JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

Security Issues in Internet of Things (IoT): Challenges and Solutions

Syeda Hijab Zahra[1*], Mudassar Rehman[2], Gohar Mumtaz[1], and Sajid Iqbal[3]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[2]Riphah International University, Sahiwal, 57000, Pakistan.
[3]Department of Computer Science, University of Lahore, Lahore, 54000, Pakistan.
[*]Corresponding Author: Syeda Hijab Zahra. Email: hijabzahra585@gmail.com

Received: June 23, 2024 **Accepted:** August 16, 2024 **Published:** September 01, 2024

Abstract: IOT is a general topic for research purpose. IOT is quite popular and has become a vital part of our lives. IOT is crucial to self-sufficiency, smart environments, health care, smart cities, and micro-grid systems. If we talk about the meaning of the internet of things, it is defined as the paradigm which involves objects that provide actuators, sensors and processors that communicate with one another for serving the meaningful purposes. Sensing, Processing and data transmission are the three important components of IOT. IOT technology improved great in recent year but there are still some problems in IOT which require the attention. One of the main problems is security. Security is crucial for IOT devices due to sensor's generation and sharing of personal data and blending the physical and digital realms. Implementation of encryption methods are crucial for IOT system. So, the main objective of this article to pinpoint the challenges for the security and problems which arise in environment of IOT. Security is one of the key concern with IOT technology. In this paper we explained security problems, challenges and solution of internet of things.

Keywords: IOT (Internet of Things); Privacy; Security; Attacks; Challenges; Solutions.

1. Introduction

Now these days we are going towards the connected systems. Development in advance technology has changed the lives of peoples, among the utmost well-known and recent is Internet of things [1]. The internet of things transforms connectivity anytime, anywhere for anyone [2]. Smart technologies are playing an important role in our daily life and we are existing in the era of smart technologies that represents "Ubiquitous Computing". IOT is emerged strongly more prosperous for express this types of new technology. It is not first technology in this field but cloud computing used for represent the ubiquitous computing. In seventh internally reports originally IRU that was launched in 1997 whose title was "challenges to the network" [3]. It first coined by Kevin Ashton in 1999 journal [4]. In 2005 its name changed with internet of things IOT [5]. Currently IOT is an emerging topic and technology which is considered as the future of the internet. Allowing devices/ things for self-configuring capabilities that has based on standard and Interoperable communication (ICP) protocol that identify and use the intelligent interface over infrastructure of dynamic global network [6] [7].

IOT concept is considered to be an extension of existing interaction between application communication and humans through new dimensions [8]. In business, IOT have enormous potential for different kinds of the organizations and companies in which include the service provider, IOT applications IOT platform provider, software vendors and telecom operator [7] [8]. Moreover, IOT will be an important impact especially in the higher education [9]. With the increase of IOT and use of IOT, many issues related to security have raised. As devices, things have to become internet structure part, accordingly such issues must be examined. As everything becomes interconnected by internet, this issue become increasingly significant. The continual worldwide internet exposure reveals several security vulnerabilities. These

security weaknesses are exploited via hackers, and they can be misused it in any uncontrolled environment by Internet of Things devices [7]. Moreover, IOT increase potential attack surface for the hackers and for other cyber criminals. A study that is conducted by the Hewlett Packard [10] revealed 70% of most common Internet of things devices contained on the serious vulnerability.

These devices contain vulnerability to security threats due to design which involve lack of the security features such as medium that is insecure insufficient authentication and also the authorization configuration. It is true that when the IOT becomes for everyone either for individual or for the companies and anywhere will concerned. In addition, crosslinking of the objects presents the new potential to influence and to be exchange. That has to be lead with the new risks that concerns with the information security and protection of the data, which need to be considered. Furthermore, lack in security creates the resistance for the adoption for IOT by the companies and individuals. Issues related to security and challenges can addressed by providing the training to developer and also to designer for integrate the security solutions into product of IOT thus encourages to the users to utilize the security features of IOT that has to be built into the devices [7]. Our motivation is to conducting the paper that provide the review on main issues of IOT related to security and that paper provides the solutions.

