SECURITY CHALLENGES IN IOT

[1]S. Selvakumari, [2]P. Ganeshbabu, [3]V. Vaneeswari, [4]K. Saraswathi

Department of computer Science, Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.

Emai : selvakumaris5589@gmail.com **(S.Selvakumari)** *Corresponding author:* S.Selvakumari

Abstract **-** In remote communication networks, security risks are particularly high. The military, business, healthcare, retail, and transportation industries are among the most common uses of distant communication networks. Wired, cell or ad hoc networks are used in these architectures. There has been a lot of attention paid to remote sensor groups, actuator organisations, and vehicle organisations. The Internet of Things (IoT) has recently received a lot of attention from researchers. For others, the IoT is seen as the web's last chapter. Moreover, the Internet of Things (IoT) will play a pivotal role in the future, transforming our lifestyles, conventions, and business models. The Internet of Things (IoT) enables billions of devices, people, and organisations to connect and exchange information. The IoT networks are vulnerable to a variety of attacks because of the increased usage of IoT devices. Effective security and protection protocols are anticipated to provide privacy, verification, access control and trustworthiness among other things in the IoT network's security architecture. IoT network security and protection are discussed extensively in this study.

Keywords—Internet of Things (IoT); security, privacy

I. INTRODUCTION

The Internet of Things (IoT) has received a lot of attention in the last few years. In 1999, Kevin Ashton came up with the concept of the Internet of Things. As a result of rapid advancements in wireless communication, wireless sensor networks (WSN), radio frequency identification (RFID), and cloud computing, IoT devices have gotten more useful than they were before. There are many IoT devices that can function together. Advanced mobile phones, personal computers (PCs), personal digital assistants (PDAs), work stations and tablets are just a few of the devices that make up the Internet of Things (IoT). Communication between IoT devices, as well as the transfer of important data into the integrated system, is based on realistic sensors and remote correspondence frameworks. IoT devices' data is processed in the included framework and sent to the intended objections. Our daily routines are more centred on the anecdotal space of the virtual world because of the rapid growth of communication and online innovation [1]. In the virtual environment provided by the organisation, individuals may work, shop, visit (maintain pets and plants), and so on. As a result, it is impossible to totally replace human activities with mechanical

ones. When it comes to the future of web administrations, there is an anecdotal area that serves as a jumping-off place. This current reality and the anecdotal space have been successfully integrated into the IoT. Smart life, clever items, sharp health, and dazzling urban environments are only a few examples of the IoT's important priority areas [2]. The Internet of Things (IoT) gadgets are catching on fast these days, with an ever-increasing number of devices connected to the internet. By 2020, there will be 30 billion linked items with around 200 billion relationships that will bring in roughly 700 billion euros in revenue, according to an investigation [3]. Currently, there are nine billion devices in China, and that number is predicted to rise to 24 billion by the end of 2020. IoT will fundamentally alter our way of life and how we make decisions in the future. Individuals and devices will be able to communicate anytime, anywhere, and with any device under perfect circumstances, using any network and any help [4]. Predominant world for humans in the future is the major goal of IoT.

Although many of these gadgets and apps are not designed to cope with the threats to the IoT firms like secrecy and authentication, information integrity, access control, and so on, this creates a slew of security and protection difficulties in the IoT organisations. Aggressors and intruders target IoT devices on a regular basis. In a study, 70 percent of IoT devices were found to be very vulnerable. An efficient method to protect web-connected electronics from hackers and gate crashers is thus needed.

II. IOT APPLICATIONS

The Internet of Things (IoT) has received a lot of attention in the last few years. In 1999, Kevin Ashton came up with the concept of the Internet of Things. As a result of rapid advancements in wireless communication, wireless sensor networks (WSN), radio frequency identification (RFID), and cloud computing, IoT devices have gotten more useful than they were before. There are many IoT devices that can function together. Advanced mobile phones, personal computers (PCs), personal digital assistants (PDAs), work stations and tablets are just a few of the devices that make up the Internet of Things (IoT). Communication between IoT devices, as well as the transfer of important data into the integrated system, is based on realistic sensors and remote correspondence frameworks. IoT devices' data is processed in the included framework and sent to the intended objections. Our daily routines are more centred on the anecdotal space of the virtual world because of the rapid growth of communication and online innovation [1]. In the virtual environment provided by the organisation, individuals may work, shop, visit (maintain pets and plants), and so on. As a result, it is impossible to totally replace human activities with mechanical

