Journal of Engineering Sciences

Vol 13, Issue 02, FEB /2022

ISSN NO:0377-9254

SLIDING WINDOW BLOCKCHAIN ARCHITECTURE FOR INTERNET OF THINGS

BANDARU SANDEEP KUMAR[1], PPALLI RAMAKRISHNA[2]

#1Student,Department of CES, KIET, KORRANG.

#2 Associate Professor, Department of CES, KIET, KORRANG.

ABSTRACT: Internet of Things (IoT) refers to the concept of enabling Internet connectivity and associated services to nontraditional computers formed by integrating essential computing and communication capability to physical things for everyday usage. Security and privacy are two of the major challenges in IoT. The essential security requirements of IoT cannot be ensured by the existing security frameworks due to the constraints in CPU, memory, and energy resources of the IoT devices. Also, the centralized security architectures are not suitable for IoT because they are subjected to single point of attacks. Defending against targeted attacks on centralized resources is expensive. Therefore, the security architecture for IoT needs to be decentralized and designed to meet the limitations in resources. Blockchain is a decentralized security framework suitable for a variety of applications. However, blockchain in its original form is not suitable for IoT, due to its high computational complexity and low scalability. In this paper, we propose a sliding window blockchain (SWBC) architecture that modifies the traditional blockchain architecture to suit IoT applications. The proposed sliding window blockchain uses previous (n − 1) blocks to form the next block hash with limited difficulty in Proof-of-Work. The performance of SWBC is analyzed on a real-time data stream generated from a smart home testbed. The results show that the proposed blockchain architecture increases security and minimizes memory overhead while consuming fewer resources.

Keywords: ***Blockchain, Internet of Things, smart home, security, sliding window.***

1. INTRODUCTION

Blockchain is a distributed ledger used to record transactions between two or more parties. Unlike relational database systems, blockchain is a data structure where new entries get appended at the end of the ledger, and there exist no administrator permissions within a blockchain which allow modification of the data. Also, the addition of a new block to the chain needs to be verified by all other parties through a consensus algorithm. Since there exists a distributed control over the blockchain, it is difficult for attackers to modify the data compared to a relational database system. Relational databases are primarily designed for centralized data storage and blockchain are specifically designed for decentralized data storage. There exist two types of blockchains: (i) permissioned and (ii) permissionless. A permissioned blockchain is a private blockchain which requires pre-verification of the participants within the network who are assumed to know each other whereas, a permissionless blockchain is a public blockchain.

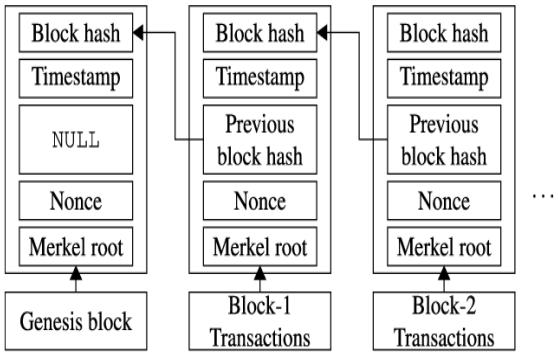

Fig.1: Blockchain Architecture

Journal of Engineering Sciences

Scalability refers to the limits on the number of transactions a blockchain can process within a specific time period. Bitcoin is a popular example of a blockchain. Bitcoin blockchain is a payment system that does not rely on a central authority to secure and control its money supply. Each block in a Bitcoin blockchain has limited block size. In Bitcoin, the block size is limited to 1 MB and a block is mined every ten minutes. Interestingly, the existing literature [3] suggests blockchain as one of the data security and privacy algorithms that can be implemented for IoT applications due to its distributed architecture.

2. EXISTING SYSTEM

Traditional blockchain approach is not suitable for IoT with real-time data streams due to their computationally complex Proof-of-Work (PoW) [2]. As the computational time increases, blockchain security becomes infeasible to be used for IoT. The two major challenges involved in applying blockchain to IoT environments include: (i) computational complexity and (ii) scalability. The computational complexity depends on difficulty level and Merkle tree size. Merkle tree is a tree in which every leaf node is labeled with the hash of a transaction data and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Merkle tree grows with the number of transactions made and, thereby, increasing the time consumed for Proof-of-Work, which is less favorable for an IoT network.

3. PROPOSED SYSTEM

In this paper, we propose a new blockchain architecture for IoT environments, especially in the context of smart home applications. A smart home monitors, analyzes, and reports the state of the home. Smart homes use devices connected to IoT to automate and monitor in-home systems [4]. Smart home can be considered as the smallest unit of a smart city. The security standardization of a smart home supports a smart city and vice versa.

