats, potential remedies, and applications. It also discusses the functional view of IoT and future challenges. The main advantage of IoT is its significant impact in creating a new dimension in the world. Key features necessary for implementing a large-scale IoT include low-cost sensors, high-speed and error-tolerant data communications, intelligent computations, and a wide range of applications. This research is presented in four main sections: an overview of IoT technology, a summary of related surveys, a review of main IoT applications, and a section on security challenges, potential attacks, and solutions for IoT.

Keywords: Internet Recognition, positioning, tracing, monitoring
Citation Umosor, E. W., Idewoh, O. G., and Akhuewu, D. E. (2024). Internet of Thing (IoT) Privacy and Security Issues. Direct Res. J. Eng. Inform. Tech. Vol. 12 (1), Pp. 1-xx. https://doi.org/10.26765/DRJEIT19928475

INTRODUCTION

Internet of Things (IoT) is simply a collection of many connectable objects (nodes) that can communicate and share information to accomplish common tasks (Adat,2018) Objects can be a person, mobile phones, home appliances, doors, cars, animals or anything else you can imagine. Each object is attached to a sensor that enables it to connect with the environment. IoT connects personal, business, industrial, and public-sector devices to each other, where the information can be sorted, analyzed, and stored. It has many applications in transportation, healthcare, energy production, and distribution. ITU-T defines IoT as: “Global infrastructure for the society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” (Leloglu, 2017). IoT can be integrated with wearable devices mainly consist of sensor nodes that the ability of transmitting data.

Very little processing often takes place within this type of devices, relying on remote services or nodes to perform the computational workload. The information collected by these devices can range from a simple heartbeat, to temperature and humidity data, to energy consumption patterns, all while providing functionality such as health monitoring and home automation. Because of the type of information these devices gather and store, they become prime targets for attackers. 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. On every day, the IoT devices are targeted by attackers and intruders. IoT solutions not only involve various technology domains such as mobile communications, cloud, data, security, telecommunications, and networking but they also lead to

Figure 1: IoT smart Capabilities and applications (Sadeeq *et al*., 2018).

cross-industrial use of data (for example, data generated in smart home and industrial applications is used in the automotive domain) (Figure 1). This opens a possibility for establishing business partnerships between horizontal industries, such as telecommunication operators, and vertical industries, such as car manufacturers, as new business models. IoT-enabled digital transformation of business is much more than just using connected objects it makes it possible to develop innovative business models that were impossible before.

Literature review

Theoretical literature

In this paper, a review of related theoretical scholarship will be conducted to align with the context of the study. It is widely acknowledged that the ongoing phenomenon of human cultural evolution, amplified by the rapid pace of technological advancement, is propelling the human race into what is commonly referred to as the information or computer age (Turban et al., 2017). Literature serves as a valuable resource for comprehending the subject matter, offering insights into previous work, solutions to existing challenges, and potential approaches for addressing them. A thorough examination of IoT privacy and security issues/concerns is essential. As highlighted by Meng et al. (2018), challenges such as jamming, spoofing attacks, and unauthorized access have jeopardized the integrity of user data. However, there exist potential solutions that individuals can implement to enhance the security of their IoT devices.

The emergence of various privacy threats in the current era has raised concerns about the security of IoT technologies and their integrated networks (Siby et al. (2017). Managing the security of IoT devices in businesses and organizations has become increasingly challenging. To address this, organizations must deploy monitoring and scanning tools for IoT devices to detect and mitigate privacy-related threats. Traffic interceptors and analyzers play a crucial role in identifying and investigating cyber threats. Despite the numerous benefits of the Internet of Things, cybersecurity and privacy risks remain significant concerns. These challenges pose a predicament for both business and public organizations, especially in light of high-profile cybersecurity attacks that have exposed the vulnerabilities of IoT technologies. The interconnectivity of IoT networks with the wider internet necessitates the development of novel security solutions to address accessibility from anonymous and untrusted sources. Emphasizing the standards and basic principles of the IoT Cyber Security Framework is essential for implementing a robust IoT security system. Leloglu (2017) underscores the importance of addressing these challenges to ensure the secure and reliable operation of IoT technologies.

