Chapter 13
Adaptation of Blockchain Architecture to the Internet of Things and Performance Analysis

Mevlut Ersoy
Suleyman Demirel University, Turkey

Asım Sinan Yüksel
Suleyman Demirel University, Turkey

Cihan Yalcin
Suleyman Demirel University, Turkey

ABSTRACT

Internet of Things (IoT) security and privacy criteria are seen as an important challenge due to IoT architecture. In this study, the security of the IoT system that is created with devices integrated into the embedded system by means of various sensors has been ensured by using a single cryptographic structure. The data transmitted between the nodes in the IoT structure is transmitted to the central node using the Blockchain data structure. The transmitted data is verified at central nodes and the energies consumed between nodes during the transmission phase is detected. An infrastructure has been developed for how blockchain technology can be used in the IoT structure. In this study, an experimental environment was developed and comparative analysis were made in terms of energy consumption and data transfer rates.

DOI: 10.4018/978-1-6684-7132-6.ch013

INTRODUCTION

IoT devices consist of different sensors and technologies in today's conditions. They collect data from certain environments, communicate with each other and create information services for the users. Within the context of IoT, an estimated 10-11 billion devices are assumed to be interconnected. These devices do not have autonomous defense skills against malicious approaches. The immature IoT standards are the main reason for this. Besides that, hardware and software modules that are used in IoT devices are non-standardized. Design, development, distribution processes are not hierarchical. Efforts to define a global security mechanism to secure the IoT devices and data transfers have also become a difficult problem to solve due to the diversity of resources on the Internet of Things. To solve this problem, the Internet of Blockchain-Based Things has been developed.

The rapid increase of the network devices and increasing number of cyber-attacks during the data transfer has revealed the necessity to develop solutions for this area. Numerous insecure IoT devices with heterogeneous nature and high computing power make them easy and attractive targets for attackers (Khan & Salah, 2018). The most up-to-date standardization and research activities are aimed at solving various security problems of IoT devices (Khorov et al., 2020). Most connected devices are easily exposed to security threats and attacks such as botnets during data transfer and these threats have proven that these devices have easily exploitable vulnerabilities (Wang et al., 2020). Due to the resource shortage and vulnerability in wireless communication, Advanced security infrastructures are needed for distributed computing systems that do not have a central control unit. (Kumar et al., 2014). The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are the types of attacks that mostly affect wireless networks. There is a lot of work involved to protect against these types of attacks. (Abramov & Herzberg, 2011, Aldaej, 2019). The addition of these protection systems to IoT structures provides significant disadvantages in terms of resource use. For this reason, protection systems added to IoT structures should be in infrastructures to eliminate such disadvantages. Likewise, the blockchain needs to be transformed into a heterogeneous system, such as users and verifiers, with clear role separations (Popov et al., 2019).

Transport and security protocols have great importance that ensure reliable and secure communication. There has been increasing interest to blockchain for security and privacy policies in the Internet of Things (Dorri et al., 2017). Blockchain is a technical framework that allows users to collectively protect the reliable database in a decentralized manner. In a blockchain system, data is generated and saved in units of the nodes. Sequential nodes are combined in a chronological order to create a chained data structure. All user nodes participate in the maintenance, repository, and validity of the data. More than half of users must approve the genesis of the new block. Data is broadcasted to all user nodes to create a network-wide synchronization (Dai et al., 2017). The neighbors of the nodes receive an identity and hash value with this broadcast. More nodes mean receiving higher validation and stronger security as a result. (Akyildiz & Jornet, 2010).The security and end-user privacy issues increase and become stricter in IoT, due to the asymmetric nature of the communications between sensors and the ordinary Internet hosts (Sahraoui & Bilami, 2014). For this reason, the use of blockchain has been proposed to contribute to the security and privacy issues of IoT applications.

In this study, the speed and energy usage of IoT with Blockchain have been analyzed. These analyzes have been compared with the non-blockchain structure in a second experiment under the same circumstances. In the developed experimental environment, Raspberry Pi 3 B + board was used as an embedded system. The IoT infrastructure has been installed with "Docker" in the Rasbian operating system.