iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52389

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Securing Smart Devices on Blockchain

Mrs. Kamala V[1], Arun D[2], Aswin Raj R[3], Gokulakrishnan S[4], Harshil S[5]
[1]*Assistant professor,* [2, 3, 4, 5]*UG Scholar, Department of Computer Science Engineering, KGiSL Institute of Technology, Saravanampatti, Coimbatore*

Abstract: ***A smart device uses information technology to integrate and manage physical, social, and business infrastructures data in order to provide better services to its dwellers while ensuring efficient and optimal utilization of available resources. With the proliferation of technologies such as Internet of Things (IoT), cloud computing, and interconnected networks, for securing smart devices, they can deliver a lot of innovative solutions. Despite a number of potential benefits, digital disruption poses many challenges related to information security and privacy. Here, this project proposes a security framework that integrates the blockchain technology with smart devices to provide security to smart devices.***
Keywords: Blockchain, Smart Contracts, Ethereum, Smart Device, IOT, Security mobility.

I. INTRODUCTION

The project aims to prevent security hacks on smart devices by using blockchain technology. The blockchain ensures that only registered or access-granted users' data is securely stored, and the data cannot be tampered with, such as adding new fingerprints or modifying it. Smart contracts are written and deployed into the blockchain, which act as the rules or functionality of the devices, and once deployed, they cannot be modified. Blockchain has several properties that make it difficult to modify data, and data can only be modified by "Data Miners" who solve a resource-consuming cryptographic puzzle called Proof of Work (POW). However, this may not be a 100% correct solution as blockchain is a relatively recent technology, and it can only be implemented through cryptocurrency. This means that users must have cryptocurrency to access the device, which may not be feasible for all users. Nevertheless, the project is attempting to implement another way of providing a solution using blockchain technology. In summary, the proposed security framework integrates blockchain technology with smart devices to ensure that only authorized users can access and modify the data. The use of blockchain ensures that the data is secure and tamper-proof, and smart contracts ensure that the device functions according to the rules set forth in the blockchain. While there may be limitations to implementing blockchain technology due to its recent development and reliance on cryptocurrency, this project demonstrates the potential for using blockchain technology to secure smart devices.

II. LITERATURE SURVEY

1) *Sunny King:* In a blockchain, not everyone can modify the data as specific nodes called miners are responsible for mining blocks. To mine a block, miners solve complex cryptographic puzzles with rewards for solving them. To maintain the security property of Nakamoto's Bitcoin, a prime chain is linked to the block hash. The prime chain acts as an adjustable-difficulty proof-of-work in a Bitcoin-like cryptocurrency. The solving of the puzzle requires finding a 64-digit hexadecimal number, which makes it very difficult to guess. This time-consuming process results in more time required for modifying IoT data, providing improved security compared to Nakamoto's original Proof of Work technique.
2) *Ali Dorri, Salil S. Kanhere, Raja Jurdak:* Integrating Blockchain into IoT poses significant challenges, including resource-intensive proof-of-work computations, slow transaction confirmation times, and limited scalability due to network-wide broadcasting. To address these challenges, the Diffie-Hellman algorithm can be employed. Devices can establish secure communication by generating shared keys based on a generalized side. While this approach offers consistent performance overhead, its scalability is dependent on the number of clusters involved. Although there are no major constraints, it may still fall short of meeting the desired processing speed for transactions.
3) *Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, Kerem Varıcı, Ingrid Verbauwhede:* In this approach, secure communication is achieved by using a shared key for all transactions. Lightweight hashing algorithms are utilized to detect any modifications in transaction content during transmission. All transactions involving the smart home are stored in a local private blockchain. When attempting to guess a number, the emphasis is on utilizing the region and computational power efficiently. The hash function employed adheres to the standard security requirements, providing a 2n/2 collision resistance and preimage resistance. Even a minor change in the data will result in a completely different and unpredictable hash value, making it difficult to compute the hashed number quickly. While this lightweight technique may not possess the same strength as well-known alternatives like SHA hashing, it is implemented to ensure uniqueness and provide an additional layer of security.

