IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Communication Security Challenges of IoT

Mr. Subhankar Sarkar
Ph.D. Enrolled Department of Computer Science and Engineering
Maulana Abul Kalam Azad University of Technology (Formerly known as W.B.U.T.)
Simhat, Haringhata, Kalyani, Nadia, West Bengal, India.

Abstract: The Internet of Things is a technology that is used to connect various sensors to exchange data according to user needs via the Internet. And to make this possible the use of the Internet of Things is increasing day by day. In other words, IoT is being used in every segment of modern technology. That is, IoT is used for the purpose of connecting with other devices through the Internet and exchanging data received from various sensor devices. IoT is one of the growing and used technologies, As IoT's use has grown, so have its security vulnerabilities. In this article of mine, I have tried to highlight some of the common IoT security issues and challenges involved in IoT technology.

Keywords: **Internet of Things, Applications, Cloud, IoT Security, Challenges.**

INTRODUCTION

The Internet of Things is a technology that connects all smart devices through the Internet. In other words, the Internet of Things is a network of various electronic devices like computer devices, vehicles, buildings, or other objects connected through sensors or software. Data can be collected from devices connected through the Internet as per user need. These electronic devices can be managed and controlled by the user. Internet to all devices, including resource-limited sensors, as well as smart devices. In today's world, we are all connected with one another using our personal devices like smartphones, tablets, laptops, and many other microdevices. All of them are working with the evolution of IoT (Internet of Things). IoT is changing day by day according to user needs, updating with technology, and improving more specifically, so as to accelerate the user experience. Nowadays IoT is being used in almost every consumable device, from small smartphones, andsmartwatches to Smart homes and appliances (like washing machines, TVs, ACs, etc.), Industry, Vehicles, Agricultural, Environmental Monitoring, Healthcare, Security, and others. But as the technology is being developed, several kinds of issues and several kinds of challenges arise when the task is to protect the communication between devices and servers as well as make the data sharing as efficient as possible so that the communication becomes seamless, hassle-free, and secure. Aswell as the underlying system (both server and client) needs to be protected from being wrongly exposed to the outside internet. The IoT depends on wire or wireless networks and provides connectivity to smart devices. These wireless technologies play an important role in mobility requirements. There are several security possibilities for IoT security, we should consider the security risks of IoT. Nowadays almost all smart devices are connected to the internet as well as the cloud. As technological development has increased, security risks also increase with the advancement of technology and its use, unless timely updates or security standards are followed. And I have highlighted the applications, security aspects, Challenges, regarding the Internet of Thingsin my article.

INTERNET OF THINGS AND APPLICATIONS

The Internet of Things is a new technology that has changed ordinary life into a high-tech life. Several technological changes have taken place in social life through IOT, Likewise, our lives have become easier due to smart cities, smart home solutions, fire control, energy saving, smart transportation, Smart Security, etc. What the Internet of Things basically does is, use smart devices and the Internet provides solutions to various challenges and problems related to different industries. Currently, due to the use of IoT, there has been a change in the use of electronicproducts in general life. IoT collects data through various sensor networks aggregates that data and stores it in a cloud database, after which it is sent to the user after analysis.

The use of the Internet of Things or IoT has increased and is being used in several applications these days. Following are the areas where IoT is being used.

- Laptop or Personal Computers
- Garden Monitoring
- Smart Phones
- Industrial Sector

- Homes and Appliances (Like Smart Lighting)
- Security Monitoring.
- Vehicle Tracking.
- Fire Fighting.
- Analytics.
- Health Care.