2. Literature Review

The Internet of Things allows considerable interconnection between devices, which improves usefulness while also posing significant security issues. IOT security is multidimensional, addressing concerns such as data protection, authentication, and system vulnerabilities. The large volume of sensitive data transmission across the network is a critical security issue in IOT. Sheer volume of data transmitted between devices demands robust security mechanism to prevent from data breaches and unauthorized access [3]. This risk is reinforced by the diverse variety of devices and communication protocols used is IOT systems, which raises the complexity of network security [2]. Authentication and authorization is more difficult in IOT system. Many IOT devices use simple authentication techniques which are insufficient against sophisticated attacks. According to [4] standard authentication mechanism may not be suitable for the IOT devices, which have limited resources. It makes them more vulnerable against unauthorized access. There have been variety of solutions offered to overcome these challenges. Advance cryptographic techniques may enhance security in IOT devices [1]. Regular updates and automatic patch management is crucial to mitigate vulnerabilities, as they ensure devices remains protected against emerging threats [4]. According to [14][19] they discuss about emerging security threats such as reply attacks and SYN flood attacks and give insights into particular vulnerabilities and potential mitigation strategies. [16] Conduct a comprehensive review on the man-in- the-middle attack, which is common threat in IOT due to frequently unprotected communication channel. [20] Contributes in the discussion by analyzing password cracker's ability to target specific passwords. This study highlights the issues of password security in IOT system, where weak or reused password can compromise device security. Similarly, [21] highlights the various types of attacks faced by IOT with an extensive overview on threat landscape to highlight the need of implementing strong security measures to mitigate risks associated with such attacks.

2.1. IOT Architecture and Security issues in layers of IOT

An Internet of Things environment that can use the internet to connect heterogeneous items. That's why there has to be need for elastic, adjustable architecture. IOT architecture has to be divided into three layers in which involve Presentation, Network and Application layers.

2.2. Perception Layer

This layer of the IOT collects information with sensing devices in which involve ZigBee, RFID and all other types of sensors. RFID helps to identify anything that has been tampered with to operate as an electronic barcode and allows microchips to be designed for wireless data communication [11]. Collected Data transmits with through the wireless network transmission. Some attacks occurred in this layer are the Fake node or malicious data, Denial of service and Reply attack etc. [12].

2.3. Network layer

Network layer supports the secure transformation of data on sensors networks and also it responsible for routing. This layer transfer data through the wireless technology such as Bluetooth, Wi-Fi,

infrared etc. [13]. Hence network layer is accountable for transmission of data from perception layer to upper layer. There have some problems in Wi-Fi, LAN and Internet. These have the illegal access of the network, confidentiality and integrities damages, and denial of service attack, eavesdropping and main in the middle attack.

2.4. Application Layer

It is the uppermost layer within the architecture of Internet of Things. It provides the delivery of the all services in different fields. It includes intelligent transportation, cloud computing, environmental monitoring. This layer has security problems such as the security of the data, data protection and also the recovery. To solve the problem related to security, privacy protection and authentication are needed. The important part for data security is password management [14].

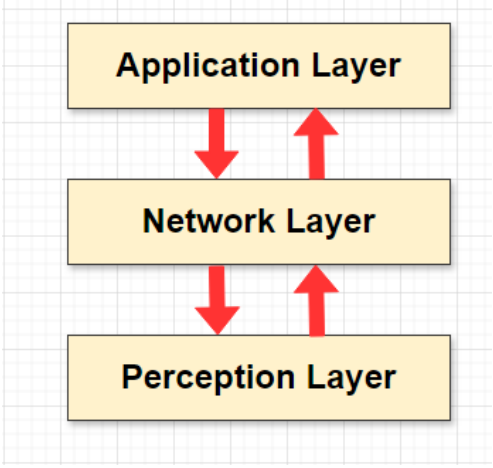

Figure 1. IOT Layers

3. Security Issues in IOT

Testing mechanism, protection both of these are the important in the implementation of Internet of things programs. We are highlighting the security issues that are top security issues that can considered which help you to build the attack proof internet of things application and connected devices. Followings are the main security concerns in which involve Denial of Service Attack (DOS), Reply Attack, Password Guessing Attack, Spoofing Attack, Insider Attack etc.

3.1. Denial of Service Attack (DOS)

It is a security breach that intends to prevent legitimate users and the entities from having legal access to the resources of the network. It is one of the most popular and also the domain attack. It comes from the single computer that sends the multiple requests to the server. This attack aims to have the overload the system or the server with request for the access of data or the resources like processor or main memory. Most of the Denial of Service (DOS) targets the servers of banks, Governments, E-commerce sites. When the Denial of Service Attack happened the sites have stopped for displaying the contents. DOS Attack can target more than one systems or sites at one time [15].