Liu et al. (2019) emphasize the importance of considering the termination of contracts involving different devices with varying communication protocols in the context of cyber security for the Internet of Things (IoT). The presence of diverse protocols can impede the implementation of separate service contracts and is a crucial aspect of the cyber security structure for IoT. To ensure the reliability of the IoT framework in the cyber security domain, it is essential to take small steps to mitigate the challenges associated with IoT cyber security. Furthermore, scalability is identified as a key measure of success for the cyber security IoT framework. Analysts highlight the need for the IoT environment to be

scalable enough to address the multitude of Internet-related and cyber security challenges. Additionally, the IoT cyber security environment should support various testing methods, including integration testing, component testing, system testing, and compliance testing, in order to effectively reduce challenges and risks.

In the current landscape, Ali et al. (2018) have outlined the existing IoT cyber security solutions, highlighting the implementation of basic security measures by suppliers. They assert that it may not be financially viable for suppliers to produce high-quality solutions, posing a challenge in developing effective cybersecurity measures for the Internet of Things. Additionally, Sadeghi et al. (2015) emphasize the pervasive nature of current embedded mobile and cyber-physical systems, encompassing industrial control systems, modern vehicles, and critical infrastructure. They point to ongoing trends and initiatives such as Industry 4.0 and the Internet of Things (IoT) as promising avenues for innovative business models and enhanced user experiences through robust connectivity and the utilization of advanced generations of embedded devices. The generation, processing, and exchange of large volumes of relevant data within industrial IoT systems have made them a prime target for cyber-attacks, posing potential physical harm and disruptions to people's lives. The need for robust cybersecurity and privacy measures is paramount due to the inherent threat they pose. The complexity of these systems coupled with the potential impact of cyber-attacks has given rise to new challenges for industrial IoT systems. Addressing these challenges will require the implementation of comprehensive security frameworks tailored specifically for industrial IoT systems. It is evident that current IoT systems have not yet reached the level of improvement necessary to adequately secure their essential functions.

The study and research of security issues in IoT have been of extreme significance. One of the main objectives in terms of IoT security is to ensure privacy, confidentiality, and better protection for every user, as well as guaranteeing the availability of various services offered by the IoT ecosystem. As a result, research in IoT security is gaining necessary momentum with the help of different simulation tools and multiple computational platforms (Izzat et al., 2020).

Conceptual framework

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 (Abomhara and Køien, 2014). The applications of IoT in industries, medical field, and in home automation are discussed in the following section.

IoT in industries

The emergence of the Internet of Things (IoT) has presented a valuable opportunity for the development of robust industrial systems and applications. Within the realm of intelligent IoT transportation systems, authorized individuals are able to actively monitor the current location and movement of vehicles, as well as predict their future locations and assess road traffic conditions. Initially, the term IoT was primarily associated with identifying unique objects through RFID technology, but it has since evolved to encompass a wide array of components such as sensors, Global Positioning System (GPS) devices, mobile devices, and actuators. The successful adoption and utilization of these new IoT technologies hinges greatly upon the protection of data privacy and information security. The IoT facilitates the interconnection, tracking, and monitoring of numerous entities, leading to the automatic collection of valuable information and sensitive data. Consequently, in the IoT environment, safeguarding privacy is a significantly more critical concern compared to traditional networks, given the heightened frequency of cyber attacks targeting IoT systems (Da Xu, He, and Li, 2014).

IoT in Personal Medical Devices

The use of IoT devices in healthcare systems has become widespread, particularly for monitoring and assessing patients (Tarouco et al., 2012). Personal Medical Devices (PMDs) play a crucial role in monitoring the medical condition of patients, either through internal implantation or external attachment. These small electronic devices are increasingly popular, with the market projected to reach a value of around 17 billion dollars by 2019 (Mohan, 2014). However, the wireless interface used by these devices for communication with base stations poses significant security and privacy threats for patients.

This vulnerability makes the devices susceptible to cyber-attacks, potentially compromising the security, privacy, and safety of the patients. In the healthcare context, the primary objective is to ensure network security to safeguard patient privacy from malicious attacks. Attackers often target mobile devices with the intention of stealing information, exploiting device resources, or disrupting applications that monitor patient conditions. It is crucial to address these security concerns to uphold the integrity and confidentiality of patient data.
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:

(i) 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.

(ii) As PMDs have no authentication mechanism for wireless communication. So, the information stored in the device may be easily accessed by unauthorized persons.

(iii) 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.

