JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Novel Approach to Securing IoT Data: UtilizingPolygon Blockchain for Data Integrity

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

Department of Computer Engineering,
R.M.D Sinhgad School of Engineering, Pune, India.

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.***

1. 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.

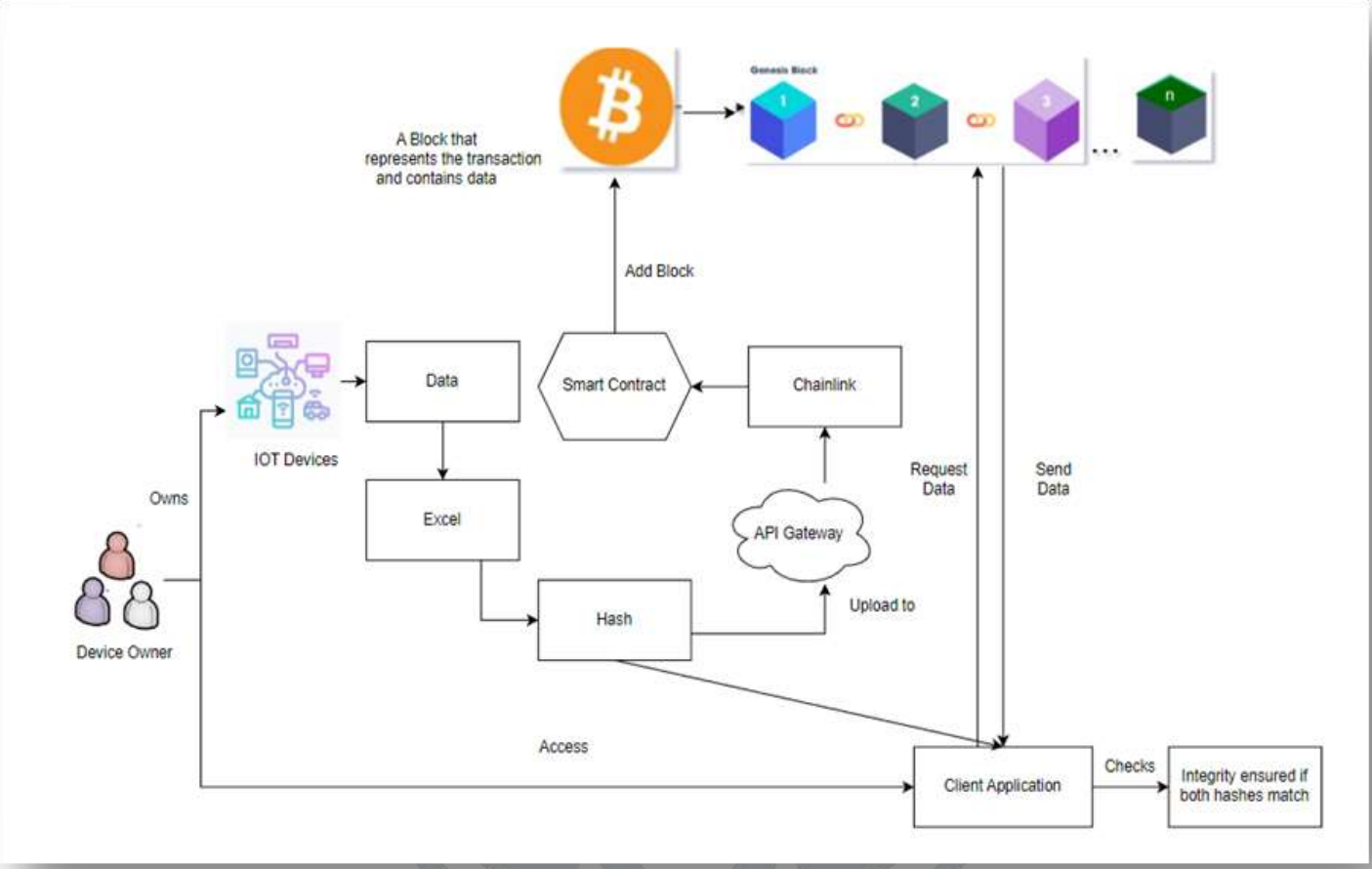
The main objectives of this system are:

1. 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 resistantto tampering or manipulation.
2. To the 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.