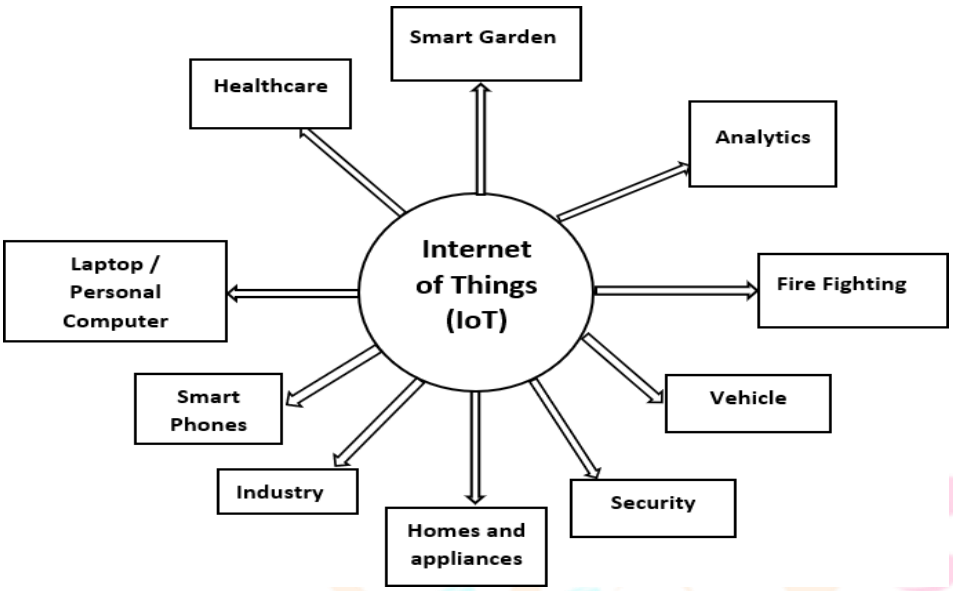

Figure-1. Internet of Things and Applications.

RELATED WORKS

I. Android-based Home Security Systems using the Internet of Things (IoT) and Firebase. (2018). Sourabh Sarkar, Srijita Gayen, and Saurabh Bilgaiyan. In this paper, they show that IoT has improved over the previous decade. It also states that millions of electronic objects are integrated to collect various types of data to communicate with or control them. And they are being done using smart and wireless devices. It is also said that handheld devices are the most widely used IoT devices today. Basically, this project was created by them, for a smart home, and in it, they showed that the user can ensure the security of the home through Elam or alert messages without being present at home. For that, several sensors have been used by Google's Firebase to collect and send data. Also, there are some services called Function as a Service (FaaS) like Cloud Functions by Google Cloud Function (GCP) or Lambda by Amazon web service (AWS) which executes corresponding codes to post-process these data is an almost infinite scale and has negligible latency.

II. IoT: Challenges and issues from an Indian perspective. Yadav, E. P., Mittal, E. A., & Yadav, H. (2018, February) This paper basically shows the advancement and market growth of IoT technology in the Indian market. As IoT is an emerging technology, the use of IoT is increasing day by day and many countries are investing in expanding IoT networks. Also, the demand for IoT automation is increasing day by day. In addition, the speed of IoT is increasing for tracking several small things, collecting or managing information through various electronic devices or monitoring a place, monitoring smart homes or other situations, and the sharing economy is responsible for accelerating the pace of IoT in the global market, The security aspect is mentioned here as the use of IoT is increasing day by day and the number of users is from lakhs to crores. As the number of users is increasing, the possibility of data theft remains here, and it can be risky or incomplete data or common people's information can be stolen and elaborated on this. They also highlighted here that private businesses private works or government departments are emerging as part of everyday households in terms of increasing and empowering IoT networks.

III. Penetration Testing in IoT Network Rahul Johari, Ishveen Kaur, Reena Tripathi, Kanika Gupta (2020) As the demand and use of IoT is increasing day by day, the security of IoT is also discussed in this paper. Besides, several methods are mentioned here like- Penetration testing is one of the testing metrics to measure the capability and efficiency of the architecture. This kind of technique has some advantages over manual testing, like easy to manage the testing process, easy to monitor the test results, the ability to mock almost every corner case situation, repeated random testing to check system capability, etc. Here are the different stages to follow while performing IoT network vulnerability and assessment and penetration are as follows- Recognise, Scanning, Gaining Access, Maintaining Access, Analysis.

IV. A Study of Various Network Security Challenges in the Internet of Things (IoT), Abdulrahman Yarali This paper mainly addresses IoT usages like home automation, smart cities, the automotive industry, manufacturing plants, smart devices and wearables, healthcare and agriculture, and security challenges in IoT Technology. In this research paper, they basically want to say that as the use of IoT has increased, the problems of connection compatibility, network security, and privacy security have increased day by day. Various smart home network techniques are used here and the Cisco Packet Tracer tool is used and tested.

Various network security-tampering nodes and remote network attack methods over the Internet are discussed. Here we see the use of different applications of smart home networks using multiple IPs or different types of IP addresses.

