Chapter 20
A Novel Intrusion Detection System for Internet of Things Network Security

Arun Kumar Bediya
Jamia Millia Islamia University, India

Rajendra Kumar
Jamia Millia Islamia University, India

ABSTRACT

Internet of things (IoT) comprises a developing ecosystem of responsive and interconnected devices, sensors, networks, and software. The internet of things keeps on extending with the number of its different equipment segments for smart cities, healthcare, smart homes, assisted living, smart vehicles, transportation, framework, and many more are the areas where the internet of things benefits human lives. IoT networks are meant to be monitored on real-time events, and if these devices get attacked, it can have an unfavorable effect on the system. This paper discussed many possible attacks at IoT networks and distributed denial of service (DDoS) attack is one of the most dangerous among them. Blockchain technology can be utilized to develop a framework to protect IoT systems; blockchain is a new technology used for cryptocurrency transactions. This paper proposed BIoTIDS an intrusion detection system for the IoT network using blockchain. BIoTIDS is able to detect an intruder in the IoT network and also able to identify DDoS attacks in IoT networks.

INTRODUCTION

The Internet of Things (IoT) technology and IoT devices are widening at a swift pace, many reports speculate that IoT devices will expand to 26 billion by 2020, Currently, it is numerous times that was evaluated total devices in 2009 and it is undeniably more than the 7.3 billion cell phones, PCs and tablets that are dependent upon to being used by 2020 (Middleton, Kjeldsen, & Tully, 2013).

DOI: 10.4018/978-1-6684-7132-6.ch020

The IoT can be defined as "an overall system of interconnected objects", these objects must have three characteristics, a unique identity by which it can be addressed, it can be accessed using the internet or smart interface, and lastly it must be self-organized and repairable. IoT is a combination of hardware and software, where hardware may consist of sensor nodes, Radio Frequency Identification (RFID), low energy Bluetooth devices, Near Field Communication (NFC) and many more. The software provides middleware, information queries, data repository, and data retrieval and exchange. All WSN devices turn on the IoT component when it is supervised using the internet and significant security issues happen just when nodes are associated with the internet. This acquires many concerns identified with privacy and security, standardization and power management (Billure, Tayur, & Mahesh, 2015; "Internet of Things,"). Internet of things architecture comprises of three layer perception layer, network layer, and application layer. At perception layer sensors and actuators perform the collecting of data from the environment and prepare data to propagate towards the network layer. At network layer transmission of data from one device to another device is the primary task performed by this layer. Gateways, cloud computing devices, Routers, Switches are connected at this layer and use 3G, 4G, Wi-Fi, and Bluetooth networks. Finally providing smart surroundings is the primary task of the application layer. Data integrity, data authenticity, and data confidentiality are ensured at the application layer(Bediya & Kumar, 2019). Distributed denial of service (DDoS) attack is possible at each layer of IoT thus it is important to secure IoT networks with DDoS. DDoS detection, identification, and countermeasure have become a critical demand to secure IoT devices (Vlajic & Zhou, 2018; Zargar, Joshi, & Tipper, 2013).

Computer systems infected by malicious programs and remotely controlled by hackers are botnets (Choi, Lee, & Kim, 2009; Cooke, Jahanian, & McPherson, 2005). Botnets are generally utilized by unauthorized users to perform activities such as monetary frauds, illegal access to computer machines, and leak information (Mahjabin, Xiao, Sun, & Jiang, 2017). Botnets are a serious issue to computer networks and currently, IoT devices and networks do not have sufficient security mechanisms but have weak configuration and obtained hard coded credentials. Finally, the IoT system becomes easy targets for attackers that have such vulnerabilities (Aldaej, 2019). Research shows that approximately 16-25% of computers linked with the internet are active participants of botnets (AsSadhan, Moura, Lapsley, Jones, & Strayer, 2009; Kambourakis, Kolias, & Stavrou, 2017; Sturgeon, 2007).

Blockchain addresses the issue of centralized DDoS mitigation frameworks by presenting a distributed database that depends on a peer to peer network, giving a significant level of assurance and reliability. Exactly when another block is gathered by a node, it is imparted to the remainder of the nodes in the system. Each node that has obtained a block verifies it and communicates it further. Only leaders (miners) are allowed to add the block in the blockchain. These leaders are chosen arbitrarily by determining consensus algorithms liable to the methodology of the Proof of Work concept. Once a block is included in a blockchain it becomes irrevocable and cannot be removed or modified (Bano, Al-Bassam, & Danezis, 2017). Public and private are two types of blockchain. Public and private are the two kinds of blockchain. Public blockchain nodes can add or leave the network but in private blockchain nodes are planned and fixed. Ethereum that adopts the PoW consensus is a Public blockchain where each transaction has cost estimated in terms of "Gas". Bitcoin is another famous variant of Public blockchain. The private blockchain is also recognized as a permission blockchain. Ripple and Hyper ledger are Private blockchain