International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

SLIDING WINDOW BLOCKCHAIN ARCHITECTURE FOR INTERNET OF THINGS

Abhilash Movva[1], Voruganti Naresh Kumar[2]

[1]*B. Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India,*
[2]*Associate Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India*

Abstract - The Internet of Things (IoT) refers to the concept of connecting non-traditional computers and resources to the Internet, incorporating basic computing and communication technologies into physical objects for daily use. However, IoT faces challenges in terms of security and confidentiality, as current security mechanisms often lack critical specifications due to the limitations of CPU, memory, and energy resources in IoT devices. Additionally, centralized security architectures are not suitable for IoT, as they create a single point of attack and can be costly to defend against targeted attacks on centralized infrastructure. To address these challenges, there is a need to decentralize the IoT security architecture while considering resource constraints. we propose a blockchain sliding window (SWBC) architecture specifically designed for IoT applications, which modifies the conventional blockchain approach. The SWBC architecture utilizes previous blocks in proof of work to shape the next hash block, creating a sliding window mechanism.

Key Words: Blockchain, Python, Security, Machine learning, Internet of Things

1. INTRODUCTION

Blockchain is a distributed ledger technology used for recording transactions between multiple parties. Unlike traditional relational databases, blockchain allows for adding new entries to the end of the ledger and does not allow users to modify data once it is recorded. Consensus algorithms are used to verify the addition of new blocks to the chain, making it difficult for attackers to manipulate data. However, traditional blockchain methods face challenges in terms of computational complexity and scalability, making them less suitable for real-time IoT applications. In this paper, we propose a new architecture for blockchain in IoT environments, specifically focusing on smart home applications. The proposed architecture aims to enhance security and reduce overhead in IoT data streams.

1.1 Blockchain Technology:

The blockchain is the process of recording the transactions in the business network where these transactions are tracked and immutable.
Once the transactions are recorded in the ledger, they cannot be tampered. If there is an error in the transaction a new transaction is added to eliminate the error and the process is visible. The blocks in the blockchain are connected and form a chain like network where each block contains the information. The records are confidential, and they are shared within the network for those who have the access.

2. LITERATURE SURVEY

The Internet of Things (IoT) is growing rapidly but faces privacy and security challenges. Traditional approaches are not suitable for IoT due to its decentralized nature and resource limitations. Blockchain technology has been used for security and privacy in similar networks, but it is computationally expensive for IoT. This position paper proposes a lightweight architecture for IoT based on blockchain, eliminating overhead while maintaining security and privacy. The architecture is hierarchical, with smart homes, overlay networks, and cloud storages coordinating data transactions with blockchain. Distributed trust methods ensure a decentralized topology. Evaluation shows the effectiveness of the proposed architecture for IoT security and privacy.

3. PROPOSED METHODOLOGY

The proposes a blockchain-based solution for securing IoT devices by utilizing decentralized data storage. To overcome the computational overhead of verifying all nodes in a blockchain, we introduced a sliding window technique to store recent transaction blocks. Additionally, they suggest monitoring data in time intervals and avoiding duplicate data to save energy.

4. RESULTS

Fig -1: Packet transfer and then select window.

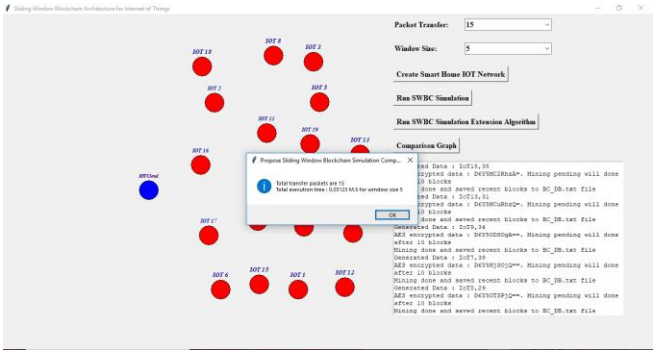

Fig -2: Sending packets.

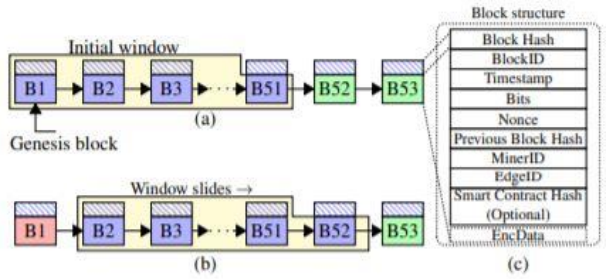

Fig -3: Architecture of the proposed model

5. CONCLUSION

Resources such as computer power, energy sources and memory are limited by IOT devices. The standard protection algorithms for IoT are therefore not feasible. We introduced a sliding window blockchain that meets the requirements of an IoT network with restricted resources by decreasing the overhead memory and restricting the overhead of the computation. The overhead memory is minimized by only keeping a small part of the lock chain in the private cloud, as specified by` the IoT's sliding fenster size and the entire blockchain. Computer overhead is reduced by the complexity level of 1 to 5 and the removal of the Merkle tree. The protection is improved by using the properties of n blocks of the sliding window to produce the block hash. Unable the previous (n−1) blocks and data on the window size are obtained, a false miner can mine a block. We have found the following from the experimental results: I PoW calculation time increases exponentially for each difficulty level. (ii) With the increase of the number of miners in the group, the total block addition time increases. (iii) The hash calculation time increases linearly as the window size increases. (iv) A random complexity selection for each block in a blockchain decreases the overall addition time of the block.

6. ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper entitled “SLIDING WINDOW BLOCKCHAIN ARCHITECTURE FOR INTERNET OF THINGS”, which provided good facilities and support to accomplish our work. We sincerely thank our Chairman, Director, Deans, Head of the Department, Department of Computer Science and Engineering, Guide and Teaching and Non-Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

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.