3. 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.

2. SYSTEM MODEL DIAGRAM :



(Figure **1:** System Model Diagram)

3. Methodology:

The methodology for ensuring IoT data integrity using blockchain involves a combination of defining the data, smart contracts, selecting the blockchain platform, developing the gateway, implementing the consensus algorithm, storing the verified data, and building the user interface. By following this methodology, organizations can create a secure, decentralized, and tamper-proof system for storing and verifying IoT data.

1. Identify the Data: The first step is to identify the data that needs to be stored and verified on the blockchain. This may includesensor data, device logs, or any other type of data generated by IoT devices.
2. Gather and Store the Data: The data collected from the IOT devices should be stored in the determined format.
3. Hashing the Data: Once the data is collected and stored in the format determined, the next step is to calculate the hash valueof the whole of the data. The hash value calculated is one-way and is in unreadable format.
4. Define the API Gateway: The API gateway is responsible for communication of the Chainlink with the original data that is stored in the system. The API gateway will consist of the hash value of the data and would be responsible for communication
5. Running the local Chainlink node: The Chainlink node need to be configured so as to run the required job and make theconnection between Blockchain and the data to be sent
6. Implement the Consensus Algorithm: The consensus algorithm is used to ensure that all nodes on the blockchain network

agree on the validity of transactions. This is necessary to prevent double-spending and other fraudulent activities.

7. Store the Verified Data: Once the data has been verified and validated, it is stored in a decentralized and distributed manneracross the network. This ensures that the data is immutable and cannot be altered or deleted by any single entity.
8. Build the User Interface: Finally, a user interface is developed that allows users to interact with the blockchain network, viewdata, and manage transactions.

4. LITERATURE SURVEY:

..

Sr.No	Name of Jornal/ Year of Published	Paper Title	Author Name	Advantages	Research Gap
1	IEEE access published on November 22,2019	Blockchain Based Data Integrity Verification for Large-Scale IOT Data	1.Haiyan Wang 2.Jiawei Zhang	Blockchain based data integrity technology can successfully avoid the trust problem of TPAs(trusted Third party Auditors)	Complex data types were not implemented
2.	Hindawi published on 9 Nov 2021	Data Integrity time Optimization a Blockchain IOT Smart Home Network Using Different Consensus and Hash Algorithm	1. Ammnar Riadh Kairaldeen 2. Nor Fadzilah Abdullah 3.Asma Abusamah	Provide high security against possible data security threads in terms of Data Integrity verification check that the purpose modified Merkle Hash Tree consensus Algorithm used in the blockchain has a very efficient execution time	Relationship between the number of transaction consensus algorithm and Hash Function was not established
3	Hindawi published on 29 April 2021	Blockchain-Based cloud data integrity verification scheme with high Efficiency	1.Gaopeng Xie 2.Yuling Liu 3.Qiuwei yang	Improve the transparency and the security of this scheme verification process	Insufficient computing power of users
4	ACM published on march 2019	Identity based public auditing for cloud storage systems against malicious auditors via blockchain	1.JingtIng XUE1 2.Chunxiang XU1 3. Jining ZHAO 4.Jianfeng MA3	Effectively resist malicious auditors unpredictability and traceability of challenge messages by relying on the nonces of the blockchain	Balance between storage overhead and communication overhead should be careful handled
5	IEEE access published on 12 August 2019	Blockchain Based personal Health Records sharing scheme with data integrity	1. Shangping wang 2. Dan Zhang	Achieve fine grained access control without relying on any third party.	Performing file update and file delete operations according to the patients the requirements during the personal health record management.