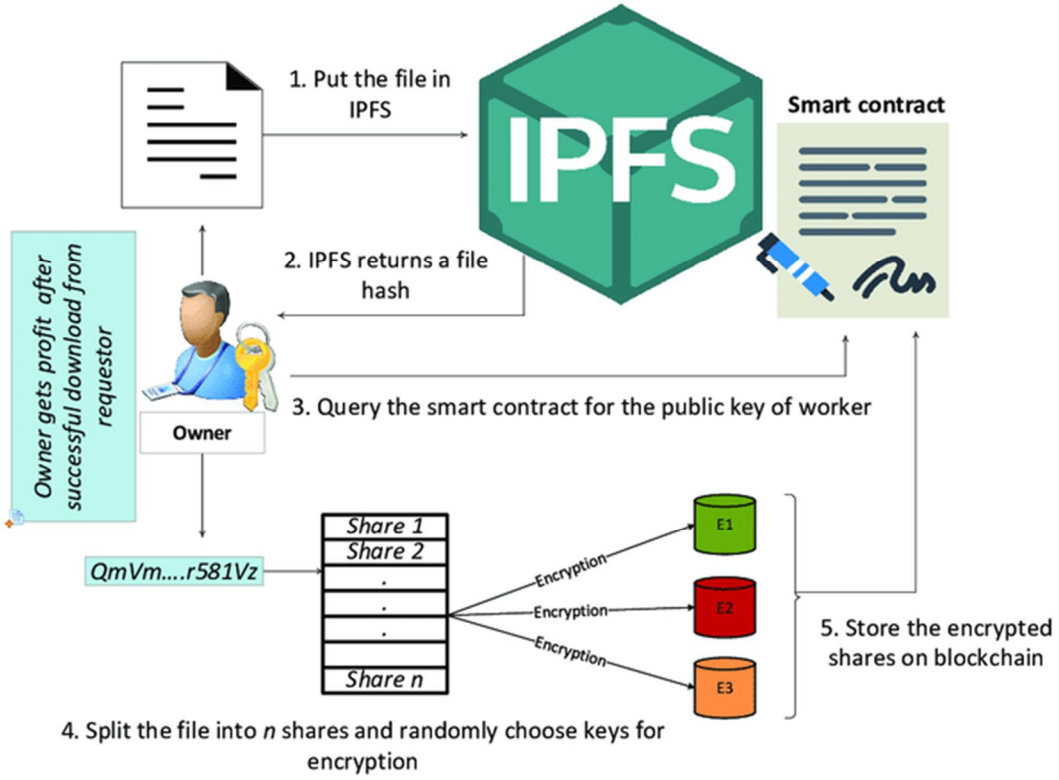


Figure.1: IPFS working diagram

Figure.2: Proposed Methodology

III. PROPOSED SYSTEM

The proposed system aims at addressing the high cost of transaction fees associated with hosting smart devices on a blockchain by leveraging the Inter-Planetary File System (IPFS) as a distributed file system. IPFS offers a cost-effective solution by decentralizing data storage and sharing. This approach not only reduces expenses but also enhances security by fragmenting data into multiple blocks, making it challenging for unauthorized individuals to manipulate or access the information. Additionally, IPFS employs content-addressing to ensure data immutability, assigning a unique identifier to each file within a global namespace. This system, combined with the utilization of SHA-256 cryptographic hashing, guarantees the confidentiality and integrity of the stored data. By incorporating IPFS into IoT data storage, we can achieve an efficient and secure solution that surpasses traditional blockchain-based methods.

Here are some advantages of the proposed system:

1) *Immutability:* Once data is added to the blockchain. It cannot be changed or deleted without the consensus of the network. This ensures that data is tamper-proof and provides high trust.
2) *Increased Efficiency:* Blockchain eliminates the need for intermediaries, which can help reduce transaction cost and processing times. Additionally, smart contracts can automate many processes, further increasing efficiency.
3) *Decentralization:* Blockchain technology enables a decentralized network, which means that no single entity controls the system. This provides increased security and resilience, as well as more democratic decision-making.
4) *Content Addressing:* Establish Each file in IPFS is given a unique content-addressed hash that allows the system to easily locate and retrieve the file from any node on the network.
5) *Distributed File System:* IPFS creates a global, decentralized file system by connecting all computing devices to a peer-to-peer network.