3.2. Reply Attack

Reply attack is considered one of the old attack in the network communication, especially in the authentication and the key exchanging of the protocol. It allows to the pirate the ability to store all or a fragment of the intercepted session in the authentic traffic [16] [17]. Later an attacker gains confidence in the unrestricted networks, they send intercepted messages to an individual that needs to be participated in the session of origin or in diverse location [18]. Responding to an attack on internet of things requires measuring a security vulnerability in which certain data must be kept without permission before being sent back to the sender. The aim of this assault is to ensure an individual in an authorization procedure [19]. Example involve in this is temperature sensors that has to be used for the detection of the temperature and then measured values are sends to the controller of the system. Based on values system run or stop the air conditioner for adaptation of the air temperatures this has to be desired by personal. If the attacker

prated temperature of the sensors he can saved the values of days and can send at the night. In this result the conditioner shall not be the functionally normally. To deals with the reply assault, solutions used the three mechanism that involve the timestamp, response challenge and nonce. First mechanism that has to be used for the detection of the reply occurrence by checking the freshness of the received messages. Assuring the time synchronization between objects of IOT is hard [20].

3.3. Password Guessing Attack

Many of the others methods are used for the crack of user password one of the prominent methods is the password guessing attack. In this technique attacker crack the password. This process includes to attempt of gain access of the system by trying the all possible passwords. Generally, attackers use the dictionary base password for guessing the password. If the attacker guises the password than he can access the remotely system access, and can steal the data and can demand for the ransom in exchange for data of system [21].

3.4. Spoofing Attack

Spoofing assault is the condition where the illegitimate object produces forged restriction [22]. The objective of the attack is to make the server consider that attacker is a legitimate individual [23]. It is a type of attack that involve communication from the unknown sources are disguised for being for the source that is known and trust by recipient. In this type of attack, attacker gains the confidence of the authorities. E.g., attackers send the false info in smart health to the authentication server and if attackers accomplished phase of validation effectively, then he should request to the victim sensor and can gain the secret information [24].

3.5. Insider Attack

An insider assault is when an employee uses the authorized access to harm the organization destroying, exposing, or stealing the organization's data. Employees can do this work individually or with the help of an outsider hacker or group of hackers [25]. The action of the authorized person can be accidental or intentional. In both of these cases, the system has considered vulnerable, and in the short term, we find the solutions. According to [26] business data almost more than 57% have a target from insider attacks [27].

3.6. Vulnerabilities

Vulnerabilities is a big problem that is recently facing by the organization and the users. Main reason for Internet of Thing devices are weak since they lack computational capability for built in safety. One more main purpose through which weaknesses should be persistent is inadequate budget for test and develop safe firmware, which is inclined by cost point of the devices besides their diminutive growth of progression. IOT devices are exposed because they lack computational capacity for built in security. Weak type of modules affecting the millions of devices. For IOT devices weaknesses in the software and in web application can lead to the compromised system. Malware operators are searching for this type of opportunities, and they have knowledge about the older vulnerabilities [28].

3.7. Encryption Issue, lacking of the Encryption

When the devices communicate with each other in the plain-text, almost all data that Is exchanged with backend service or client service get by the main in middle attack. Typically, login details can be accessed by the main in the middle attack. A main in the middle attack access communication secretly without participating in this communication. That's why its solution has to be choose the encrypted version rather than the plain version [29].

3.8. Ransomware Attack in IOT

A type of malware attack in which attacker encrypt the data (victim), and files that are important and then demanding for payment for unlocking or decryption of the data. This attack has an advantages on IOT devices, computer mobiles devices etc. [30]. Ransom-ware in IOT is not a new discussion. When IOT had started to expand and ransom-ware were increasing, security experts began to looking the potential ransom-ware attack risks. Now different others ransom-ware are targeting the organizations and uses of the IOT has spread in the organizations and industries [31].

3.9. Gateway Attack

These types of attacks cut the connection between the infrastructure of the internet and the sensors. Gateway attack can be the routing attack that has to be launched in the gateway resulting the wrong or no information between internets and the sensors or actuators thereby sub-domains jeopardizing functioning such as smart cities or the network of the vehicle [32].

