(IJIEEE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9592; p-ISSN: 2454-8081**

ANALYZING THE KEY INFLUENCES IMPACTING EXISTING AND EMERGING INTERNET OF THINGS (IOT) SECURITY FEATURES INCLUDING BLOCKCHAIN TECHNOLOGIES TO MITIGATE CYBER-ATTACKS AND ENHANCE SAFEGUARD

Romharsh Mittal

ABSTRACT

Objective: This study presents IoT security features, IoT security layers' challenges with the application layer and network layer.

Methods/Findings: Major security concerns of IoT development are caused by the heterogeneity of interconnected entities, as well as the incompatibility of the development and communication protocols used. Authentication, integrity, and availability are compromised by attacks as man-in-the-middle, replay, and denial of service attacks. Looking into the future, blockchain and software-defined network technologies, are promising to deliver a more secure IoT operational environment, and could, therefore, reduce associated cyber-attack instances.

Application: Furthermore, IoT security solution with current IoT security arrangements incorporate trust foundation, a move towards an integrated design and architecture is also discussed.

1. INTRODUCTION

The technology domain is ever disrupted by rapid developments and innovations that come along with opportunities and threats. For every opportunity provided by any technological innovation, hackers and scammers find ways of maliciously exploiting them. Cyber-attacks have been known to It security experts since the dawn of computers and the internet. The internet became a primary playground for attackers and has been used to launch devastating attacks on individual users, small, medium, and large business organizations as well as governments. The nature of attacks has grown to match technology, and the application of sophisticated tools has resulted in increased magnitude and number of cyber-attacks.

The world now relies on powerful computing technologies such as Big Data, Internet of Things, Data Analytics, Machine Learning, Artificial Intelligence, Smart Grid Systems, Cloud Computing, and Business Intelligence. All these run on highly complicated platforms that must always be tamper-proof lest attackers compromise them services and components. IoT is one of the fastest-growing technologies which bring together millions of interconnected objects, services, devices, and humans (things). The interconnected entities communicate by sharing data and information through a stack of rules and protocols. IoT devices use uniquely identified by both the region they are in and their IP

addresses using a typical identity management system. Radio Frequency Identification and Wireless Sensor Networks have attributed to the rapid development of this technology and have attributed to the development of smart cities, homes, and transportation infrastructure. The RFID tagging of every device provides an identification mechanism for connected devices. WSN, on the other hand, has allowed the interconnected things to be wireless identifiable and communicate with the physical, cyber, and digital world. The main motive of this work is to investigate the purpose of this paper is to research on the current state and future trends of security in the Internet of Things (IoT) as the computer revolution moves with speed to interconnect millions of devices and individuals, and enabling communication between them. Section II, III, IV, and V of this paper describe the IoT security features, IoT layers' security challenges, IoT security solutions, and future trends of IoT security, respectively.

2. IOT SECURITY FEATURES

Security challenges in this development are either caused by technological or safety problems. Security challenges are related to the functionalities and principles that must be enforced to create a securely-networked environment. Such challenges require that end-to-end security, integrity, confidentiality, authentication, and authorization features be implemented. The features and privacy challenge general background is stated. Technology defined problems are as a result of the heterogeneous and ubiquitous nature of IoT devices. They are caused by IoT features such as scalability, wireless connections, energy, and distributed environment. IoT platforms provide security by running authorized software on all devices, running an authentication program whenever a new device (or thing) is turned on or connected to the network, and by installing necessary software updates and patches. Security practices are anchored on the CIAConfidentiality, Integrity, and Availability security goals. Confidentiality means that communications and transactions only reach the intended persons and are not exposed to unauthorized attacks. Integrity refers to the security mechanisms used to preserve the authenticity of data- whether stationary or in transit. In IoT, security experts must make sure that sensors conceal information about other neighbours. To secure data, IoT users must understand how data is managed plus all the involved processes. The integrity feature is based on data exchanges between many different devices. It ensures that information is not tampered or interfered with, and is not manipulated during the transmission. The availability feature is the backbone of IoT technology- connecting millions of devices. Data and connected 'things' must always be available to end-users. As a security requirement, every IoT device must identify and correctly authenticate other devices and users accessing them, or requesting access to their data and services. However, this is a security challenge due to the nature of entities and objects involved.