V. Security on the Internet of Things (IoT) with Challenges and Countermeasures. R. Vignesh and A. Samydurai. This review paper is made by investigating the current status and analysis of IoT. This paper has been mainly developed by investigating the current state of IOT and its analysis. It also discusses the different types of connectivity of IoT, the connection of sensors to different machines, and the wired and wireless network layers. And the layers that different networks have, those layers are described at different levels for security or implementation Also discussed are matching relays to enforce security at different layers of IoT.

VI. A Review on the Internet of Things (IoT) by M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal- In this review paper they basically want to say that it is about the technological developments and innovations that have taken place in the Internet world and which are transforming and new types of software and hardware are being invented. In addition to the great promise that the Internet of Things holds for the future, there are also some types of IoT communication such as machine-to-machine. Or the communication system that humans from machines. Apart from discussing the sensor technology of IoT or sensor networks, the main challenges related to the 6-layer architecture of IoT are discussed. Also, several applications related to IoT, and radio frequency identification, wireless sensor network cloud computing or optical technology, nanotechnology are also described.

CLOUD COMPUTING

Cloud Computing is an internet technology where users can store and access data from anytime anywhere if an Internet Connection and Computer Device are required. Here users can Store and manage data on remote servers. Cloud computing is always changing because it is being updated technically. Cloud computing is essential to make the Internet of Things work. Cloud computing generally uses services provided by the Internet and helps perform the following tasks. Currently, cloud computing and the Internet of Things are related to each other. Due to the rapid development of technology, the role of cloud computing is important for processing large amounts of data and storing data. Data can be uploaded and stored through sensors in cloud computing. This is exactly why problems arise in data storage, data processing, or access. All data stored in cloud computing can be intelligently monitored to make subsequent decisions, and other data can be converted into insights and productive actions by the user.

Data can be stored using IoT in cloud computing and the resulting data problems are as follows-

- **Data breaches and security:** Now if there is a problem or bug in the network connected with cloud computing then users' data can be stolen, or unauthorized users can take control of this data.

- **Internet connectivity:** As I mentioned earlier, an internet connection is important for accessing data in IoT or cloud computing. So, if there is any problem with the internet connection then the user will not be able to access his data.

- **Migration:** When transferring stored data from one provider to another provider, transferring large amounts of data can be time-consuming and may cause technical problems. Automation solutions can be used to avoid various problems or workload issues in data transfer.

- **Costs:** An ioT cloud storage base can cost more than a normal storage base. Especially if a domain is needed in the case of a company or individual case it becomes expensive.

- **Environmental concerns:** First, cooling- Cooling is a method of keeping data centers where datais stored cool. And these data centers have to try to keep cool for 24 hours and having these data centers in a warm environment can be a concern in terms of data storage. Secondly, due tofloods most of the world's communications traffic is carried by undersea fiber, but flooding or rising sea levels can disrupt these cables, making them more vulnerable. In some cases, thisproblem can become dangerous.

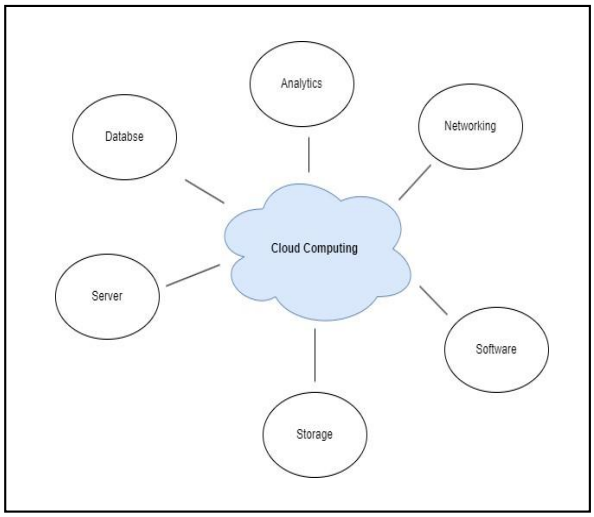

Figure-2. Cloud Computing.

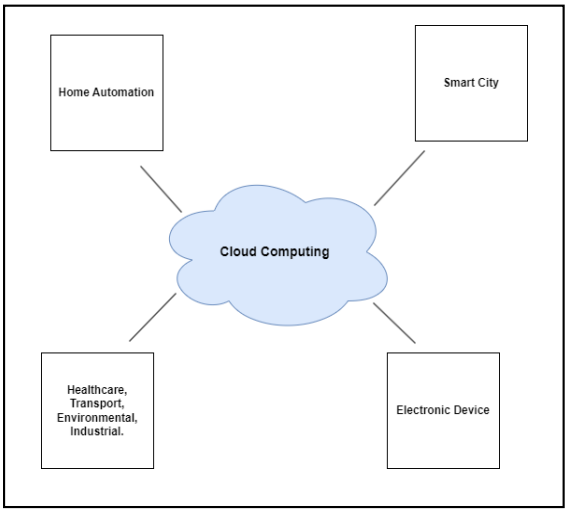

Figure-3. Integration of Cloud Computingand IoT.

