IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203030 |

A Novel Approach to Securing IoT Data: Utilizing Polygon Blockchain for Data Integrity

Ajinkya Kotwal[1], Omkar Satpute[2], Prem Khandelwal[3], Rishikesh Mahajan[4], Pradnya Kasture[5]

U.G. Student, Department of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India[1,2,3,4]

Project Guide, Department of Computer Engineer, RMD Sinhgad School of Engineering, Maharashtra, India[5]

ABSTRACT: Traditional methods often rely on trusted Third-Party Auditors to execute auditing tasks and the burden of users during the verification phase can be decreased. For example, in Wise Information Technology of 120, massive electronic health records are collected by wearable devices and then stored. To collect, process, store and analyze these large-scale IoT data securely has therefore become one of the most important issues for further applications of Internet of Things. Traditional distributed database systems cannot fully satisfy the requirements of data management in the IoT devices environment and there was authority of a single entity over data generated. Achieving data integrity verification for large- scale lot data safely and efficiently has become one of the hot topics with further applications of Internet of Things. Traditional data integrity verification methods rely on trusted Third-Party Auditors.

KEYWORDS: API, Consensus Algorithm, Gas Fee**,** Hash, Merkle Tree, Smart Contract, Polygon.

I. INTRODUCTION

IoT devices have no identification number so data can be tampered easily so we can remove TPA's and Introduction of Blockchain for data integrity with less power consumption in an efficient manner reduces many severe data issues. The Blockchain technology has shown its revolution in the field of information registration and distribution which removes the requirement for an intermediary expert to enable the digital relationships. With the help of Blockchain technology, basically, it is possible to impact a varied range of processes and techniques. It eliminates the need of trusted third parties in the transactions. In a blockchain, transactions are verified by distributed nodes, and anyone can join or leave the network as they please without disrupting the network's ability to form consensus on transactions. The proposed approach can ensure the integrity of IoT data with minimal overhead and high efficiency and power consumption. This paper provides insights into how blockchain can be applied to address the challenges of securing IoT data and highlights the potential of using Polygon blockchain as a reliable and scalable solution. Blockchain technology has emerged as a promising solution for ensuring the security and integrity of data.

II. MOTIVATION

Traditional IoT data security solutions involved TPA (Third Party Auditors) to ensure the security of their IOT Data, which made it susceptible to the attacks. However, with the introduction of the Blockchain, we tend to eliminate these auditors and propose a system which would also ensure data integrity. The architecture of the Blockchain is tailor-made for our use case as the data once entered in the Blockchain cannot be tampered, thus providing a coveted solution to the security of the IOT Data. The use of blockchain technology for ensuring the integrity of IoT data is a promising solution due to its characteristics of decentralization, transparency, and immutability. However, traditional blockchains, such as Bitcoin and Ethereum, have limitations in terms of scalability and high transaction fees. These limitations make it difficult to use traditional blockchains for IoT applications, which generate a large amount of data and require high-speed data processing.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203030 |

III. OBJECTIVE

To use blockchain, for ensuring IoT data integrity is to create a secure, decentralized, and tamper-proof system for storing and verifying IoT data. By leveraging the unique features of blockchain, such as its distributed architecture, immutability, and transparency, organizations can ensure the integrity and accuracy of their IoT data. By using cryptographic algorithms and distributed consensus mechanisms, blockchain ensures that the data stored on the network is highly secure and resistant to tampering or manipulation. Blockchain's decentralized architecture ensures that data is stored across multiple nodes in a network, making it highly resistant to hacking or attacks on any single point of failure.Once data is stored on the blockchain, it cannot be altered or deleted, ensuring the integrity and accuracy of the data over time. To use Polygon Blockchain as a medium to store user's data. By using Blockchain technology, we intend to eliminate Third Party Auditors (TPA). Using Polygon Blockchain which will significantly reduce power consumption of the system.

IV. RELATED WORK

Haiyan wang, jiaweizhang, "Blockchain Based Data Integrity Verification for large-scale IoT data", IEEE Access, vol.10, pp.120168-120180, 2022. Blockchain based data integrity technology can avoid the trust problem of TPAs. Complex data types were not implemented. [1]

Anmarriadh, Asma AbusamahVolume, "Data integrity time optimization of a blockchain lot smart home network" 2021 | Article ID 4401809 | https://doi.org/10.1155/2021/4401809. Provide high security against possible data security threat in terms of data integrity verification check. Relationship between the number of transactions,consensus algorithm and hash function [2]

Gaopeng, Yuling, Qiuwei," Blockchain based cloud data integrity verification scheme with high efficiency". Volume 2021 | Article ID 9921209 | https://doi.org/10.1155/2021/99212. Improve the transparency and the security of the scheme. Insufficient computing power of users.[3]

Jingting, chunxiang, jining,,"Identity-based public auditing for cloud storage systems against malicious auditors' Volume 2020 | Article ID 9787821209 | https://doi.org/10.1155/2021/99212. Effectively resist malicious auditors' unpredictability and traceability. Balance between storage overhead and communication.[4]

Poornima M. Chanal, Mahabaleshwar S. Kakkasager "Blockchain based personal health records sharing scheme with data integrity variable."Volume 2021 | Article ID 9921209 | https://doi.org/10.1155/2021/99212. Achieve fine grained access control without relying on any third party. Performing file update, delete operations according to the patient's requirement. [5]