4. Security Challenges in IOT

Although the IOT technologies have many benefits and advantages and solve the many problems in many sectors, but it still faces some security challenges. Security is a big issue that is currently faces by the IOT development. Providing the security to IOT is a big challenge. Here we discussed some of the security challenges in the internet of things environment.

4.1. Lacking in skills

For designing, developing, implementation and managing expertise and specific skills are important that must to be consider. Disruption of this factors cause the damaging of the security in IOT. Lacking in skills and in expertise causes slow adoption in the IOT [33] [34]. There are few skilled people that handles the IOT techniques. Gaining the advantages of IOT and deals with its challenges is depends upon the skills of the individuals.

4.2. Security Trade-Offs Vs Cost

Cost is an important for any project. Hardware and the unit's price contribute for the increase of security purpose, safety and also overcome the potential risks. Equipment that has high cost require many cost of money. In these high cost equipment People are also facing the challenge of the security. This equipment is not reliable and people pay a lot of money for purchasing these equipment [35] [36] [37].

4.3. Protection of the Privacy

IOT enables the embedded devices to access anyone and anywhere which effects sensitive data privacy. Therefore, some rules must be establishing for avoiding the privacy violations. For example, IOT devices shares data with other devices and this data become insecure, which make easier for attacker to enter the malicious code and then breach the data privacy and confidentiality [38][39].

4.4. Challenges in IOT architecture

IOT contains on many sensors and connected devices. Every device uses the different set of protocols for the communication purpose. There are no well-defined rules and standards for communication [40]. According to report of some researches numbers of the internet connected devices exceed of the 30 billion. Moreover, applications of the IOT is increasing day by day and it is not limited. These of the devices produced by many of the manufacturers even if they perform the same functionalities. This is a challenge that refers in IOT nature and lead in the lacking of the unified standardization.

4.5. Storage of data in IOT

Storage of data is a major problem due to increase of the amount of data size. Data storage is also effect the protection of the data. Damage of the stored data is difficult to back-up [41]. There has not clear criteria that ensure the distributed data in the IOT devices has to be transferred securely to main data-center because the process of transferred has not synchronized and make the disproportionate to data center. It is the major challenge for data management and data storages companies for creating the standards and tools that provide the security correctly and address the data.

4.6. Complication of the expanded system

Internet of things is widely expanded system and also a complex system. Increasing in number of people, devices and interaction is a mainly reason of increase the data security risks, and the challenges of the managing all of the points within network has maximize security is increase [42][43]. Another important component for IOT wirelessly sensors networks which serves as the collection of data by the ad hoc sensing. However, density nodes and random density in WSNs make the complexity and difficulty for implementation.

4.7. Power sources lower and capacity

A key component in IOT devices is power without it, the battery has not charges, so the limited the capacity and network failure because of the insufficient of battery of device. Development in IOT a

significant challenge is energy efficiency. Energy sources have a great importance therefore, especially in the unit of sensors which have powered battery [44] [45] [46].

5. IOT Security Challenges Vs Solution

Table 1. IOT Security challenge vs Solution

Source	Challenges	Description	Solution
[47]	Insufficient Testing & updating	Recently, there have 23 billion IOT technology or devices are in the world. It will rise up to 60 billion in the end of the 2025. One of the issue with companies That built these devices they take too little care for managing the security. Mostly these IOT product & devices do not receive enough update. As a result, gadget that originally considered secure when the customer purchases it insecure and can be easily hacked by hacker or attacker.	Before launching the device into general public each device need to be test and need companies to update The devices regularly. Failing is bad for both the consumer And also for the company.
[48]	Prevention & Identification go parallel	Eventually occur. But breach does not mean that your system is insecure. It just gives hints to that intruder will find the network. Because of many devices there is difficult to find the breaches. It is not easy task to find extend, confidential data has to be compromised if of the any. To overcome the threat, it is necessary to identify the vulnerability into the system.	In order to prevent cyberattacks, an organization should choose long-term strategy that places vulnerability detection at its center and continuously Improves cyber-security. In the dynamic virtual world, there is no strategy that can be used to address IOT security issues and Threats. Businesses should combine the following with their other core functions. -using the IPS and intrusion detection system causes increasing the challenging of cyber security. Using the analytics and security