NETWORK TECHNOLOGIES USED IN IoT

The Internet of Things is a network technology where various devices are connected to each other over the Internet so that the devices can exchange data. IoT Devices basically work to exchange data among themselves. Networking or network technology is required to enable these functions. Several networking technologies are used in IoT, some of them are shortly discussed below

I. **Bluetooth Technology**: Bluetooth is a network technology used to connect devices in close proximity, this technology is typically used where data transfer rates are low. Examples include connected IoT devices such as smart watches various automation devices or devices such as fitness trackers.

II. **Wi-Fi (Wireless Fidelity) Technology:** Wi-Fi is a networking technology that allows wireless internet connection between different computing devices. This Wi-Fi technology is commonly used in offices or commercial establishments and even at home to connect various IoT devices. It requires uninterrupted internet connection service and a high data rate.

III. **LoRaWAN (Long Range Wide Area Network):** LoRaWAN is also a wireless communication networking protocol designed for IoT Devices. So that communication or monitoring can be done from far away. For example, LoRaWAN is useful for smart garden monitoring or for various trucking or new applications.

IV. **Zigbee:** This technology is suitable for some applications that require low data rates. They are commonly used in areas such as home automation industrial control or smart lighting systems.

V. **LTE-M (Long-Term Evolution for Machines):** LTE-M is a cellular technology and is designed to support IoT applications. This network technology provides wide-area communication capabilities to IoT devices. And it requires more data to use.

VI. **Threads:** Threads are an important networking protocol, this protocol is used for communication between IoT devices. And it uses IPv6 for communication between IoT devices. This wireless technology is designed to provide reliable and secure communication, It is used in IoT applications where security and interoperability are essential.

VII. **MQTT (Message Queuing Telemetry Transport):** MQTT is a lightweight messaging protocol that uses IoT technology. It is used to publish data streams for IoT devices. It is a network medium suitable for devices with network connections to be efficient in bandwidth usage, and to have limited processing power.

VIII. Apart from the above, several other network technologies are used in IoT respectively- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network), NB-IoT (Narrowband Internet of Things), and LTE-M (Long-Term Evolution for Machines), Sigfox, CoAP (Constrained Application Protocol) Technology etc.

INTERNET OF THINGS ARCHITECTURE

The Internet of Things architecture refers to a seamless connection or communication with the core system through a device or sensor over the Internet. It includes the entire IoT system, such as communication protocols, data processing, data collection, hardware software, etc. There are several layers in the architecture of IoT, the layers are discussed below.

I. **Application Layer:** The third important layer of the IoT architecture is the Application Layer. This layer focuses on the processing and analysis of the data received from the lower layers. The data is then transformed into actionable information through an analytics platform or algorithm. Not only that, at the application level, the integrity and confidentiality of the received data is guaranteed.

II. **Network Layer:** The second important layer of IoT architecture is the network layer. The main function of the network layer is to transmit the data collected by different types of devices or sensors to a higher layer or perform communication functions at the next layer. Various network technologies are used for this communication such as Wi-Fi, Bluetooth networks, cellular networks, Wired Networks, 3G, 4G, etc. This layer acts as a network gateway, sending the data received and stored by sensors to the next layer over the network.

III. **Perception Layer:** The perceptual layer is an important layer of IoT. This layer is the sensor layer. This layer mainly consists of physical devices, which collect various types of data from the environment. That is, the perception layer first collects and stores the data through various sensors like temperature sensors, motion detectors, cameras, etc. then after processing the data, delivers it to the network layer and converts it into digital data.

