Chapter 11
A Reliable Hybrid Blockchain-Based Authentication System for IoT Network

Ambika N.
https://orcid.org/0000-0003-4452-5514
Department of Computer Applications, Sivananda Sarma Memorial RV College, Bangalore, India

ABSTRACT

IoT is an assembly of equipment of different calibers and functionality working towards a single goal. A blockchain is a computerized record that contains the whole history of exchanges made on the system. A multi-WSN arrangement model is structured. The hubs of the IoT are isolated into base stations, group heads, and conventional hubs as per their capacities, which encourage the administration and participation of the hubs. A hybrid blockchain model is proposed. To fit the multi-WSN arrange model better, as indicated by the various capacities and energies of various hubs, neighborhood blockchain and open blockchain are sent between group head hubs and base stations individually, and a crossbreed blockchain model is framed. A shared validation plot for IoT hubs is proposed. For group head hubs, the creators utilize the worldwide blockchain for validation, and for customary hubs, they utilize the nearby blockchain for confirmation. The proposal aims in increasing reliability by 1.17% and minimizes sinkhole attack by 2.42% compared to previous contribution.

1. INTRODUCTION

The Internet-of-things known as IoT (Alaba, 2017) (Ambika N., 2019) is a get together of numerous supplies of various gauge and usefulness progressing in the direction of a solitary objective. The gathering point in speaking with one another using the regular stage gave to them. The gadgets in IoT (Khan & Salah, 2018) control distantly to play out the ideal usefulness. The data sharing among the gadgets at that point happens through the system utilizes the standard conventions of correspondence. The brilliant associated devices or ‘’things’’ extend from preliminary wearable accomplices to enormous machines, each containing sensor chips. The surveillance cameras introduced for reconnaissance of an area can be

DOI: 10.4018/978-1-6684-7132-6.ch011

checked distantly anyplace on the planet. Different shrewd gadgets perform assorting functionalities. An example, observing medical procedure (Ambika N., 2020) in clinics, home surveillance (Al-Ali, Zualkernan, Rashid, Gupta, & Alikarar, 2017), recognizing climate conditions, giving following and availability in autos and ID of creatures utilizing biochips are now serving as the network explicit requirements. The information gathered through these gadgets might be handled continuously to improve the effectiveness of the whole framework.

A blockchain (A & K, 2016) is a modernized record that contains the entire history of trades made on the framework. It is a fundamental purpose behind existing clear outcasts from money trades by bringing in trustworthy progressed cash. It is an assortment of associated blocks that are joined by hash regards made after some time. All information on the blockchain is never-ending and can't be changed. It is arranging worldview utilized for revelation, valuation, and move of quanta is the thing that we characterize as blockchain innovation. The innovation has its job in legislative issues, compassionate, social, conservative, and logical areas.

The invention utilizes to reinforce bitcoin. The blockchain is an open record that decentralizes a trustless framework to move money starting with one point, then onto the next over the web. The innovation intends to take care of the twofold spend issue. The go-between trust is not necessary for the use of the technique. It is a mix of open key cryptography and BitTorrent distributed document sharing. It makes a section of the coin proprietorship affirmed by cryptographic conventions and the mining network. The exchanges that occurred adds to the records. Two components are required – a private key and wallet programming. Utilizing the credentials gives the admittance to the sellers to make exchanges over the web. Wallet programming may record the trading made. The aptitude used in broad daylight record archives includes the report library, the vault of occasions, personalities, and occasions. Any advantage is it controls, follows, and traded. A standard calculation brings innovation into play. The computation acknowledges a document to change over into 64-character code. It guarantees the hash code created can't recover the source record. The exchange utilizes the hash code and timestamp. The source recovers from the proprietor's machine.

The previous contribution (Cui, et al., 2020) uses a hybrid blockchain system. It is a mix of a private and public system. The framework consists of different kinds of devices. Sink nodes gather data for further analysis. Regular devices deployed senses and transmit the processed data to the group heads. The client will be gaining access to the sensed data after authenticating themselves. The sink node and the customers incorporate a public blockchain system. The in-between group heads and regular devices use the local one.

The contribution is an enhancement of the previous suggestion. The nodes use identification and Ethernet address to derive the hashed value. The sink node will be able to map the address of the device to the Ethernet address. Other compromised devices using a similar Ethernet address will come into notice early. The reliability increases by 1.17% in comparison to previous work.

The work divides into seven divisions. The motivation of the proposal is in segment two. The literature survey follows the motive of the contribution. Segment four describes the proposal in detail. The discussion of the analysis of the contribution is in division five. The sixth part discusses future work. The writing concludes in section seven.