(iv) 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.

IoT in Smart Home

The IoT smart home services are increasing day by day, 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 (Yoon et al., 2015). 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 (Figure 3) below. 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.

METHODOLOGY

Architecture of interment of thing iot

The architecture contains 5 layers in (Figure 2). The layers include: Perception Layer, Transport Layer, Processing Layer, Application and Business Layer.

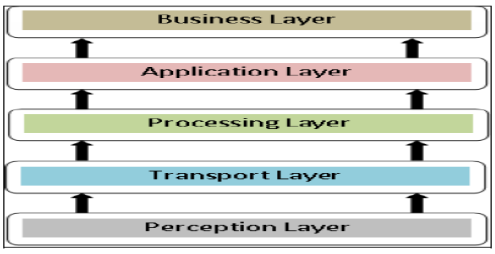

Figure 2:5-Layered Architecture of IoT Source: Aqeel et al. (2016).

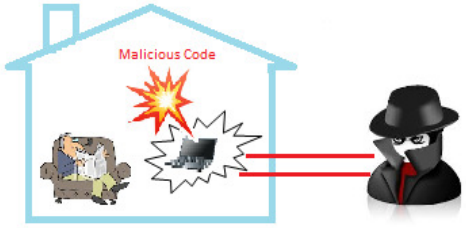

Figure 3: Threats in smart home in IoTs.

Perception layer

This is responsible for the identification of physical properties (e.g. location, temperature etc.) with the help of using various sensors used in IoT and performing conversion of signal to digital signal according to the transmission network. Sensing technology is the major technique for this layer which includes technologies like RIFD, GPS, 2-D barcode and so on.

Transport layer

Transport layer is often called Network Layer in 5 layer architecture used for the purpose of transporting the received data to the processing center. This transportation takes place through different network. IPv6 is considered to be the key protocol for this layer and FTTx, 3G, Wifi, Bluetooth, ZigBee, infrared technology are the important techniques used on this layer.

Processing layer

In the processing layer, all data transmitted from the transport layer is stored, processed, and analyzed. This layer involves the use of databases, intelligent processing, cloud computing, ubiquitous computing, and other advanced approaches. Experts consider the processing layer to be crucial for the future development and research of the Internet of Things. It is believed that further advancements in IoT can be achieved through innovations in the processing layer.

Application layer

The Application Layer is crucial for the functioning of IoT systems, as its tasks rely heavily on data from the processed layer. Its primary goal is to develop distinct IoT applications, such as intelligent transportation, logistics management, and identity authentication. These applications are essential for various industrial uses, and the Application Layer plays a key role in providing them.

Business Layer

The business layer plays a crucial role in managing tasks

such as application management and business model development. It is responsible for overseeing the realization and charge management of different applications, as well as conducting research on business and profit models. This layer recognizes that the efficiency of IoT depends on long-term development of the business model. Additionally, the business layer is accountable for safeguarding user privacy and conducting research related to IoT applications (Aqeel et al, 2016).

Security requirements

In the realm of IoT, the interconnectedness of devices and individuals enables the provision of services without constraints of time or location. However, a significant proportion of internet-connected devices lack robust security measures, rendering them susceptible to a range of privacy and security concerns such as confidentiality, integrity, and authenticity. To safeguard IoT networks from malicious attacks, it is imperative to adhere to specific security requirements as outlined in the works of Tarouco et al. (2012), Weber (2010), and Babar et al. (2010). These measures are essential for ensuring the integrity and reliability of IoT services in the face of potential threats.

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.

IoT security, privacy, threats and challenges

The era of IoT has changed our living styles (Hwang, 2015). 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 (Qureshi et al., 2012; Abdur et al., 2017).

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:

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.

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.

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.

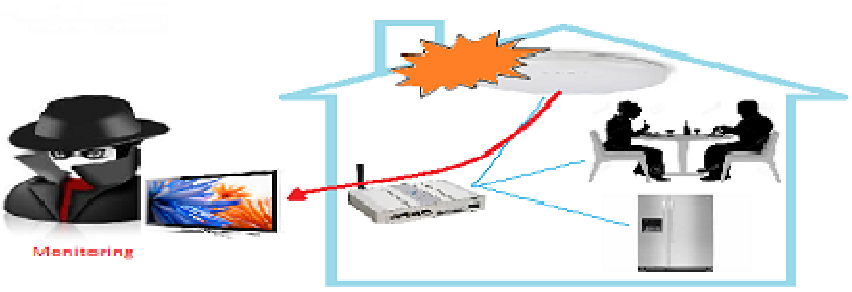

Figure 4: An example of Trespass attack, hacking a door lock. (Source: Abderahmanet, al 2019).