ones. When it comes to the future of web administrations, there is an anecdotal area that serves as a jumping-off place. This current reality and the anecdotal space have been successfully integrated into the IoT. Smart life, clever items, sharp health, and dazzling urban environments are only a few examples of the IoT's important priority areas [2]. The Internet of Things (IoT) gadgets are catching on fast these days, with an ever-increasing number of devices connected to the internet. By 2020, there will be 30 billion linked items with around 200 billion relationships that will bring in roughly 700 billion euros in revenue, according to an investigation [3]. Currently, there are nine billion devices in China, and that number is predicted to rise to 24 billion by the end of 2020. IoT will fundamentally alter our way of life and how we make decisions in the future. Individuals and devices will be able to communicate anytime, anywhere, and with any device under perfect circumstances, using any network and any help [4]. Predominant world for humans in the future is the major goal of IoT.

Although many of these gadgets and apps are not designed to cope with the threats to the IoT firms like secrecy and authentication, information integrity, access control, and so on, this creates a slew of security and protection difficulties in the IoT organisations. Aggressors and intruders target IoT devices on a regular basis. In a study, 70 percent of IoT devices were found to be very vulnerable. An efficient method to protect web-connected electronics from hackers and gate crashers is thus needed.

B. Medical Devices

Additionally, IoT gadgets in medical care frameworks are used to monitor and evaluate patients [7]. Personal Medical Devices (PMDs) may either be implanted in a patient's body or connected to the patient's body through a wireless connection. PMDs, or personal monitoring devices, are becoming more commonplace and well-known. It is estimated that by 2019, the value of these devices would be worth an estimated $17 billion [8]. They employ remote interfaces to communicate with a base station, which is also used to read the gadget status, clinical reports, and adjust the limits of the gadget, or update status on the gadget. The patient's safety and security are jeopardised significantly when they are exposed to remote interface. Such devices are vulnerable to cyberattacks that might jeopardise the patient's safety, security, and well-being. For medical treatment, the most important goal is to ensure the safety of the organisation in order to prevent the patient from being attacked out of revenge. A typical goal is to steal data, attack devices to get access to their resources, or turn off particular programmes that monitor a patient's status.

Among the various attacks on medical devices include eavesdropping where the privacy of the patient is violated, respectability errors where the message is tampered with, and accessibility concerns where the battery is depleted. The following are a few network security threats related to the safety, security, and well-being of patient clinical information:

Any project that relies on battery power requires the use of power management devices (PMD). Because of this, only a limited amount of data can be sent using these devices. A device's categorization, accessibility, security, and honesty are all jeopardised if it's part of many groups.

Due to the fact that PMDs do not have a means for verifying distant communications.

It also exposes the devices to several additional security threats, which might lead to nasty attacks.

In the C. Smart House

Advanced gadgets may effectively communicate with one another using Internet Protocol (IP) addresses as IoT eager home administrations grow [9]. In a smart home atmosphere, all of your slick home devices will be linked to the internet. Increasing the number of devices in the smart home raises the risk of malicious attacks. Malicious attacks are less likely to occur if smart home devices are used freely. As of today, web-enabled smart home devices may be accessed from any location at any time. It increases the likelihood of malicious attacks on these devices. In a smart home, a variety of devices are linked together and intelligently communicate information through a home network. As a result, there is an entrance to the home network that restricts the flow of data amongst shrewd devices connected to the outside network. There is a specialised co-op that provides a wide range of services to the home organisation.

III. SECURITY REQUIREMENTS

In the Internet of Things (IoT), devices and people are linked together to provide various forms of help at any time and from any location. Web-connected devices lack appropriate security components and are vulnerable to a wide range of protection and security concerns, including the categorization, honesty and validity of the information they contain, and so on and so forth. The Internet of Things (IoT) necessitates that certain security requirements be met in order to protect the company from malicious attacks [7, 10]. In this section, the most critical capabilities of a safe company are briefly reviewed.