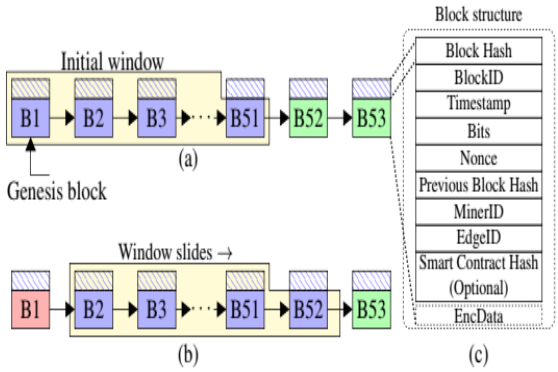

Fig.2: Sliding window blockchain architecture

The Sliding Window Blockchain (SWBC) utilizes a window that slides through the blockchain for every block addition. The window initially consists of one block and increases up to n blocks as defined by the window size. The blocks in the sliding window are used while creating a new block. In the proposed SWBC architecture, the block hash is generated by hashing the blocks in the window as shown in Figure 2. The size of the sliding window determines the number of recent past blocks used to perform the hash update function. The sliding window blockchain has a computational overhead of O(n) for a constant difficulty of mining, where n is the number of blocks in the window used for the hash update function.

Sliding window improves the immutability of the blockchain records. A false miner requires previous (n − 1) blocks and the window size n to mine a block. The window size is kept secret and sent only to the miners along with the genesis block. The limited part of the chain, i.e., the recent n blocks is stored in the memory of IoT device and the whole blockchain is stored in a private cloud. When the window slides, the older block comes out of the window (block B1 as shown in Figure 2(b)) and is deleted from the IoT device memory. Therefore, the memory overhead to store the blocks in IoT device is reduced.

Figure 2(c) shows the sliding window block structure. The SWBC block consists of block

hash, blockID, timestamp, bits, nonce, previous block hash, minerID, and edgeID. Block Hash is generated by hashing current block and previous (n − 1) blocks. The BlockID represents a unique ID of a block. Only the members are allowed to access the block ID of the newly added block. The field Timestamp shows the time at which the block is created. The field Bits represents the difficulty level of mining. The difficulty level of mining is decided by the number of initial zeros of the hash value. Each zero is represented by four bits. The difficulty levels are represented as follows: Level 1 (4 bits), Level 2 (8 bits), Level 3 (12 bits), Level 4 (16 bits), and Level 5 (20 bits). As the number of zeros increases, the difficulty level of mining (i.e., computation time) increases rapidly. A high difficulty level for PoW leads to an increase in computing resources, which makes Bitcoin blockchain not suitable for IoT. Also, to reduce the total computation time to mine the blocks, the difficulty level can be chosen at random between 1 and 5. The Nonce value represents the iteration for which the proof of work gets solved. The Previous block hash is the hash of the previous block which inherits the properties of previous n blocks, where n is the size of the window. MinerID represents the ID of the gateway and EdgeID represents the ID of the edge device. Smart Contract Hash represents the hash value of the smart contract accepted by all the miners. Smart contract hash field is optional and activating this field secures the smart contract from reentrancy attack. Smart contract hash field is not included in our experiment. The EncData consists of sensor data encrypted using the Advanced Encryption Standard algorithm with Password Based Key Derivation Function (PBKDF2).

4. RELATED WORK

4.1 A review on the use of blockchain for the Internet of Things.

The paradigm of Internet of Things (IoT) is paving the way for a world where many of our daily objects will be interconnected and will interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment and self-maintenance. Such features can be brought by blockchain, a technology born with a cryptocurrency called Bitcoin. In this paper it is presented a thorough review on how to adapt blockchain to the specific needs of IoT in order to develop Blockchain-based IoT (BIoT) applications. After describing the basics of blockchain, the most relevant BIoT applications are described with the objective of emphasizing how blockchain can impact traditional cloudcentered IoT applications. Then, the current challenges and possible optimizations are detailed regarding many aspects that affect the design, development and deployment of a BIoT application. Finally, some recommendations are enumerated with the aim of guiding future BIoT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BIoT applications.