Every interaction must, therefore, be mutually authenticated, especially where entities are interacting for the first time. Lightweight solutions offered a unique security feature and were introduced due to the computational and power limitations of IoT entities. Since these solutions are meant to run on a device with varying and limited capabilities, they need to be compatible with each device's computational capabilities.

3. IOT SECURITY LAYERS' CHALLENGES

3.1 Application Layer

Signals in IoT are transmitted over long distances from sensor nodes to entities using wireless technologies. Disturbing waves could compromise the efficiency of wireless signals. Maliciously intended people can physically attack sensor nodes because they operate in an external environment. The limited storage and computational capacities and power consumption of IoT entities, which are inherent to the nature of network topology, expose IoT entities to many types of security attacks, threats, vulnerabilities, and risks. Replay attacks could easily be used to compromise the system's confidentiality by spoofing, altering, and replaying identity information belonging to other devices. Other attacks include node capture attacks, which add another node to the network, denial of service (DoS), and timing attack, which occurs when attackers successfully analyze the time needed to encrypt IoT messages and data.

3.2 Network Layer

At the network layer of IoT, man-in-the-middle attacks are widespread. The susceptibility is caused by the nature of access mechanisms and data exchange. The communication channel quickly gets compromised when attackers launch eavesdropping attacks. The introduction machine to machine communications in IoT has resulted in incompatibility issues, which make it difficult for traditional internet protocols to operate. Attackers, in turn, take this advantage to gain more information about users and interconnected devices and later use this information for criminal activities. Both the network and connected objects must be protected and well secured. Artifacts should have the ability to learn a network's state of security and operation to protect them from any form of attack. This creates the need for compatible protocols and useful software applications to enable objects' automatic responses to abnormal situations and network behaviour. By focusing on network layer functions, different technologies such as Device to Device (D2D) need different protocols to be operated.

3.3 Application Layer

The global community has not established any standards and policy statements that could be used to govern the development of, and interaction between IoT entities. Different systems use different authentication mechanisms, making it challenging to integrate them and ensure data privacy and identity authentication. Interconnected objects share extensive data, resulting in high overall costs in the applications used to analyze the data. These general costs could negatively affect the availability of system services. The general study of the application layer is mentioned6.

4. IOT SECURITY SOLUTIONS

Current IoT security solutions include building trust, a move towards a federated architecture, authentication measures, and security awareness. Authentication measures allow entities to authenticate themselves before they can access corporate and other entities' services and data. End-to-end encryption algorithms prevent any unauthorized access, attacks, and interference. Firewalls are extensively used to filter traffic from external networks; therefore, allow the use of secure resources.

(IJIEEE) 2019, Vol. No. 5, Jan-Dec **e-ISSN: 2454-9592; p-ISSN: 2454-8081**

A federated architecture aims to solve compatibility problems in IoT by providing a centralized unit which goes beyond the nature of the heterogeneity of IoT entities. The general security context is established 7. 5. Future trends in IoT security The emergence of more powerful technologies such as blockchain and software-defined networks (SDN), the probability of new effective security solutions in the IoT is increasing. There is accelerated research on the applications of blockchain technology to provide IoT. A blockchain can be used to create a mesh network that It allows IoT entities to connect securely and reliably and avoid any possibility of identity theft and identity theft. Any device registered with the blockchain would have a unique identifier. For such devices to connect, the blockchain ids will be used as URLs, while the local blockchains wallets will raise identity requests8. SDNs have improved network operations, made them more flexible, and made network management activities easier. This technology can also be used to ensure the security of the IoT. SDN controllers could be configured in such a way that after adequately authenticating connected devices and establishing a secure connection between the switch and the controller, all other ports on the switch are automatically blocked. SDN controllers are typical security guards who receive the initial transmission flow whenever two or more devices wish to communicate. It ensures that the methods know the destinations of the requested transmission flow before they can start exchanging data.

5. CONCLUSION

The Internet of Things (IOT) is a powerful technology that has interconnected millions of devices, including humans, across vast geographic areas. The main security concerns of this development are due to the heterogeneity of the interconnected entities, as well as to the incompatibility of the development and communication protocols used. Authentication, integrity, and availability are compromised by attacks such as intermediate attacks, repetition, and denial of service. Looking into the future, blockchain and software-defined network technologies, are promising to deliver a more secure IoT operational environment, and could, therefore, reduce associated cyber-attack instances.