Strength in the face of adversity: In the case of a system failure during data transfer, the framework should be able to self-recover. Models and servers functioning in multi-user environments should be intelligent enough to protect themselves from gate-crashers and other

nosy neighbours. For the current circumstances, if it were to go down, it would be able to recover without alerting its customers.

It's important to verify the accuracy of the information and its associated data. To ensure that only genuine devices may transmit data, a validation mechanism is used.

Only those who have been pre-approved are granted access control. It is the chairman of the framework who should be in charge of restricting access to the data set or projects for different customers by dealing with their usernames and passwords and describing their entry freedoms.

The client's data and information should be protected. In order to safeguard customers, only authorised individuals should be able to access their personal data. Because of this, no framework or non-essential verified client may have access to a client's personal information.

IV. CHANLLENGES

The Internet of Things (IoT) era has altered our way of life [12]. There are several security risks associated with the Internet of Things (IoT), despite its many benefits. Data leakage and administration loss are two of the most common security threats. There is a clear correlation between IoT security risks and the real risk. The Internet of Things (IoT) consists of a wide range of devices and platforms, each with its own set of certifications and security requirements. It is also critical to ensure customer security since personal data is increasingly being dispersed across several devices [13], [14]. Individual data will now be protected by a reliable mechanism. In addition, a wide range of devices that communicate with many organisations are available for IoT administrations. To put it another way, it suggests that there are a lot of security vulnerabilities on both the client and network layers. Various courses might also give information about customer protection. In the IoT, some security risks are as follows:

Data lifecycle assurance from end-to-end E2E: Data in an IoT environment must be protected from beginning to end in order to ensure its safety. Information is acquired from a variety of devices linked together and immediately sent to further devices. In this way, it is necessary to have a system in place to maintain the security of information, classify information, and monitor data protection across the whole life cycle of information.

Organizing things in a safe way: The IoT devices' connectedness and correspondence shifts as a result of the situation. The devices must be able to stay up with the current degree of security. For example, if adjacent gadgets and sensors in a home-based business are able to communicate securely with one another, their communication with external devices should also be safe.

Misconfigurations by customers are the primary cause of security issues, and the majority of these issues can be remedied. It is very difficult and unfair for customers to implement these complicated security systems. It's anticipated that you'll choose security measures and, if necessary, security measures and tactics that may be used in the future.

The Dangers of an Intelligent Home

A huge portion of the home service providers don't consider about security limits when they start out, putting them at risk for cyberattacks. Unauthorized access to a smart home network compromises its security by listening in, causing a Distributed Denial of Service (DDoS) attack, and leaking data.

1) Trespass: The aggressor may enter the clever house without smashing the entrance if the lock on the clever door is impacted by noxious codes or is accessed by an unapproved person. This impact might result in a mortality toll or a loss of property. In order to prevent such attacks, passwords should be updated often and include at least 10 characters, which is very difficult for attackers to crack. Access control may also be used in conjunction with the verification component.

Monitoring and leakage of personal data are two important reasons for a smart home. Consequently, there are a lot of sensors that are used to monitor fires, children, and housebreaking. If these sensors are hacked by a trespasser, he will be able to monitor the residence and acquire personal information. Encryption of entryway and sensor data, or client validation to detect unapproved gatherings, should be used to ward off this attack.

For example, an attacker could gain access to the home organisation and send mass messages to devices like Clear To Send (CTS)/Requested To Send (RTS) (RTS). DoS attacks on various devices in a smart home can also be performed against a designated gadget using vindictive codes. As a result, high-tech devices are unable to carry out their intended functions because of dwindling resources. Confirmation may be used to prevent and detect unauthorised access and evade this attack.

The attacker may collect the packages by modifying the directing table in the door when smart home devices communicate with the app server. An aggressor may be able to circumvent the SSL (secure attachment layer) approach, even if it has been applied, even though the declaration has been generated. As a result, the aggressor has the ability to confuse the content of information or to disclose information classifications. So that this attack might be used to get the keen domestic organisation , SSL method with legitimate verification system ought to be applied. It is too critical to impede unapproved gadgets that might attempt to get to brilliant home organization.

