e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:02/ February -2022 Impact Factor- 6.752 www.irjmets.com

IOT SECURITY THREATS AND CHALLENGES

Noman Masher*1, Kashaf ul Mahjoob*2

*1Department of Information Technology1, University of Gurjat, India.

*2Department of software engineering, University of Gurjat, India.

ABSTRACT

Modern humankind is equipped with hundreds of inventions, embedded devices, wireless networks, cloud computing, and numerous handheld devices are; some examples of these. Embedded intelligent devices connected with the internet make the concept of the Internet of Things(IoT). IoT is one of the most widespread technologies that aim to change the classical internet of contents scenario. With the help of IoT, all of our daily routine devices, even refrigerators, AC, vehicles, and other things, will be connected with the internet to participate in easy human life. IoT networks face numerous challenges; the security and privacy of IoT devices and networks are critical challenges for IoT researchers and engineers. In this paper, we investigate security issues of IoT networks in a broad range.

I. INTRODUCTION

IoT, cloud computing, big data, Metaverse and quantum computing are the most demanding technologies of today's world[1-7]. IoT involves embedding our everyday objects with internet connectivity to share data and communicate among themselves[8]. Our daily life objects are embedded with sensors, software, and communication resources to exchange data with other such embedded devices. The remarkability of this advancement is that the internet is connected to technical devices such as mobile devices and our traditional physical objects that one uses in their routine. This research deals with the security risks and challenges IoT system faces regarding the devices' security and privacy. Physical objects such as cupboards and drawers can be protected from theft by placing locks n them. What happens when all of our everyday objects are connected through the internet? It increases security threats as there is a risk of cyber attacks and mishandling of personal information. In recent years, while more and more people have become aware of the benefits of IoT, there is still a large community of people that find it untrustworthy ad creepy to connect their daily life objects over the internet. These trust issues arise from increasing cyberattacks day by day and people losing their valuable information over the internet. Since IoT involves every object around us, other than just technical devices, it faces considerable security risks and challenges.

Fig 1: IoT involving everyday objects

The above picture shows how the information of things system involves things from houses, cars, flights, wall clocks to as little as the pens and table lamps we use. Handling the security of such an extensive collection of connected objects in one system is demanding and challenging. A few reasons for those challenges are:

- IoT involves highly personal user information.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:02/ February -2022 Impact Factor- 6.752 www.irjmets.com

- Data storage is distributed.
- Incorporation of sensors in devices.
- Malfunction caused by bad actors.

The above mentioned are a few reasons that cause people to mistrust IoT systems. We will explore them further in this article.

Causes of security threats

First, we will talk about the personal information that IoT devices collect. For example: if a user's car is incorporated with sensors and made a part of the IoT system, it would track their travelling history. Many users may feel insecure about someone watching their every move. Wherever the user drives to is recorded in the system database. If a house is connected with an IoT system and all the devices are made part of the said system, it may reveal the personal behaviour of the residents and their way of living. If medical devices are attached to the IoT, they may reveal information and record about a user's health. In a 2016 survey, the users revealed that they are concerned about sharing information that may reveal their personal information. This causes the consumers to mistrust the IoT system.

Now, on to the next issue. The data in IoT devices is processed locally, and there is usually no central data server to store and process information. Decentralized storage implies that the may user have to take responsibility for the security of their information in some aspects. The integrity of the system relies on individual users to maintain. Individual actors may deviate from their response to IoT devices that may cause inaccuracy inaction taken by the said devices.

Next is the incorporation of sensors in objects. Though it is highly beneficial to incorporate sensors in IoT devices, it may cause some harm. Cyber attackers can give false input to the sensors and control the flow of actions. For example, an attacker may input the wrong location into the car's sensors, leading the car to ward off in the wrong direction.

It can cause false users to control the devices and breach security. The IoT devices are partially programmable, and primarily they run on sensors. A user might input a wrong response by accident that may cause the device to take a wrong turn. For example, average consumers are not aware of using medical devices. Tey may mishandle the device or give false commands that could lead to health risks. In this sense, IoT devices can be corrupted by bad actors.

There may be insecure communication between IoT devices. Devices may share inaccurate information among themselves that could cause the system to malfunction.

Hence, it is customary to provide solutions to these threats so the users can put their trust in the IoT system.