			intelligence for detection the real time and reporting the security.
[49]	Lacking in the Security	Attacker have an ability to make change in IOT devices physically and the location is remotely for large period. For example, attacker spread the malware in the USB. Manufacturer need for insuring the security of devices.	Security analytics overcome the issue of security in the devices. Use the security analytics to overcome the security issues. Security analytics collects the data from many sources and detect and provide prevention from the attacks. They also detect the malicious anomalies.
[48]	Weak Password	Although how ridiculous it may sounds, a lot of devices installation executives forget that IOT devices require their default login and passwords to be updated. People still use factory default passwords, which puts their IOT devices and networks at serious risk. The list of IOT security issues is frequently topped by weak and default passwords. Hackers break passwords using preset passwords and brute force in order to access the IOT device and, in turn, all the devices on the entire network.	When you get the device, make sure to change you default passwords. Use the password that should not be the common words must be strong password. Attacker the software that have the database for the common passwords.

A survey conducted, the objective of the survey is views about the security challenges. The number of the participants who's take participants in this survey are 190. For lacking in skills security challenge we gain 38.9% votes. For security trade-offs vs cost challenge, we gain 32.4% vote. For protection of the privacy we gain the 18.4% vote. For storage of data in IOT challenge we gain the 22.4% votes. Privacy protection for IOT we get the 45.4% vote.

6. IOT Security Solutions

After the security issues that faced by the IOT devices this section discussed the security solutions for the IOT. IOT have include the many solution or security features such as authorization, availability, confidentiality, authentication and non-repudiation as showing in table 2.

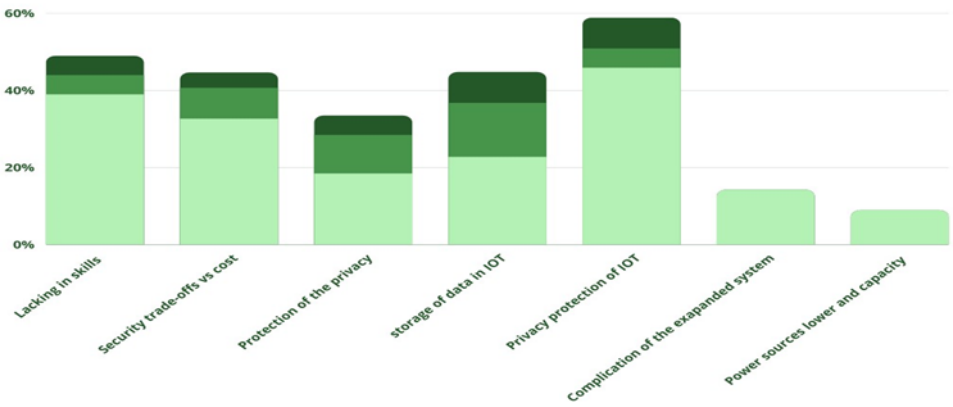

Figure 2. IOT Security Challenges

Table 2. Requirement of the security for the IOT layers

Security Services	Perception	Network	Application
Authentication	✓	✓	✓
Confidentiality	✓		
Authorization	✓	✓	✓
Integrity	✓	✓	
Availability	✓	✓	✓
Non-Repudiation		✓	

6.1. Confidentiality

It is defined as aptitude and capabilities prevent from the unauthorized person for accessing the private data. It gives guarantees that personal data is only access by the authorized person and can also edit, remove by the authorized person [50]. Confidentiality is a significant security service within the IOT network. Furthermore, confidentiality is considered the mostly attacked security service [51]. Trojan, spyware, viruses targeted data privacy of users. They interact with system in executables programs which have an objective to unauthorized data access [52]. Within context of IOT, for assuring confidentiality in personal data, encryptions algorithms are used [53]. Therefore, the data that is transmit between both devices has encrypted [54].

6.2. Authentication

In the infrastructure of the internet of things, many distributed and inter-connected devices are communicated with each other. That idea highlights the importance for having strong, trustworthy, scalable method of authentication in place in which every device of IOT is validate for assuring the authentication and from prevention the IOT devices, unwanted installation over the network. When IOT devices are communicates with one another they have need to identify one another for making the authentication. It is gained from the cryptographic techniques that varies in security level and complexity terms [57].