Vasimla Khan, Abdula Rahim, "Volume "Data integrity time optimization of a blockchain lot smart home network" 2021 | Article ID 4401809 | https://doi.org/10.1155/2021/4401809. Provide high security against possible data security threat in terms of data integrity verification check. Relationship between the number of transactions,consensus algorithm and hash function [6]

Jianbin Wu, Manish Bhardwaj, Aditi Sharma, and Piyush Singhal,"Blockchain-Based Data Audit Mechanism for Integrity over Big Data Environments", 2022 | Article ID 4401809 | https://doi.org/10.11554401809. Data integrity proof metadata generation and integrity audit speed are high, which can meet the requirements of data heterogeneity.[7]

Jubin Chanda, Omkar Pandit, "The generation of the proof metadata in the scheme of this paper needs to be realized based on generating a random sequence". IBPA scheme, which can effectively resist malicious auditors. This approach achieves unpredictability and traceability. Resistance to malicious auditors increases the computational overhead on the user side. In future work, we will further explore efficient public auditing mechanisms[8]

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203030 |

Aditi Sharma, and Piyush Singhal ,"Integrity over Big Data Environments" 2019 | Article ID 4401809 | https://doi.org/10.1155/2401809., Data integrity proof metadata generation and integrity audit speed are high, which can meet the requirements of data heterogeneity.[9]

Dahu Wang, Neeraj Kumar, "Enhancing the performance of the blockchain validation process is a challenging and crucial task." Major focus of the paper is to enhance the perception of security issues of data integrity methods based on blockchain technology the enhancing performance of the blockchain validation process is a challenging and crucial task. [10]

V. CONCLUSION

Above proposed system can ensure integrity of large IoT data using blockchain. An energy efficient method was used to solve the problem of power consumption. We can use machine learning technology for further reduction of data.

REFERENCES

1. Blockchain Based Data Integrity Verification for Large-Scale IoT Data. F. Xiao, G. Ge, L. Sun, and R. Wang, ''An energy-efficient data gathering method based on compressive sensing for pervasive sensor networks,' Pervasive Mobile Comput., vol. 41, pp. 343–353, Oct. 2020.
2. M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' Future Gener. Computer. Syst., vol. 82, pp. 395–411, May 2021.
3. Y. Deswarte, J.-J. Quisquater, and A. Saïdane, ''Remote integrity checking,'' in Proc. 6th Work. Conf. Integrity Internal Control Inf. Syst. (IICIS), 2004, pp. 1–11.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ''Provable data possession at untrusted stores,'' in Proc. CCS, 2007, pp. 598–610.
5. C. Wang, Q. Wang, K. Ren, and W. Lou, ''Ensuring data storage security in cloud computing,'' in Proc. IEEE 17th Int. Workshop Qual. Service (IWQoS), Jul. 2009, pp. 1–9.
6. Juels and B. S. Kaliski, Jr., ''PORs: Proofs of retrievability for large files,'' in Proc. CCS, 2007, pp. 584–597.
7. Wang, Q. Wang, K. Ren, and W. Lou, ''Privacy-preserving public auditing for data storage security in cloud computing,'' in Proc. IEEE, INFOCOM, Mar. 2010, pp. 1–9.
8. L. Zhang, Z. Zhang, W. Wang, Z. Jin, Y. Su, and H. Chen, "Research on a covert communication model realize by using smart contracts in blockchain environment," IEEE Systems Journal, 2021.
9. S. M. Alrubei, E. A. Ball, J. M. Rigelsford, and C. A. Willis, "Latency and performance analyses of real- world wireless IoT-blockchain 2020.
10. L. V. Kiong, Metaverse Made Easy: A Beginner's Guide to the Metaverse: Everything you need to know about Metaverse, NFT and GameFi. Liew VoonKiong, 2022.
11. O. L. Mokalusi, R. B. Kuriakose, "A Comparison of Transaction Fees for Various Data Types and Data Sizes of Blockchain Smart Contracts on a Selection of Blockchain Platforms",https://doi.org/10.1007/978-981-19-5221-0_67 2021.
12. Haiyan wang, jiaweizhang, "Blockchain Based Data Integrity Verification for large-scale Iot data", *IEEE Access*, vol.10, pp.120168-120180, 2022. Blockchain based data integrity technology can successfully avoid the trust problem of TPAs. Complex data types were not implemented.
13. Anmarriadh, Asma Abusamah Volume, "Data integrity time optimization of a blockchain lot smart home network" 2021 | Article ID 4401809 | https://doi.org/10.1155/2021/4401809.
14. Gaopeng, Yuling, Qiuwei," Blockchain based cloud data integrity verification scheme with high efficiency". Volume 2021 | Article ID 9921209 | https://doi.org/10.1155/2021/99212. Improve the transparency and the security of the scheme. Insufficient computing power of users.
15. Jingting, chunxiang, jining, "Identity-based public auditing for cloud storage systems against malicious auditors" Volume 2020 | Article ID 9787821209 | https://doi.org/10.1155/2021/99212. Effectively resist malicious auditors' unpredictability and traceability. Balance between storage overhead and communication.
16. Poornima M. Chanal, Mahabaleshwar S. Kakkasager, "Blockchain based personal health records sharing scheme with data integrity variable."Volume 2021 | Article ID 9921209 | https://doi.org/10.1155/2021/99212. Achieve fine grained access control without relying on any third party. Performing file update, delete operations according to the patient's requirement.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details