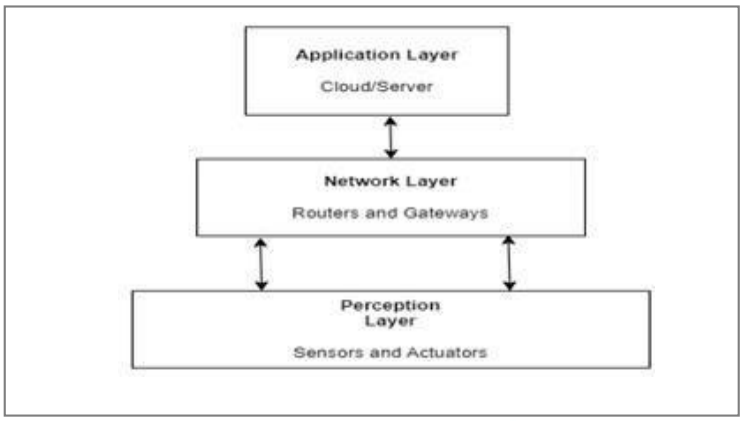

Figure-4. Three-layer IoT Architecture.

Apart from these three main layers, there are several other layers in IoT architecture which are –

IV. **Business Layer:** After the main three layers of IoT architecture (Perception, Application, Network), there is one more important layer which is the business layer. The processed data obtained and stored here are used to create various types of values for businesses and users. That is, it acts as an IoT manager and manages an application. That is, this layer performs the important functions of creating or storing various types of data along with the business flow, controlling user privacy access, etc. For example, monitoring from a remote location or any smart city service or any maintenance work, etc.

V. **Security and Privacy Layer:** This layer is also one of the most important layers of IoT architecture Because this layer ensures the confidentiality and integrity of the data received across the IoT system. Here authentication mechanisms, encryption techniques, or access control are security measures to prevent data breaches. Also prevents controlling data from unauthorized access at this level.

VI. **Management Layer:** This management layer in the IoT architecture system performs the functions of system management, this layer of IoT also handles other computer device management tasks, this level includes several functions viz device provisioning, firmware updates, configuration management, and monitoring of device health.

VII. **Cloud / Edge Layer:** This is also an important layer of IoT architecture because here the data collected through IoT sensor devices are processed, analyzed, and stored at this level. This layer can be divided into two, one is the cloud and the other is the edge. Cloud is usually long-term and it manages storage. However, the edge is closer to the data source and allows data processing to make real-time decisions.

VIII. **Middleware Layer:** This layer usually acts as an intermediary between different layers. The middleware layer serves to connect various complex and existing programs. It also acts as an interface between the various components of the IoT. It Handles different types of devices, data routing, or communication system protocols.

IX. **Service Layer:** The last and most important layer of IoT architecture is the service layer. This is the service layer or Platform layer. The main function of this layer is to provide various IoT-related services, Such as different types of reporting notifications or warning message visualizations, etc.

ISSUES AND SECURITY CHALLENGES OF IoT

As the usage definition of IoT devices is increasing day by day, attackers are discovering new ways to break IoT security systems. There are several security issues in using IoT, they are- Device security, Data security, Communication security as well as privacy. IoT systems need to be addressed to secure their use. For this, the communication system of the channels needs to be proven so that no unauthorized person can access the nodes. on the other hand, it also should be private, so that any intruder might not steal any communication or stored data. Some of the recent issues of IoT technologies are-

I. **Device Security**:

Inadequate Security Measures: IoT devices are often designed according to user needs with typically limited resources that are susceptible to security vulnerabilities. That is, here according to user demand, manufacturers prioritize functionality over security. I think this is one of the security risks of IoT devices and data.

Lack of Regular Updates: If IoT devices are not regularly updated, or lack regular updates, devices and data are vulnerable to known exploits.

II. **Data Privacy:**

Data Collection and Sharing: IoT devices are usually made with various sensors to collect data, but here it can be seen that when the devices are collecting large amounts of sensitive data and that data is being managed or shared or handled inappropriately, there is a breach of privacy.

Consent and User Awareness: Users of IoT devices may not know exactly what kind of data their devices are collecting and how they are collecting it. And may not be fully aware of how that collected data is being used. which may lead to potential privacy violations.

III. **Network Security:**

Vulnerable Networks: Many IoT devices operate on wireless networks, which wireless networks often experience connectivity issues. In that case, it may be susceptible to a denial-of-service (DOS)-like attack or an intrusion attack.
Network Segmentation: The use of IoT devices can be seen in the use of several critical business networks that cannot or fail to properly segment devices. This can lead to compromise of sensitive data or systems.

IV. Communication Security:

Insecure Communication: Sometimes there is a need for communication between different device to devices or between different devices to users. these communications often involve the use of insecure communication protocols or weak communication protocols, which can expose sensitive data to interception and manipulation.
Man-in-the-Middle Attacks: As seen in IoT use cases, there are usually several attackers who are able to intercept data between the device and the back-end system. which may lead to unauthorized access to data or alteration of data.