6.3. Authorization

It is the process that gives some one's ability for accessing the resources. An example has the ownership of the house. The number of devices on the internet are increasing day by day; therefore, authorization is an important issue in IOT. Authorization refers to services of the securities that are responsible for the privileges and right of the user. It provides a collection of the access control rules that ensures or refuse authorization for IOT devices [58] [59].

6.4. Integrity

Integrity is when message not altered by the unauthorized person during communication. It gives guarantee that exact message has reach as they sent and not altered. The basic goal is to prevent from unlawful access or altering an object. For devices safety in the network of IOT system gives guarantee for the data integrity. Cryptography techniques are used when the data are important [60].

6.5. Encryption Technologies

The idea that useful information is delivered is what gives sensor networks their significance. It introduces a lot of bugs at once. Web, database and the authorized computer gained the information must function the all efficiently. The abuse illustration in application of IOT, linked channel. To stop a potential attack like that, handle password-based authentication to assist with server and database-based protection. Recently there are several corporations that are design the reachable applications of the authentications. It permits appropriate usage of encryption software since we still use it without performing the necessary first testing to determine whether it works. This software is frequently created and validated by data protection practitioners from around the world, making it a crucial component of information protection [61].

7. Research Questions

Q1: What is the Evolution of IOT hacking?

Q2: How to detect the IOT attacks.

Q3: Which layer of IOT is more vulnerable to attack and why?

7.1. Solution Q1

IOT hacking is now become less effort and high reward for the cyber-criminals. Mirai botnet is an attack mechanism which is known for conveying the Internet of Things hacking to the mainstream. A report was publishing about the Mirai botnet in August 2016, despite previous incidents of cyber-attacks on the internet connected system dating back to as early as 2011. First IOT attack was occurred in 2016, helped by "Mirai botnet" infected more than 600,000 Internet of Things devices in which most of the devices were Internet routers and other most devices were the Internet connected cameras which was attacked [63]. Self-propagating is one of the reason for Mirai spread quickly. In 2018 hackers changed their methods and their focus was on the Z-wave which was the protocols that worked wirelessly for smart homes. In 2018, researchers exposed the vulnerabilities which were affecting more than 100 million smart homes [62]. Smart speaker is the smart homes gadgets which works as doorway for hackers. In 2014 Amazon had released the Alexa technology in small speaker. One of the estimated was cybercrimes costs could higher $6 trillion in 2021 [63].

7.2. Solution Q2

Table 3. Attacks and detection

Sr No.	Attack Name	Detection
1	Denial of Service Attack	Denial of Service attack is detected using monitoring the packet using TTL approach
2	Reply Attack	Reply attack can detected using the frequency base approaches.
3	Spoofing Attack	Spoofing attack can be detected using the machine learning methods to use the physical layer information.
4	Insider Attack	Insider attack can be detecting using the Hunting insider threat monitoring the activity of the user.
5	Ransomware Attack	Ransomware attack can be detected by using the watch out for the known extension of file and watch out increase in the files rename.
6	Gateway Attack	Gateway attack can be detected using the wirelessly virtual clients.

7.3. Q3 Solution

The physical layer of the IOT is more vulnerable to attack because in this layer sensors, actuators and the objects takes a part in the data generation. Hence physical layer is targeted the attack such as the DOS attack, jamming, tampering as well as eavesdropping. In mostly cases the sensors are targeted by the jamming and the tampering.

8. Conclusion

IOT gives many opportunities for the research. People are doing number of research on the topic related to security issues of the IOT. This research has objective to give you knowledge about the important IOT aspect especially focus on the security issues. There are several security issues in Internet of Things. There have still need for the solutions related to security of IOT. This paper explained the security issues in internet of things and the challenges related to security. This paper also describes the safety measures for the IOT which include the confidentiality, availability, authentication, authorization and data integrity.

