Security, Privacy, and Trust in IoT

Saanjith

January 22, 2023

1 Introduction

The term ”Internet of Things,” which is frequently abbreviated as ”IoT,” has various definitions available .IoT describes and depicts the interconnection of numerous ”things,” sensors, and smart devices. It is embedded with a variety of sensors, actuators, and software programs to gather, exchange, and collect data further. It connects to the internet via connectivity. There are a few well-known IoT initiatives that concentrated on security and their comparison.

2 TRADITIONAL INTERNET AND INTERNET OF THINGS

The absence of a human role distinguishes the internet of things (IoT) from regular internet. The Internet of Things (IoT) apps and devices offer a variety of services and amenities that are beneficial to human life. The phrases ”Internet” and ”Things” are seen as one word, giving the idea that many physical devices of various standards from around the world are connected to the internet for a particular purpose. Boost and cover the effectiveness of information exchange on the internet. Machines produce content by initiating processes and pushing data. Employing operators with the use of sensors, produce (e.g. Temperature, pressure) Incorporate intelligence into the process

3 SECURITY, PRIVACY, AND TRUST IN THE INTERNET OF THINGS

In terms of usefulness, efficiency, and dependability in IoT, security is crucial. The fundamental requirement of self-actualization in the IoT is the desire for privacy. Applications for patient monitoring systems, traffic management, energy consumption inventory management, smart parking, civil protection, and many others are all in use today. The end user should be given a guarantee of privacy. According to the internet of things, the key feature that arises is privacy, and with privacy comes trust. When a device has a security and privacy component, the end user develops trust, which is a crucial aspect or factor.

4 WAYS FOR SECURITY, PRIVACY, AND TRUST IN IoT

TRadio frequency identification (RFID), near field communication (NFC), and wireless sensor networks (WSN) are a few of the IoT core technologies. The automated exchange of information between two devices or two ends in the internet of things occurs through some of the communication technologies that are described below. The internet of things relies heavily on wireless sensor networks (WSNs). RFID Radio frequency identification (RFID) is one of the key components of the Internet of Things (IoT) and its applications, claims. RFID One of the crucial components in the Internet of Things and its applications, according to is radio frequency identification (RFID). The development of microchips for wireless communications is made possible by a significant advancement in the embedded transmission and communication paradigm. The specifics of the RFID concept are covered in

5 OPEN CHALLENGES

IoT is a topic for the modern and new eras. IoT is a vast concept that connects billions of things with complete efficiency and usability. It is a significant research challenge to manage such big data, heterogeneous networking environments, and secure information and communication technologies. The areas that will represent the unresolved problems and challenges are listed below.

6 CONCLUSION

As we have discussed in this paper about the security, privacy, and trust that what is security, trust, privacy, importance, needs, issues, and challenges. IoT is an emerging technology that has gained importance over the past decade. In order to perform and use the technology in our daily routines, we must understand the major and fundamental concepts of IoT. IoT is used in a specific zone but it is applied on multiple zones, including homes, the grid, health care, industry, agriculture, and other entities. For this reason, we must understand the IoT and the critical aspects of it.