4.2 Internet of Things for ambient assisted living: Challenges and future opportunities:

As the age profile of many societies continues to increase, supporting health, both mental and physical, is of increasing importance if independent living is to be maintained. Sensing, monitoring, recognizing activities of daily living, ultimately delivering immediate healthcare services has been perceived as a prerequisite for detecting the health status of the users. To date, extensive research been made in abovementioned areas, which is frequently named Ambient Assisted Living (AAL). Recently, the term of Internet of Things (IoT) has been emerging, which emphasizes the interconnection of all available resources both physical and virtual with the purpose of collecting and exchanging data. Thus, IoT technologies have been widely adopted for the gathering of health related resources to provide reliable and effective healthcare services especially to elderly and people with chronic diseases. Thereby, the aim of this paper is to present a brief overview of IoT enabled AAL systems and application particularly in the healthcare domain, and then identify the existing

Journal of Engineering Sciences

challenges and future research opportunities in this field.

4.3 Novel anonymous key establishment protocol for isolated smart meters:

In smart grid, fine-grained usage reports of consumers are gathered using some computationallyconstrained smart measurement devices. One of the most challenging requirements in the data aggregation is how to securely read the consumption data while putting the least possible overhead on the smart meters. For this reason, recently, two efficient security protocols have been proposed to be used for subsequent secure consumption reports gathering from isolated smart measurement devices. Nonetheless, in the both protocols, for each key establishment, the smart reader requires to connect to the electricity service provider (ESP) via the Internet. This paper proposes a novel key establishment protocol, which is both free from the ESP involvement during the key agreement and benefits from notable reduction in the communication cost. Our thorough efficiency and security analyses indicate the eminence of the proposed security protocol.

5. IMPLEMENTATION

In this paper author is describing concept to provide security to IOT devices using Blockchain technology as this technology supports decentralized data storage which means data will be stored at multiple nodes compare to centralized storage where data is stored at single centralized server. Decentralized data storage provides facility of receiving data from any available node and it has strong security where a single data store will verify hash value of all nodes. Verification of all nodes hash is computation intensive and its cannot be applied to IOT small devices due to memory, CPU and energy consumption restrictions. To overcome from this problem author introduce Sliding window technique where the window size will be fixed and all Blockchain transaction hash values will be stored in window and if window size exceeded then old transaction blocks will be slided or removed and maintain only recent blocks due to this technique memory storage and data transfer overhead will be reduced.

In this paper author is using sensor and other devices for implementation but we don't have any devices or sensors so I implement this project as simulation.

6. EXPERIMENTAL RESULTS

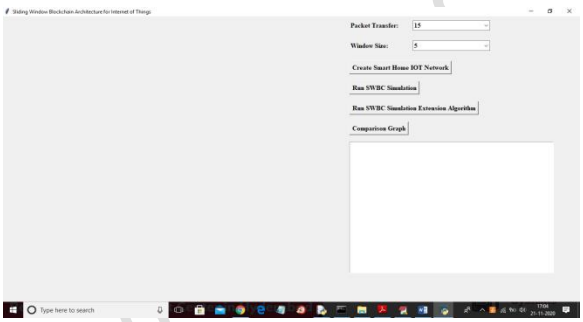

Fig.3: Home screen

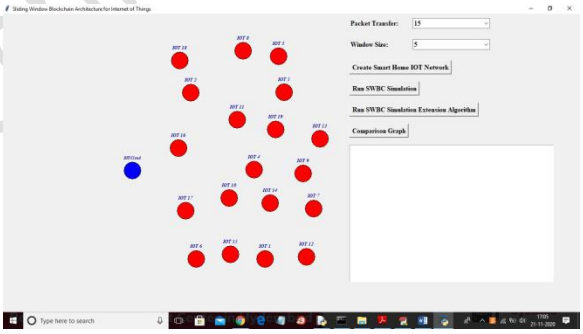

Fig.4: Create smart home IOT network

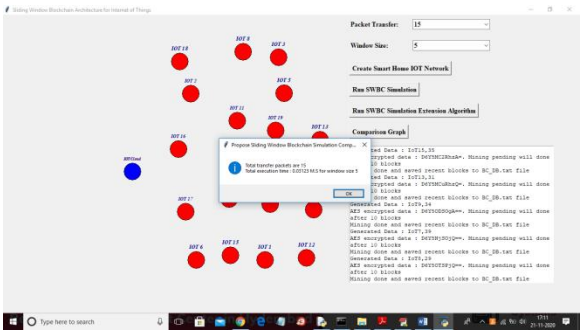

Fig.5: SWBC simulation

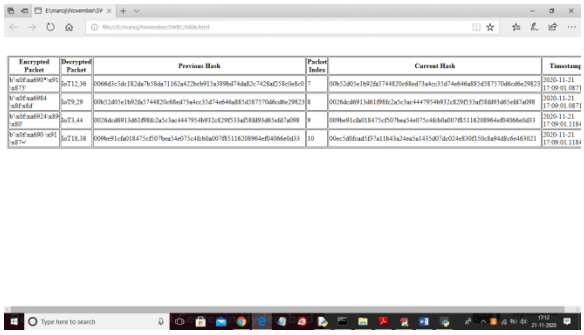

Fig.6: Blocks store at IOT memory

EXTENSION WORK:

In extension author is saying to further save energy so I am adding concept of monitoring data in time interval and if sensor generate same random data within time interval then IOT will not process that data to store in Blockchain and this duplicate avoidance can further save energy.