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 (Figure 4).

Trespass

If the smart door lock is affected by malicious codes or it is accessed by an unauthorized party, the attacker can trespass on smart home without smashing the door way as shown in (Figure 5). 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 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.

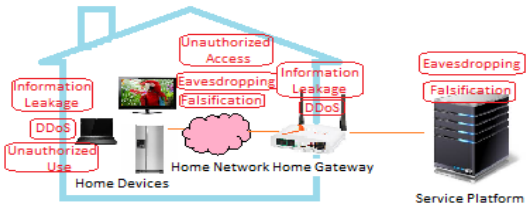

Figure 5: An example of monitoring personal information. (**Source:** Mirza et al., 2017).

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 (Figure 6). 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.

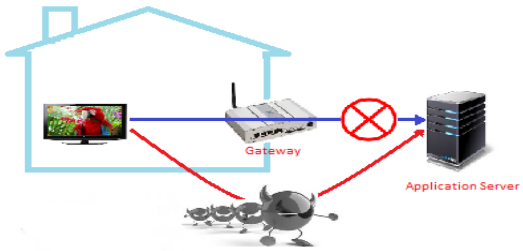

Figure 6: An example of DoS attack.(Source: Hassan and Abudurazzag, 2021)

Denial of service attack (DoS)

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 (Figure 7). As a result, smart devices are unable to perform proper functionalities because of draining resources due to such attacks. To avoid this type of attack, it is very important to apply authentication to block and detect unauthorized access.

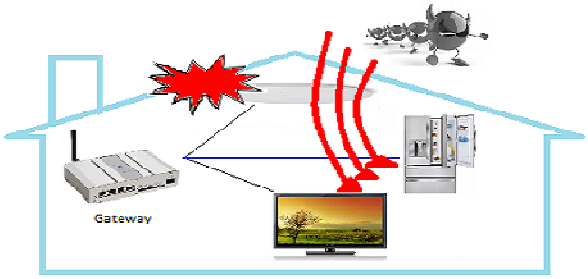

Figure 7: An example of falsification (Source: Hassan and Abudurazzag, 2021).

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 (Figure 8). 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. 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 . The IoT system consists of smart objects, smartphones, tablets and intelligent devices etc. as shown in (Figure 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.

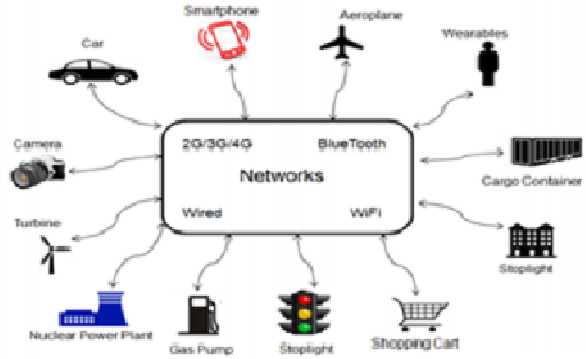

Figure 8: Example of IoT system (Source: Alberto et al., 2021).

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 patient's 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.

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.

Data security

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

Insurance concerns

The insurance companies installing IoT devices on vehicles collect data about health and driving status in order to take decisions about insurance.

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.

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.

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 (Ning et al. 2013).

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.

Application security

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

Table 1: Analysis of different attacks

Type	Treat level	Behaviour	Suggested solution
Passive	Low	Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Where attackers secretly listen the communication 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 impersonates 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.

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.

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 don't 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 1) below presents different types of attacks, their threat levels, their nature/behavior, and possible solution to handle these attacks.

Summary

The main emphasis of this seminar work 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 seminar work, the security requirements are discussed such as confidentiality, integrity, and authentication, etc. In the analysis, 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 were discussed.

Conclusion

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.