References

1. Vermesan, O., & Friess, P. (2014). Internet of things applications-from research and innovation to market deployment (p. 364). Taylor & Francis.
2. Kraijak, S., & Tuwanut, P. (2015, October). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In 2015 IEEE 16th International Conference on Communication Technology (ICCT) (pp. 26-31). IEEE.
3. Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): definitions, challenges and recent research directions. International Journal of Computer Applications, 128(1), 37-47
4. Chaudhari, K. G. (2019). Review on Challenges and Advanced Research Areas in Internet of Things. International Journal of Innovative Research in Computer and Communication Engineering, 7(7), 3570-3574.
5. Alam, S., Chowdhury, M. M., & Noll, J. (2010, November). Senaas: An eventdriven sensor virtualization approach for internet of things cloud. In 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications (pp. 1-6). IEEE.
6. Van Kranenburg, R. (2008). A critique of ambient technology and the all-seeing network of RFID. Institute of Network Cultures.
7. Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In 2014 international conference on privacy and security in mobile systems (PRISMS) (pp. 1-8). IEEE.
8. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European research projects on the internet of things, European Commision, 3(3), 34-36.
9. Aldowah, H., Rehman, S. U., Ghazal, S., & Umar, I. N. (2017, September). Internet of Things in higher education: a study on future learning. In Journal of Physics: Conference Series (Vol. 892, No. 1, p. 012017). IOP Publishing.
10. Gen, H. P. C. S. A., & Controllers, R. A. I. D. (2015). Hewlett-Packard Enterprise Development LP.
11. 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.
12. Matharu, G. S., Upadhyay, P., & Chaudhary, L. (2014, December). The internet of things: Challenges & security issues. In 2014 International Conference on Emerging Technologies (ICET) (pp. 54-59). IEEE.
13. Pawar, R. A., & Karahari, C. R. An Efficient Context Aware Automatic Security Mechanism for IoT.
14. Zuin, N. K., & Selvarajah, V. (2021, September). A Case Study: SYN Flood Attack Launched Through Metasploit. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 520-525). Atlantis Press.
15. Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). Encyclopedia of cryptography and security. Springer Science & Business Media.
16. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE communications surveys & tutorials, 18(3), 2027-2051.
17. Behrooz, S., & Marsh, S. (2016). A trust-based framework for information sharing between mobile health care applications. In Trust Management X: 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings 10 (pp. 79-95). Springer International Publishing.
18. Rughoobur, P., & Nagowah, L. (2017, December). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In 2017 international conference on Infocom technologies and unmanned systems (trends and future directions)(ICTUS) (pp. 811-817). IEEE.
19. Feng, Y., Wang, W., Weng, Y., & Zhang, H. (2017, July). A replay-attack resistant authentication scheme for the internet of things. In 2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC) (Vol. 1, pp. 541-547). IEEE.
20. Jensen, C. (2023). Asserting password crackers ability to target Swedish passwords: An analysis.

21. Somasundaram, K., & Selvam, K. (2018). IOT–attacks and challenges. Int. J. Eng. Tech. Res, 8(9), 9-12.
22. Archana, K. C., & Harini, N. (2019). Mitigation of spoofing attacks on IOT home networks. International Journal of Engineering and Advanced Technology, 9(1S), 240-245.
23. Kamal, A. H. A., Yen, C. C. Y., & Ling, P. S. (2020). Security and Privacy Issues in Wireless Networks and Mitigation Methods.
24. Haddon, D. A. (2020). Attack Vectors and the Challenge of Preventing Data Theft. In CYBER SECURITY PRACTITIONER'S GUIDE (pp. 1-50).
25. Keim, Y., & Mohapatra, A. K. (2022). Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology, 14(1), 521-530.
26. Ye, N., Zhu, Y., Wang, R. C., Malekian, R., & Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things.
27. Crelier, A. (2019). The Challenges of Scaling the Internet of Things. ETH Zurich.
28. Langkemper, S. (2020). The most important security problems with IOT Devices. Eurofins Cyber Security.
29. Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware prevention and mitigation techniques. Int. J. Comput. Appl, 177(40), 31-39.
30. Brierley, C., Arief, B., Barnes, D., & Hernandez-Castro, J. (2021, November). Industrialising blackmail: Privacy invasion based iot ransomware. In Nordic Conference on Secure IT Systems (pp. 72-92). Cham: Springer International Publishing.
31. Kanuparthi, A., Karri, R., & Addepalli, S. (2013, November). Hardware and embedded security in the context of internet of things. In Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles (pp. 6164).
32. Mainetti, L., Manco, L., Patrono, L., Sergi, I., & Vergallo, R. (2015, December). Web of topics: An iot-aware model-driven designing approach. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 46-51). IEEE.
33. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business horizons, 58(4), 431-440.
34. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia computer science, 132, 1815-1823.
35. Alharby, S., Harris, N., Weddell, A., & Reeve, J. (2018). The security trade-offs in resource constrained nodes for IoT application. International Journal of Electronics and Communication Engineering, 12(1), 56-63.
36. Aman, W., & Snekkenes, E. (2015, December). Managing security trade-offs in the internet of things using adaptive security. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 362-368). IEEE.
37. Middha, K., & Verma, A. (2018). INTERNET OF THINGS (IOT)ARCHITECTURE, CHALLENGES, APPLICATIONS: A REVIEW. International Journal of Advanced Research in Computer Science, 9(1).
38. Haroon, A., Shah, M. A., Asim, Y., Naeem, W., Kamran, M., & Javaid, Q. (2016). Constraints in the IoT: the world in 2020 and beyond. International Journal of Advanced Computer Science and Applications, 7(11).
39. Burhanuddin, M. A., Mohammed, A. A. J., Ismail, R., & Basiron, H. (2017). Internet of things architecture: Current challenges and future direction of research. International Journal of Applied Engineering Research, 12(21), 1105511061.
40. Alansari, Z., Anuar, N. B., Kamsin, A., Soomro, S., Belgaum, M. R., Miraz, M. H., & Alshaer, J. (2018). Challenges of internet of things and big data integration. In Emerging Technologies in Computing: First International Conference, iCETiC 2018, London, UK, August 23–24, 2018, Proceedings 1 (pp. 47-55). Springer International Publishing.
41. Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. Procedia computer science, 52, 1089-1094.