5. RESULTS AND CONCLUSION:

Result

To achieve our goal, we developed a decentralized auditing platform on the Polygon blockchain. The platform utilizes smart contracts to store and verify financial transactions securely and transparently. We conducted extensive evaluation of the system, considering factors such as transaction speed, scalability, and energy consumption.

The results of our experimental implementation demonstrated several key findings. Firstly, the use of the Polygon blockchain significantly improved the transaction speed compared to traditional auditing methods. The platform was able toprocess a large volume of transactions quickly and efficiently, reducing the overall auditing time.

Polygon:
Annual carbon footprint: 50.13 tCO2e
Marginal electricity consumption per transaction: 0.608776 Ws per Tx

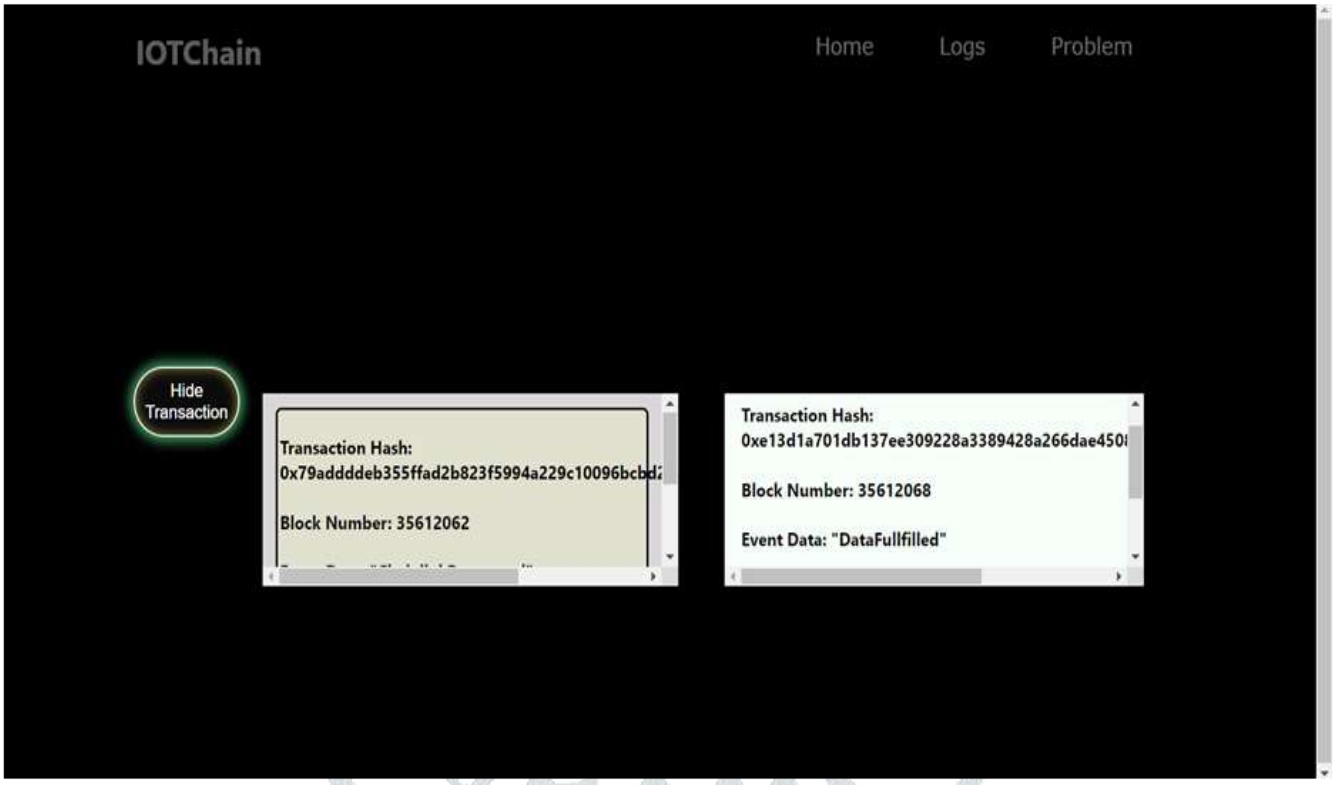
Ethereum:
Annual electricity consumption: Annual carbon footprint: 35.4 MTCO2e
Marginal electricity consumption per transaction: 124.34 kg CO2 per transaction