IV. METHODOLOGY

The implementation of securing smart devices using blockchain system involves several key steps and methodologies to ensure its successful deployment and operation. Here is a suggested methodology for developing securing smart devices using blockchain system:

1) *Requirement Gathering:* Identify stakeholders and conduct interviews to gather their input and insights, followed by organizing workshops to collaborate and refine the requirements for implementing IPFS in the smart device hosting system.
2) *Design:* Utilize an iterative and collaborative approach, involving stakeholders and designers in brainstorming sessions and prototyping to create a user-centered and scalable design for integrating IPFS into the smart device hosting system.
3) *Deployment and Connectivity:* Establish a secure and scalable network infrastructure for seamless communication between smart devices and the IPFS network, ensuring reliable connectivity and efficient deployment of the system across various devices and platforms.
4) *Data Collection and Processing:* Implement efficient mechanisms for collecting data from smart devices, ensuring data integrity and security, and employ robust processing techniques to analyze and derive insights from the collected data, enabling informed decision-making and enhancing system performance.
5) *User Applications and Interfaces:* Design intuitive and user-friendly applications and interfaces that provide seamless interaction between users and the system, offering easy access to functionalities, real-time monitoring, and control of smart devices, ensuring a positive user experience and maximizing user adoption.
6) *System Integration and Testing:* Conduct thorough integration testing to ensure seamless communication and compatibility between different components and modules of the system. Perform rigorous testing, including functional testing, performance testing, and security testing, to identify and resolve any issues or bugs, ensuring the system operates efficiently and reliably.
7) *Deployment and Maintenance:* Follow a systematic deployment process, including installation, configuration, and monitoring of the system in the production environment. Establish proactive maintenance procedures, including regular updates, backups, and security patches, to ensure the system's stability, reliability, and optimal performance throughout its lifecycle.

V. ARCHITECTURE DIAGRAM

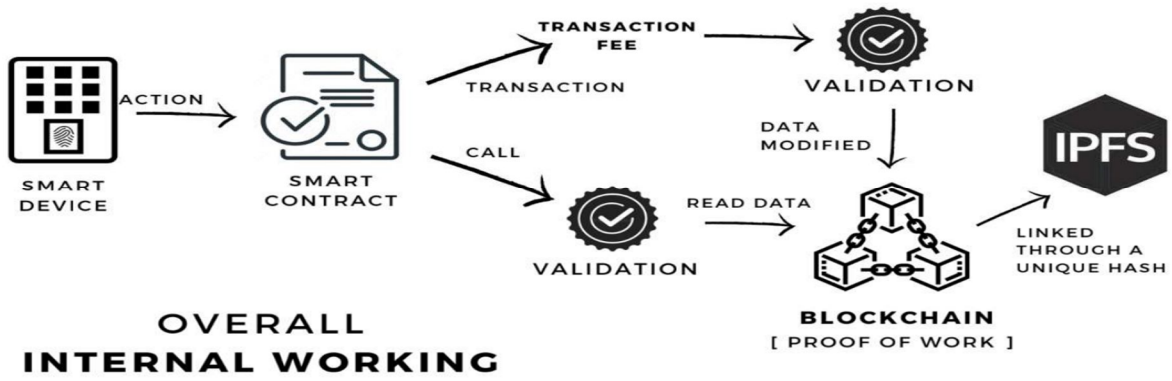
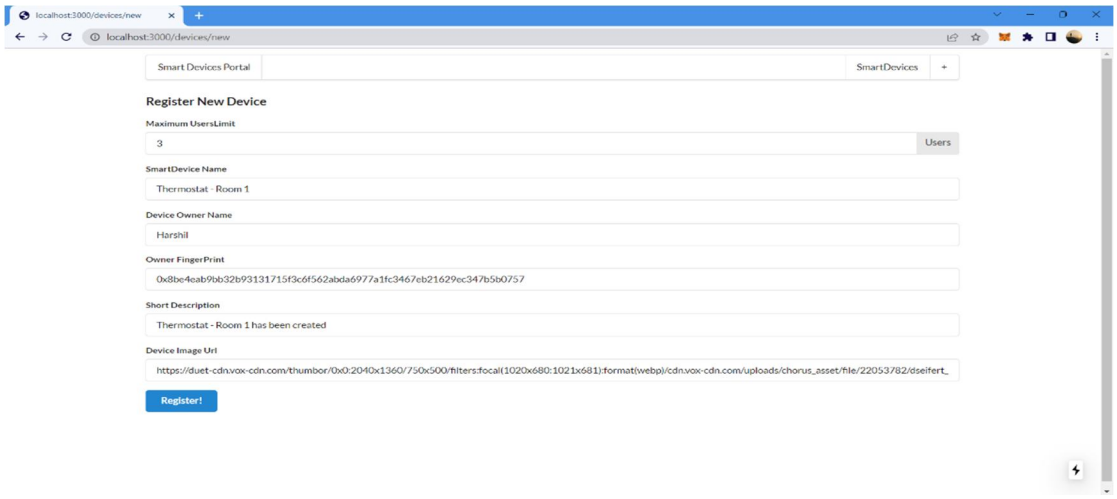
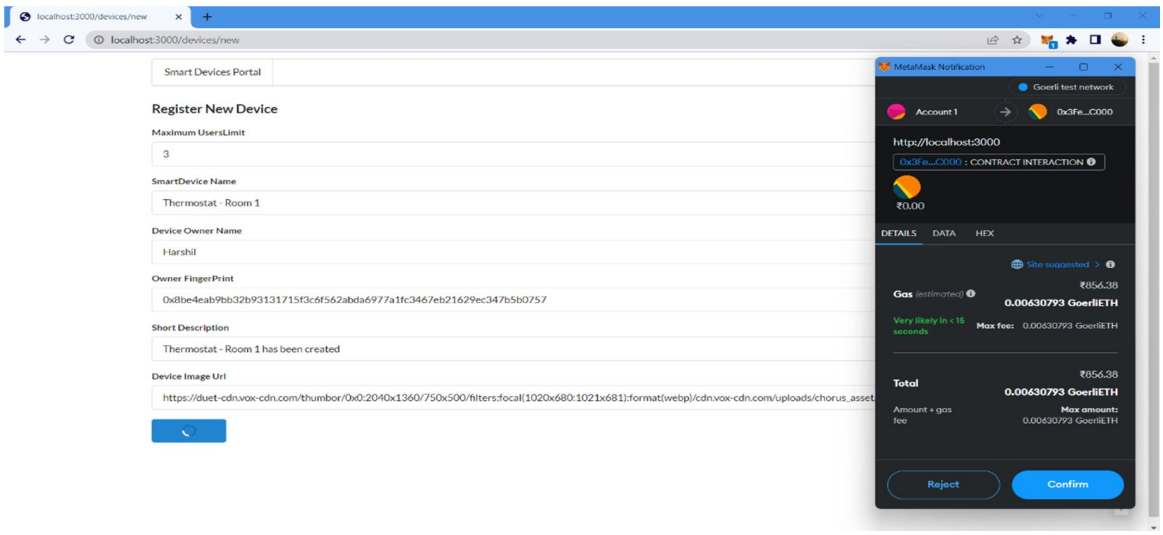