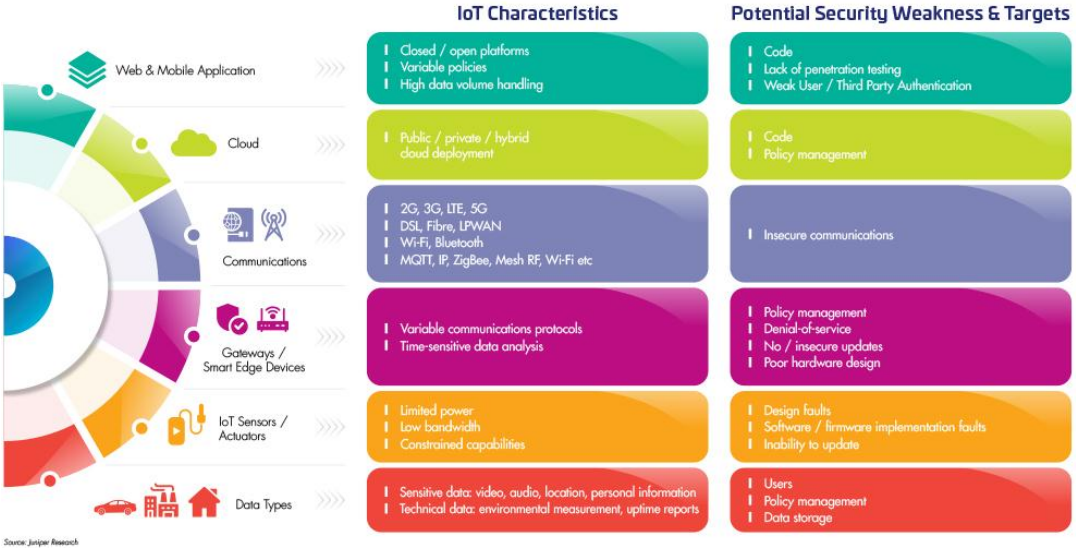

Fig 2: IoT security threats

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:02/ February -2022 Impact Factor- 6.752 www.irjmets.com

II. THE SOLUTION TO SECURITY THREATS

This section will discuss the possible solutions and actions an IoT system can perform to reduce the security risks in the devices.

Redundancy inherent:

Redundancy inherent may be used to avoid and reduce cyber attacks in the system. A redundant node is an unnecessary node that may not be crucial for a function in the system. Accountability is used to check different calculations from each node. If the calculations do not match the node being checked, the node is declared false and redundant.

State estimation:

State estimation is the process that terminates insecurities in the network and estimates the network state. It is used to adjust the results closer to the observed values. This process can be used to avoid attacks on sensors. It estimates all the possible outcomes from a particular sensor. If the response collected from said sensor falls outside the estimated range, then the sensor is isolated from the system for security reasons.

Data centralization:

So the user does not have to concern over the integrity of the devices, and the processes can take place over a more centralized server.

III. CONCLUSION

The solutions mentioned above can also be compromised. For example: in the inherent redundancy process, if the nodes assigned to check the calculations of the redundancy node are attacked and compromised, they will fail to identify the false node. Similarly, regarding state estimation, the estimated range can be attacked. Hence, no solution could eliminate the security threats to IoT devices. All we can do is maximize the probability of tackling security risks mitigating the threats.

IV. REFERENCES

[1] G. K. Sriram, "Edge Computing vs. Cloud Computing an Overview of Big Data Challenges and Opportunities for Large Enterprises," International Research Journal of Modernization in Engineering Technology, 2022.

[2] G. K. Sriram, "Security Challenges of Vehicular Cloud Computing," International Research Journal of Modernization in Engineering Technology ..., 2022.

[3] M. G. K. Sriram, "Advantages Of Leveraging Machine Learning In Healthcare Industry."

[4] M. G. K. Sriram, "Azure Quantum–An Emerging Quantum Computing Ecosystem."

[5] M. G. K. Sriram, "Challenges Of Cloud Compute Load Balancing Algorithms."

[6] M. G. K. Sriram, "Security Challenges Of Big Data Computing."

[7] G. K. Sriram, "A Novel Approach for Cloud Exchanger Problem Using Blockchain Based Solution," International Research Journal of Modernization in Engineering Technology, 2022.

[8] S. A. Shah and N. Mazher, "A review on security on internet of things," in November 2018 Conference: 1st International Multi-Disciplinary Research Conference (IMDRC 2017).