V. Lack of Standardization:

Heterogeneous Ecosystem: Builders use a variety of devices when constructing an IoT landscape. Many times, different operating systems or protocols are used here, In many cases the use of old operating systems has also been seen. As a result, it is challenging to establish consistent safety standards.

VI. Scalability and Management:

Device Management: Nowadays the use of IoT is increasing day by day, that is why the use of IoT devices is also increasing day by day. That's why managing a large number of IoT devices together is quite difficult and complex. Especially when it comes to monitoring updating or adjusting security configurations.

Identity and Access Management: As the number of IoT device users is increasing day by day, so is the number of unauthorized users. For that IoT device users should be properly identified and access controlled, to prevent unauthorized access.

VII. Physical Security:

Physical Tampering: It is not recommended to install IoT devices in unsafe or unsecured locations. If IoT devices are placed in unsecured locations, the devices may be physically tampered with data manipulated, or unauthorized data access.

VIII. Lifecycle Security:

Secure Deployment of IoT Device: IoT devices should be securely installed and securely supplied to prevent early compromise. So, it is quite important to place IoT devices in a secure location.
End-of-Life Disposal: IoT devices should be properly decommissioned and disposed of to prevent reuse. It can prevent data loss.

IX. Supply Chain Vulnerabilities:

Compromised Components: Many times, IoT devices are designed with fake components which can introduce vulnerabilities in IoT devices, which may compromise security.

X. Regulatory and Legal Challenges:

Compliance: Using IoT systems must comply with several laws such as data protection laws that are complex to navigate in a global context.

Some of the current issues of IoT technologies are in Table:

Issues	Causes
Incorrect access control	**Same Default password** **Weak password** **Lack of privileges**
Large attack surface	**Insecure open ports** **Proper port protection**
Outdated software	**Device firmware version** **Software version** **Operating system version**
Encryption	**Proper encryption on storage and medium** **Proper authentication** **Proper authorization**
Application bugs	**Known application bugs** **Unit testing**
Execution environment	**Code signing** **Digital signature**
Physical security	**Unique security for each device**
Cyberattacks	**Botnets and DDoS Attacks** **Ransomware** **Zero Day Exploits**

Lack of Standards	**Interoperability** **Security Standards**
Regulatory and Legal Challenges	**Compliance**

Table- 1. Current security issues of IoT.

POSSIBLE SECURITY SOLUTIONS OF IoT

So far, I have discussed IoT architecture, Network Technologies, and different problems of IoT, Now I will discuss the possible solutions to the problems of IoT.

I. **Use IoT security analytics:** IoT security problems can be reduced if security analysis is done properly before implementing any IoT task, When various data are collected from multiple sources and that data is properly analyzed then potential threats can be identified and security teams can prevent these security issues. This security analysis can identify these inconsistencies when correlating data from different domains and creating problems with network traffic. That is, security analysis usually prevents negative impacts on connected devices because problems are detected early.

II. **Endpoint Detection and Response (EDR):** Users are usually not always in control of IoT devices and due to this, important data is often lost, as IoT devices are always streaming data. Real-time attacks happen on that occasion, but EDR technology helps us prevent these real-time attacks and avoid data loss. Another major advantage of EDR technology is that it can automatically block any suspicious activity in real-time.

III. **Secure APIs:** IoT devices typically use APIs to collect data or in some cases retrieve lost data. The API uses a number of security techniques to collect data. Several checks are undertaken and then ensured that hackers cannot access IoT devices through poorly configured or unauthenticated APIs in the system.

IV. **Encryption communication:** Encryption is a communication method that prevents third parties from intercepting the communication between two devices or between two entities. Communicating or sharing information in this manner cannot be intercepted by third parties or create any problems. And information can be shared between two devices with certainty.

V. **Improve network visibility:** Network visibility is the awareness of when data is being exchanged within a computer network or between devices. this method is used to increase the awareness of various IoT devices or data or other computer content. Visibility tools such as network access control are used in this case to inventory and perform tasks on connected devices and should automatically update the inventory. Not only this, tagging IoT devices can automatically report security incidents to organizations and take necessary action if security risks are identified**.**

VI. **Authentication:** Authentication is a term used to protect users, Basically Authentication is a process where a user has to prove his identity to a server or client. In this case, a user is already registered with the server or client, and that user is required to use his username and password for authentication, often at intervals. The authentication process is used on both the client and the server. Here, since the user accesses the server with his own user ID and password, the server can know whether the real user is accessing the data on the server or not. In the case of authentication, there is a user ID password system. Also, there are more authentication systems like retina scans and biometric authentication systems with fingerprints.