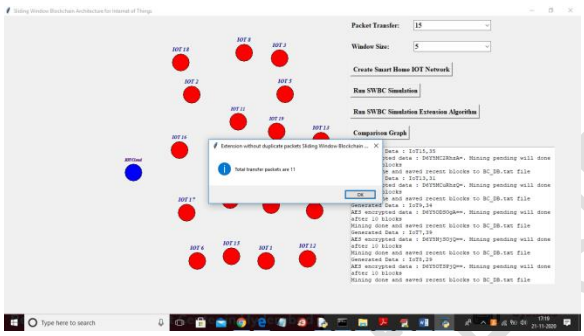

Fig.7: SWBC simulation extension algorithm

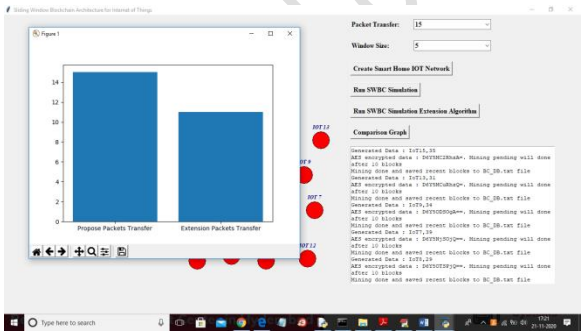

Fig.8: Comparison graph

7. CONCLUSION

IoT devices face constraints on resources such as computational capability, energy sources, and memory. Therefore, the standard security algorithms are not feasible for IoT. We proposed a sliding window blockchain that meets the requirements of a resource constrained IoT network by reducing the memory overhead and limiting the computational overhead. From the experimental results, we observed the following: (i) The computational time of PoW for each level of difficulty increases exponentially. (ii) The total block addition time increases with the increase in the number of miners in the group. (iii) As the window size increases, the hash computation time increases linearly. (iv) A random selection of difficulty for each block in a blockchain reduces the total block addition time

REFERENCES

[[1] S. Kulkarni, “The beauty of the blockchain,” Open Source for You, vol. 06, pp. 22–24, June 2018.

[2] T. M. F. Carames and P. F. Lamas, “A review on the use of blockchain for the Internet of Things,” IEEE Access, vol. 6, pp. 32 979–33 001, May 2018.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: challenges and solutions,” arXiv preprint arXiv:1608.05187, August 2016.

[4] IoT Agenda, “Smart home or building,” April 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/ smart-home-or-building

[5] L. Jiang, D. Y. Liu, and B. Yang, “Smart home research,” in Proceedings of 2004 International Conference on Machine Learning and Cybernetics, vol. 2, August 2004, pp. 659–663.

[6] theinstitute.ieee.org, “Towards a definition of the Internet of Things (IoT),” May 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE IoT Towards Definition Internet of Things Revision1 27MAY15.pdf

[7] J. Wan, X. Gu, L. Chen, and J. Wang, “Internet of Things for ambient assisted living:

Challenges and future opportunities," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), October 2017, pp. 354–357.

[8] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Novel anonymous key establishment protocol for isolated smart meters," IEEE Transactions on Industrial Electronics, vol. 67, no. 4, pp. 2844–2851, April 2020.

[9] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman, and T. Y. Lin, "The role of prediction algorithms in the MavHome smart home architecture," IEEE Wireless Communications, vol. 9, no. 6, pp. 77–84, December 2002.

[10] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," Security and Communication Networks, vol. 2018, pp. 1–11, June 2018.

[11] C. Lee, L. Zappaterra, K. Choi, and H. A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in IEEE Conference on Communications and Network Security, October 2014, pp. 67–72.

[12] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," Computer, vol. 50, no. 9, pp. 14–17, September 2017.

[13] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "To blockchain or not to blockchain: That is the question," IT Professional, vol. 20, no. 2, pp. 62–74, March 2018.

[14] P. A. Laplante and B. Amaba, "Introducing the Internet of Things department," IT Professional, vol. 20, no. 1, pp. 15–18, January 2018.

[15] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy," IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, January 2018.

Journal of Engineering Sciences