42. Hernandez-Bravo, A., & Carretero, J. (2014). Approach to manage Complexity in Internet of Things. Procedia Computer Science, 36, 210-217.
43. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 ieee world congress on services (pp. 21-28). IEEE.
44. Bellavista, P., Cardone, G., Corradi, A., & Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal, 13(10), 35583567.
45. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems, 82, 395-411.
46. Alghentawi, M. (2021). Evaluation of IoT: Challenges and Risks on Communication Systems. Journal of Millimeterwave Communication, Optimization and Modelling, 1(2), 37-43.
47. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, 100129.
48. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. Computer Networks, 141, 199-221.
49. Panchiwala, S., & Shah, M. (2020). A comprehensive study on critical security issues and challenges of the IoT world. Journal of Data, Information and Management, 2, 257-278.
50. Canzanese, R., Kam, M., & Mancoridis, S. (2013, September). Toward an automatic, online behavioral malware classification system. In 2013 IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems (pp. 111-120). IEEE.
51. Javed, Y., Khan, A. S., Qahar, A., & Abdullah, J. (2017). Preventing DoS attacks in IoT using AES. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(3-11), 55-60.
52. Sharma, G., & Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. Journal of information security and applications, 42, 95-106.
53. Azrour, M., Farhaoui, Y., & Ouanan, M. (2017). A server spoofing attack on Zhang et al. SIP authentication protocol. Int. J. Tomogr. SimulationTM, 30(3), 4758.
54. Domb, M. (2019). Smart home systems based on internet of things. In Internet of Things (IoT) for automated and smart applications. IntechOpen.
55. Shah, T., & Venkatesan, S. (2018, August). Authentication of IoT device and IoT server using secure vaults. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 819-824). IEEE.
56. Farukul Islam, M. (2020). IoT security study for domestic devices.
57. A. Jebrane, A. Toumanari, N. Meddah, and M. Bousseta, "A new efficient authenticated and key agreement scheme for sip using digital signature algorithm on elliptic curves," Journal of Telecommunications and Information Technology,
58. Erikson, K. (2020). Frameworks for centralized authentication and authorization.
59. Hong, S. (2019). Authentication Techniques in the Internet of Things Environment: A Survey. Int. J. Netw. Secur., 21(3), 462-470.
60. Thirupathi, L., & Padmanabhuni, V. N. R. (2021). Multi-level protection (Mlp) policy implementation using graph database. International Journal of Advanced Computer Science and Applications, 12(3).
61. Singh, A., Kumar, G., Saha, R., Conti, M., Alazab, M., & Thomas, R. (2022). A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture, 127, 102503.
62. Kayla Metthews, "The Evolution of IOT hacking", October 25, 2018.
63. Sharma, N., Shamkuwar, M., & Singh, I. (2019). The history, present and future with IoT. Internet of things and big data analytics for smart generation, 27-51.