- **Single-Factor Authentication:** Single-factor authentication or SFA is one of the simplest forms of authentication. The most popular form of SFA is username and password-based authentication. Nowadays there are many applications that are using SFA as their primary authentication method. The password authentication method here relies on mutual confidentiality between the user and the online service provider.
- **Two-factor Authentication:** Two-factor Authentication 2FA is one kind of multi-factor authentication process that requires two methods to verify identity. Similarly, we can say it is a two-step verification process which is for the verification of identity. like as Name and Password or OTP (One-time password) based verification before login. This 2FA Authentication method protects the user's login and data from various unwanted attacks or data theft.
- **Multi-factor Authentication:** When the user has to go through multiple verification processes it is called multi-factor authentication. Here, since the user has to go through several verification steps, it is a key component of strong identity and access management policies. in the case of MFA, having additional verification mechanisms greatly reduces the number of changes to a successful cyber-attack.

Famous Authentication techniques are:

- Single-factor authentication.
- Passwordless Authentication.
- 2FA/Two-factor Authentication.
- Single Sign-on.

Also, some possible security solutions of IoT are given in a table-

Security Issues	Solution
Secure Device Design	**Security by Design.** **Regular Updates (Security).**
Network Segmentation	**Isolation.Firewalls.** **Intrusion Detection Systems (IDS).**
Device Management	**Remote Wiping. Centralized management.**
Physical Security	**Tamper-Proofing.Enclosures.**
Security Audits and Testing Regularly	**Vulnerability Scanning.Code Review.**
Data Minimization	**Collect Necessary Data.Anonymization.**
Security Updates for Legacy Devices	**End-of-Life Planning.**
Regulatory Compliance	**Data Protection Laws.**
Blockchain Technology	**Immutable Records.**
Collaboration and Standardization	**Information Sharing.Industry Standards.**

Table-2. Possible Security Solutions of IoT.

CONCLUSION

In this paper, I have tried to review some of the security issues of IoT devices and their details. The popularity of IoT technology is increasing day by day, and this technology has opened many business opportunities. Also, IoT technology can now be controlled remotely from one place, Automation has made it easier. IoT will continue to grow in popularity in the future. Not only that the security standards have to be increased, but if the security standards are maintained in a specific way and if they are followed, the use of IoT devices can spread to some sensitive sectors if the manufacturers follow those standards. For example, a core system is like a core government, where a government controls the rest of the country through a core system of governing the country. Again, the banking sector is a prime example of a core system. Also, in this review paper of mine, I have discussed IoT and cloud computing used in IoT. And tried to give an idea about various network technologies that are used in IoT. Various issues of IoT and its security challenges are also discussed.

REFERENCES

[1]. Cloud Computing: https://www.geeksforgeeks.org/iot-and-cloud-computing
[2]. IoT and Cloud Computing: https://research.aimultiple.com/iot-cloud
[3]. Networks: https://www.tutorialspoint.com/types-of-iot-networks
[4]. https://www.sprintzeal.com/blog/iot-security-challenges

