IOT-CHALLENGES AND OPPORTUNITIES

Pallavi Murghai Goel, Associate Professor, Department of Computer Applications,
Galgotias University

ABSTRACT

The internet of things (IoT) is made up of the notion of the free flow of information between different low-power embedded devices which utilise the Internet to connect. The IoT is projected to be extensively used and to be applicable in several fields of life. IoT requests have recently received enormous attention and enterprises are thrilled about the financial value of the data created by the deployment of these networks. In contrast, IoT has different security and privacy considerations that restrict the proliferation of end-users. In this work, we have identified, classified and addressed numerous threats to security and state-of-the-art efforts to address these difficulties.

KEYWORDS: IOT, Challenges, Opportunities

INTRODUCTION

Emerging advancements in embedded technology and the Internet have allowed items around us to be interconnected. We are looking for a future in which IoT devices are invisibly integrated into the world around us and generate a huge quantity of data. These data should be preserved and processed in order to make them intelligible and valuable.

An IoT model includes a number of players, including mobile carriers, software developers, providers access technologies, etc. IoT applications are also quite wide-ranging and may be used in production, utility administration, agriculture and healthcare. IoT may be considered as a next generation paradigm for connection between devices and machines that allows action to occur without human interference. A combination of another communication infrastructure is necessary for the development of the IoT world. This has resulted in the invention of intelligent gateways for IoT devices connected to the conventional Internet. The latest efforts are aimed at integrating IoT infrastructure with cloud computing, which enhances IoT's potential.

More and more complicated IoT networks also add to the security issues of these networks. The complexity of the IoT networks is due to the massive number of internet-connected devices and the enormous data created by these devices. IoT attacks are conceivable because infiltration devices inside the IoT network are
an accessible target. Hackers may take control and do harmful operations when hacked and target additional devices near to the compromise node. IoT devices have no malware or virus prevention software. This is a natural result of the minimal memory and low power features of these instruments. The inaccessibility of virus and malware on IoT devices makes them very prone to becoming bots and malicious activities on other network devices. Once an IoT device is compromised, the attacker may also deter the device's routing and forwarding activities. Besides hacking many other network devices, attackers may also get access to IoT devices' sensitive data. This lack of confidentiality, integrity and data safety in IoT may interfere with the mainstream use of this technology.

**CHALLENGES**

Each such confidentiality or framework in IoT should handle the following challenges:

Tracking and profiling. Associating an identity with a given person is a danger that may lead to profiling and monitoring. Therefore, one of the main issues is to discontinue IoT activities and to take certain precautionary action.

Tracking and location. Tracking. Localization is another hazard as technologies are attempting to identify and record the whereabouts of each son in time and place. One of the primary problems of IoT security solutions is to develop protocols for IoT interactions which prevent such activities. In e-commerce applications, profiling information about a certain person to infer interests in the correlation between other profiles and data is quite prevalent A major difficulty is to balance company goals with user privacy needs for profiling and data analysis.

Secure transmission of data. Yet another security is that data are delivered securely over the public media without someone being caught and so avoided.

**OPPORTUNITIES**

The latest work addressing the security and privacy problems of cloud-based IoT is available. Cloud-based IoT security and privacy needs as identified by the authors include the privacy of identity, location, node compromise attack, removal/add layer, forward and backward security, and semi constrained and malicious security in the cloud. Another recent endeavour is an effort to examine current data protection technologies. The writers identified the gaps in different plans and suggested that they should be removed. Authors in current IoT apps have been surveyed. In this study, the authors propose to translate their modules into a common system model while simultaneously identifying and studying the behavioural differentiation of the generation of sensor data. The investigation revealed that practically all apps collect information about the location and the time. Any data collected may be of several sorts, including video and audio. The authors examined up-to-date data protection procedures. In addition, possible dangers to user privacy in participatory sensing resulting from uncontrolled personal information disclosure to untrusted persons were highlighted.
The authors also mapped their study to a suggested shared system model for the security analysis of mobile participatory sensing applications..

A full explanation of security and privacy risks may be found in IoT designs. The talk starts with IoT's detailed architecture. Privacy and security risks are studied in depth at every level of the architecture. State-of-the-art threat scenarios are explored in depth on several levels of IoT architecture. Based on the scenarios outlined, the security challenges at stake include eavesdropping, human assaults and other similar assaults that compromise the confidentiality and integrity of data and the collection of controls over certain components. The authors also investigate the upcoming EU IoT laws. It is necessary to understand the IoT architectural management domains. EU law demands that a person be able to monitor his or her information at all levels of architecture. Further studies need a thorough examination of how this kind of control is technically provided. Energy components of privacy and risks need to be further studied.

CONCLUSION

In this article, we have classified and discussed the cutting edge effort to ensure IoT network security. Data protection efforts, light-weight encryption frameworks, safe transmission and routing, robustness and resistance management, service de- nial and insider threat detection are examined in depth. Data protection is of particular importance in IoT, as the features of such a network differ from the normal Internet network. This paper identifies and discusses such challenges and needs. In addition to privacy, lightweight cryptographic primitives are necessary for the security of the IoT network. All efforts are collated in this regard and future measures are addressed. To safeguard privacy, tech-nics and lightweight context-conscious protocols are developed and virtualization methods are most recently utilised to ensure the integrity of data. Novel methods that employ limited IoT mote resources are needed for lightweight cryptography primitives. In addition, SDN solution offers lightweight cryptographic IoT solutions with the help of centralised SDN controller routing. IoT network encounters problems owing to heterogeneous network assaults on IoT nodes.

REFERENCES


traceability in cyber-physical manufacturing systems. *Sensors (Switzerland), 16*(3).
https://doi.org/10.3390/s16030382


https://doi.org/10.1016/j.procir.2017.02.035


https://doi.org/10.1109/ACCESS.2017.2777438