Metrics	**Polygon**	**Ethereum**
Average transaction speed	65,000 TPS	15 TPS
Average transaction cost	$0.00001	$0.005
Annual electricity consumption	109,213.48 kWh	75 TWh

Moreover, the scalability of the Polygon blockchain allowed for seamless integration with existing auditing systems, ensuring compatibility and ease of adoption. The smart contracts executed flawlessly, providing an immutable and transparent ledger for auditing purposes.

Furthermore, we analyzed the energy consumption of the Polygon blockchain and found it to be considerably lower compared to the Ethereum blockchain. This highlights the sustainability aspect of our solution, as it reduces the carbon footprint associated with auditing processes.

(Screenshot 1)



(Screenshot 2)

(Screenshot 3)

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.

In conclusion, our project successfully demonstrated the potential of utilizing the Polygon blockchain to eliminate the need for third-party auditors in the auditing process. The technical results revealed the advantages of the Polygon blockchain in terms of transaction speed, scalability, and energy efficiency.

By leveraging blockchain technology, specifically the Polygon blockchain, we have achieved a more secure, transparent, and sustainable auditing process. Our solution not only reduces speed with traditional auditors but also enhances data integrity and trust.

Moving forward, further research and development in this field could explore additional functionalities and address any challenges that arise. The adoption of blockchain technology in auditing has the potential to transform the financial industry by providing a decentralized, efficient, and trustworthy approach to auditing processes.

Overall, our project highlights the significant impact that blockchain technology can have on enhancing data privacy, integrity, and efficiency in AI systems.

6. ACKNOWLEDGMENTS:

It gives us great pleasure in presenting the preliminary project report on

"A Novel Approach to Securing IoT Data: Utilizing Polygon Blockchain forData Integrity".

I would like to take this opportunity to thank my internal guide ***Prof. Pradnya Kasture*** *for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.*

I am also grateful to ***Prof. Vina M. Lomte****, Head of Computer Engineering Department, RMD Sinhgad School of Engineering, for her indispensable support, suggestions.*

Ajinkya Kotwal
Omkar Satpute
Prem Khandelwal
Rishikesh Mahajan

(BE Computer Engg.)

7. 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 atuntrusted 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 17thInt. Workshop Qual. Service (IWQoS), Jul. 2009, pp. 1–9.
6. A. Juels and B. S. Kaliski, Jr., ‘‘PORs: Proofs of retrievability for large files,’’ in Proc. CCS, 2007, pp. 584–597.
7. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-preserving public auditing for data storage security in cloudcomputing,’’ 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 realizedby 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-worldwireless IoT-blockchain 2021.
10. L. V. Kiong, Metaverse Made Easy: A Beginner’s Guide to the Metaverse: Everything you need to know aboutMetaverse, NFT and GameFi. Liew Voon Kiong, 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, jiawei zhang, "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. Anmar riadh, 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

8. AUTHORS & MENTOR:

Mr. Ajinkya Kotwal
RMD School of Engineering,
Warje, Pune-58
(Computer
Engineering)

.

Mr. Omkar Satpute
RMD School of
EngineeringWarje,
Pune-58
(Computer Engineering)

Ms. Rishikesh Mahajan
RMD School of
Engineering,
Warje, Pune-58
(Computer
Engineering)

.

Mr. Prem Khandelwal
RMD School of Engineering,
Warje, Pune-58
(Computer
Engineering)

.

Prof. Pradnya Kasture
Project Guide
Department of
ComputerWarje,
Pune-58

.