[5]. IoT Security: https://securityboulevard.com/2022/05/5-top-iot-security-challenges-and- solutions
[6]. (IoT): Issues and Possible Solutions: https://www.researchgate.net/figure/Security-and-Privacy-issues-in-IoT_fig2_329969562
[7]. IoT Security Threats: Website security - Learn web development | MDN (mozilla.org)
[8]. The Internet of Things (IoT): Applications, investments, and challenges for enterprises.Business Horizons, 58(4), 431-440. Lee, I., & Lee, K.
[9]. Android-Based Home Security Systems Using Internet of Things (IoT) and Firebase. Sarkar, S., Gayen, S., & Bilgaiyan, S. International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 102-105). IEEE.
[10]. IoT: Challenges and issues in Indian perspective. Yadav, E. P., Mittal, E. A., & Yadav, H. In 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT- SIU) (pp. 1-5). IEEE.
[11]. Penetration Testing in IoT Network. Johari, R., Kaur, I., Tripathi, R., & Gupta, K. In 2020 5th International Conference on Computing, Communication and Security (ICCCS) (pp. 1-7). IEEE.
[12]. IoT and cloud convergence: Opportunities and challenges. Biswas, A. R., & Giaffreda, R. IEEE World Forum on Internet of Things (WF-IoT).
[13]. Internet of Things security: A review of risks and threats to the healthcare sector. Abouzakhar, N. S., Jones, A., & Angelopoulou, O. In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), and IEEE Smart Data (SmartData) (pp. 373-378). IEEE.
[14]. Security on the Internet of Things (IoT) with Challenges and Countermeasures R.Vignesh and A.Samydurai Student, Associate Professor Department of Computer Science and Engineering, Valliammai Engineering College SRM Nagar, Kattankulathur-603203, Tamil Nadu, India. IJEDR| Volume 5, Issue 1 | ISSN: 2321-9939
[15]. Internet of Things (IoT) Security: Issues, Challenges and Solutions. Saira Afzal, AbdullahFaisal, Imran Siddique, Mariam Afzal Department of Information Technology, Lahore Leads University, Lahore. Department of Computer Science, Afro Asian Institute, Lahore. University of Narowal, Punjab, Pak. International Journal of Scientific & Engineering Research Volume 12, Issue 6, June-2021 52 ISSN 2229-5518.
[16]. A Review on Internet of Things (IoT) by M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal.
[17]. Securing IoT devices and securely connecting the dots using rest api and middleware Garg, H., & Dave, M. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoTSIU) (pp. 1-6). IEEE.
[18]. Threats in IoT Dorobantu, O. G., & Halunga, S. Security In 2020 International Symposium onElectronics and Telecommunications (ISETC)(pp.1-4).IEEE.November2020. DOI:10.1109/ISETC50328.2020.9301127
[19]. Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review Rao Faizan Ali, Amgad Muneer, P.D.D Dominic, Shakirah Mohd Taib and Ebrahim A. A. Ghaleb Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar 32160, Malaysia. DOI: 10.1007/978-981-16-8059-5_9:https://www.researchgate.net/publication/356728249.
[20]. Internet of Things (IoT) Security: Issues, Challenges and Solutions. Saira Afzal, AbdullahFaisal, Imran Siddique ,Mariam Afzal. International Journal of Scientific & Engineering Research Volume 12, Issue 6, June-2021 52 ISSN 2229-5518 IJSER © 2021 http://www.ijser.org
[21]. A Study of Various Network Security Challenges in the Internet of Things (IoT) Abdulrahman Yarali, Institute of Engineering Murray State University Murray, KY USA ayarali@murraystate.edu Manu Srinath , Randal G. Joyce, Telecommunications Systems Management Murray State University Murray, KY USA msrinath@murraystate.edu, rjoyce@murraystate.edu.
[22]. Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware HittuGarg Department of Computer Engineering Nit Kurukshetra Haryana, India hittugarg6@gmail.com Mayank Dave Department of Computer Engineering Nit Kurukshetra Haryana, India mdave@nitkkr.ac.in 978-1-7281-1253-4/19/$31.00 © 2019 IEEE
[23]. Security threats in IoT Octavia Georgiana Dorobantu, Simona Halunga Dept. of Telecommunications of Faculty of Electronics, Telecommunications and Information Technology, 978-1-7281-9513-1/20/$31.00 ©2020 IEEE.
[24]. Security Solutions- https://www.esecurityplanet.com/products/iot-security-solutions/
[25]. Security Solutions(ii)- https://www.geeksforgeeks.org/10-security-tips-for-iot-devices/

AUTHORS PROFILE

Sarkar received his Bachelor of Technology Degree in Computer Science and Engineering [B.Tech-CSE] titute of Engineering and Technology (DIET) under West Bengal University of Technology (now MAKAUT), labad, W.B. India, in 2014. He also completed B.ED in Pedagogy of Mathematics from Purbanchal B.ED [EPA) from Sadikhandearh, Jalangi, Murshidabad,W.B in 2019. He received his Master of Technology Degree ence and Engineering [M.Tech-CSE] from Brainware University, Barasat, Kolkata, India, in 2022. He is nrolled (Enrollment Application No- R-02-2023/CSE/2------355) in the Department of Computer Science and ulana Abul Kalam Azad University of Technology (MAKAUT) Simhat, Haringhata, Kalyani, Nadia, West Bengal. India. Since 2022, His research interests focus on the Internet of Things. Email- elinksuvankar.sarkar@gmail.com