Imagine a future when physical items linked to the web can communicate with one other and differentiate themselves for various devices. This is known as IoT (Internet of Things). Associating one person with another, a human with real articles, and an actual thing with other actual objects was made easier by the Internet of Things. IDC estimates that by 2020 there will be 30 billion web-connected devices. In order to keep up with the rapid growth of online content, more substantial and safe structure is needed.

Challenges Faced by the Internet of Things

The biggest challenge in IoT is dealing with the issue of security. An application of IoT's application information might be contemporary, a business endeavour, or an individual buyer. Moreover, this application data must be collected and kept private against theft and alteration. It's possible that a patient's health or purchasing habits may be recorded by IoT apps. Interaction between devices is a key component of the Internet of Things, yet there are challenges related to the IoT's flexibility, accessibility and response time. Security is a concern when data is sent via the Internet. Unofficial laws, like as the Health Insurance Portability and Accountability Act (HIPAA), may be used to protect the information when it travels across international borders. The most major IoT security concerns are discussed, among a variety of others.

There are certain smart TV manufacturers that collect information about their customers in order to better understand their survey propensities so that the information they obtain may be tested for data security during transmission.

It's also a great test to see how secure your data is. Avoid being distracted by web-connected items when transferring data perfectly.

IoT-enabled devices on automobiles may be used to collect information about a driver's health and driving habits, which insurance companies can use to make decisions regarding insurance coverage.

As a result, there is a lack of a standard for IoT devices and IoT-related businesses. As a result, determining which devices are authorised and which are not is a significant challenge.

Due to the increased use of IoT devices, the amount of traffic generated by these gadgets is also increasing. As a result, there is a pressing need to extend the network's capacity, and it is also a challenge to store the enormous amount of data for further research and final storage.

In the context of system security, the IoT framework is used to identify different security threats, create different security systems, and establish acceptable security rules to ensure network security.

For IoT applications, the application security works to deal with security risks as per the situation's requirements.

It's important to have a secure network in place to ensure that different IoT devices can communicate with one another.

V. CONCLUSION

This paper's primary focus was on highlighting important IoT security challenges, with an emphasis on security attacks and responses. Numerous IoT devices become susceptible targets due to the lack of a safety component, and in fact, this isn't even in the casualty's information about being infected. In this study, the security requirements, such as categorization, trustworthiness, and verification, are studied in detail. A total of twelve distinct attacks are evaluated, each with a corresponding degree of severity (low, medium, substantial, and wonderfully significant) and their inclination/conduct, as well as possible responses to the assaults' experience.

Considering the importance of security in IoT applications, include security features into IoT devices and communication networks. In addition, avoiding using default passwords for devices and reading the security requirements for devices before using them for the first time are recommended for preventing gate crashers and security risks. Reduce the likelihood of safety attacks by incapacitating provisions that aren't being used. Examine various security protocols used by IoT devices and organisations. Besides that,

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

[13] M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, “Comparativeanalysis and implementation of efficientdigital image watermarkingschemes,” International Journal of Computer and Electrical Engineering, vol. 4, no. 4, p. 558, 2012.

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

[15] S. Singh and N. Singh, “Internet of things (iot): Security challenges,business opportunities & reference architecture for e-commerce,” inGreen Computing and Internet of Things (ICGCIoT), 2015 InternationalConference on. IEEE, 2015, pp. 1577–1581.

[16] S.Kannadhasan, G.Karthikeyan and V.Sethupathi, A Graph Theory Based Energy Efficient Clustering Techniques in Wireless Sensor Networks. Information and Communication Technologies Organized by Noorul Islam University (ICT 2013) Nagercoil on 11-12 April 2013, Published for Conference Proceedings by IEEE Explore Digital Library 978-1-4673-5758-6/13 @2013 IEEE

[17] K. Rose, S. Eldridge, and L. Chapin, “The internet of things: Anoverview,” The Internet Society (ISOC), pp. 1–50, 2015.