Recommendations

With the goal to achieve security and privacy in IoT, significant of research is needed. Some of the key areas for research are namely Scaling, Architecture and Dependencies, Utilization of Big Data, Robustness, Openness and off-course Security and Privacy. Since in IoT, large number of devices are connected together which in result affects the utilization of system, therefore, scaling of a system is required and research work need to be done in this domain for the successful working of IoT. Since there is no standard architecture for IoT and billions of objects are getting attached with the traditional internet day by day, it is very much important to have an architecture which is adequate in nature and allows easiness in connectivity, communication and control.

REFERNCES

Abderahman. R., John G., and Horst T.(2019). Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. Future Internet 2019, 11, 161.

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

Abomhara, M., and Køien, G. M., (2014). "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, pp. 1–8.

Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy.

Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019).Blockchain for Internet of Things (IoT) z

Ali, S., Bosche, A., and Ford, F., (2018).Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018.

Aqeel-ur-Rehman1, Sadiq Ur Rehman2, IqbalUddin Khan, MuzaffarMoiz and Sarmad

Babar, S., Mahalle, P., Stango, A., Prasad, N., and Prasad, R., (2010). "Proposed security model and threat taxonomy for the internet of things (IoT)," in International

Chen, S., Xu, H., Liu, D., Hu, B., and Wang, H., (2014)."A vision of IoT: Applications, challenges, and opportunities with China perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359.

Conference on Network Security and Applications. Springer, 2010, pp. 420–429.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and

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

forensics: Challenges and opportunities. doi.org/10.1016/j.future.2017.07.06

Hasan (2016). "Security and Privacy Issues in IoT" in International Journal of Communication Networks and Information Security (IJCNIS) Vol. x, No. x, November 2016.

Hassan, A., and Abdurazzag, A. (2021), An evaluation of machine learning classifiers for

Hassan, W. H., (2019). Current research on Internet of Things (IoT) security: A survey. Computer.Network. 2019, 148, 283–294.

Hossain, M. M., Fotouhi, M., and Hasan, R. (2015) "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.

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

Izzat, A., Chuck, E., and Lo'ai, T., (2020). The NICE Cyber Security

Framework, Cyber Security Management; Springer: Basel, Switzerland; ISBN 978-3-030-41987-5.
Kassem F. and Kang G. (2018), Security and Privacy in the Internet of Things. IEEE COMPUTER SOCI E T Y 001 8 -9162 / 19©2019 IEEE.
Khan, M. A., & Salah, K. (2018).IoT security: Review, blockchain solutions and 11.022
Leloglu, E., (2017)."A Review of Security Concerns in Internet of Things,"Journal of Computer and Communications, vol. 5, pp. 121-136.
Liu, X., Zhao, M., Li, S., Zhang, F., Trappe, W., (2019). A security framework for the internet of things in the future internet architecture.Future Internet 2017, 9, 27.
Meng, Y., Zhang, W., Zhu, H., and Shen, X. S., (2018). Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures.IEEE Wireless Communication. 2018, 25, 53–59.
Mirza, A. R., Sajid, H. G., Muhammad, A. Q., and Saleem, U., (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017 p.384.
Mohan, A., (2014). “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.
of Things security: a survey. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 162-166). IEEE.
prediction of attacks to secure Green IoTinfastruture. International journal of emerging trends in Engineering Research.Volume 9. No, may 2021
Qureshi, M. A., Aziz, A., Ahmed, B., Khalid, A., and Munir, H., (2015). “Comparative analysis and implementation of efficient digital image watermarking schemes,” International Journal of Computer and Electrical Engineering, vol. 4, no. 4, p. 558, 2012.
Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., Jacksi, K. (2018). Internet
Sadeghi, A. R., Wachsmann, C., and Waidner, M., (2015).Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
Siby, S., Maiti, R. R., and Tippenhauer, N. O., (2017). IoT scanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.
Tarouco, L. M. R., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M. R., Carbone, F., Marotta, M., and Santanna, de J. J. C., (2012). “Internet of things in healthcare: Interoperability and security issues,” in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
Turban, E., Maclean, E., and Wetherbe, J. (2017). Information technology for management.Transforming organizations in the digital economy. Hoboken, NJ: John Wiley & sons.
Weber, R. H., (2010). “Internet of things–new security and privacy challenges,” Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.
Yoon, S., Park, H., and Yoo, H. S., (2015).“Security issues on smart home in IoT environment,” in Computer Science and its Applications. Springer, 2015, pp. 691–696.