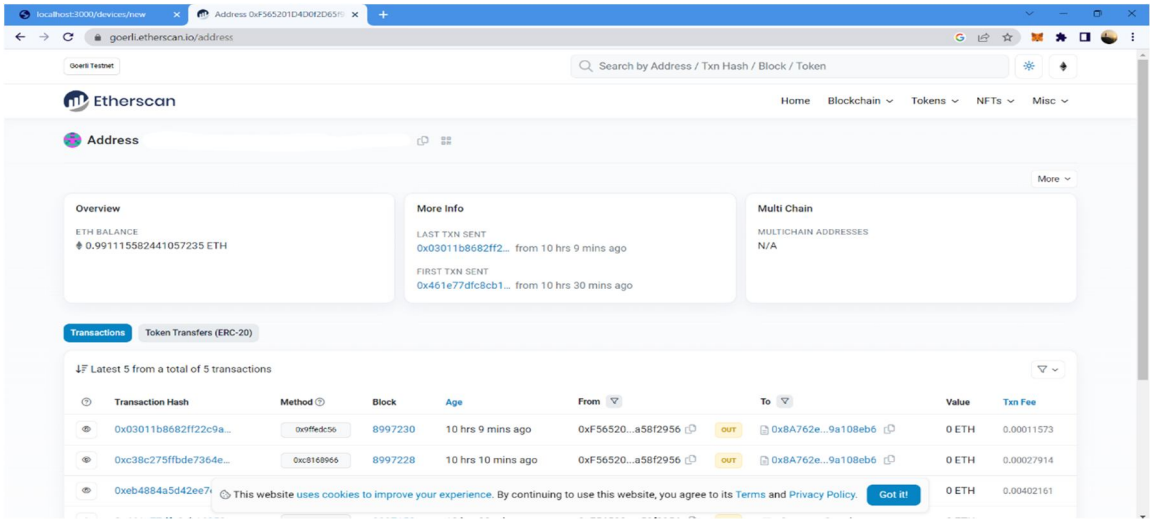
Figure.3: Architecture Diagram

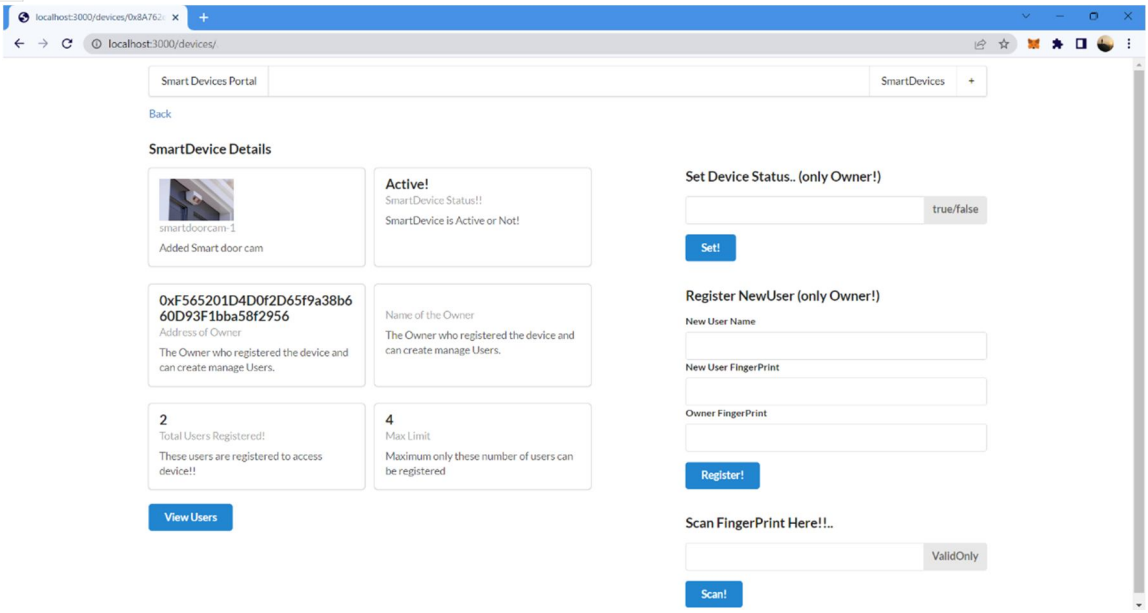
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

VI. RESULT









VII. FUTURE SCOPE

The future scope for securing smart devices on blockchain systems is promising, as the adoption of blockchain technologies continues to grow and urbanization increases. Here are some potential areas of development and expansion for securing smart devices using blockchain systems:

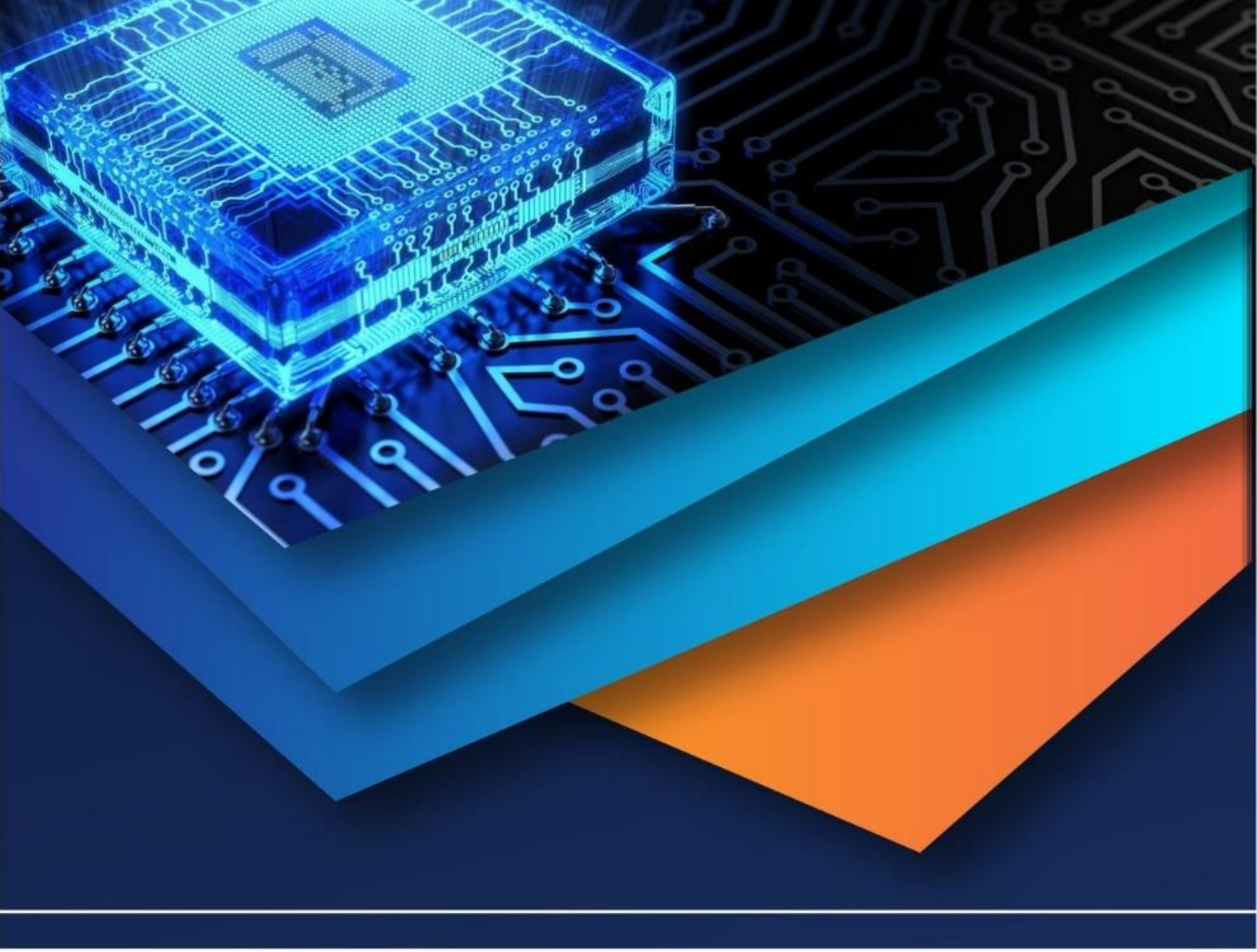
1) *Integration with Machine Learning:* Enhance the system by incorporating machine learning algorithms to analyze and predict patterns in smart device data. This can enable proactive decision-making, anomaly detection, and predictive maintenance.
2) *Enhanced Security Measures:* Implement advanced security measures such as multi-factor authentication, encryption, and biometric verification to strengthen the protection of smart devices and user data. Explore the integration of decentralized identity solutions for improved user authentication.
3) *Scalability and Interoperability:* Focus on enhancing the system's scalability to accommodate a larger number of smart devices and ensure interoperability with various IoT platforms. This will enable seamless integration and communication between different devices and systems.
4) *Blockchain Interoperability:* Investigate the possibility of integrating with other blockchain networks or protocols to enhance compatibility and facilitate data sharing across multiple blockchain systems. This can enable broader connectivity and collaboration in the decentralized ecosystem.
5) *User-Friendly Interfaces:* Continuously improve the user interfaces of the system, both for device management and data access, to ensure a seamless and intuitive user experience. Implement interactive visualizations and customizable dashboards to provide users with meaningful insights from the collected data.

VIII. CONCLUSION

In conclusion, this project serves as a practical demonstration of how blockchain technology can be utilized to enhance the security of smart devices. By developing a website and deploying it on the Goerli test network, which mirrors the Ethereum network, we have provided an innovative solution for safeguarding the privacy of these devices. While we acknowledge that there may be other approaches available, this project offers a fresh perspective on addressing the challenges associated with securing sensitive data. Looking ahead, our future endeavors involve expanding the project's scope to encompass a wider range of smart devices and seamlessly integrating them into their respective environments. By doing so, we aim to create a comprehensive and holistic solution that can effectively protect interconnected devices in various settings. The experience gained throughout this project has been invaluable, deepening our understanding of blockchain technology and its potential applications. Overall, this project has been an exciting journey, motivating us to explore new frontiers in device security. We remain enthusiastic about further research and development in this field, as we continue to leverage blockchain's capabilities to advance the privacy and protection of smart devices. conservation.

REFERENCES

[1] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," July 7th, 2013.
[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
[3] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede, spongent: A Lightweight Hash Function. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 312–325
[4] Shivam Saxena, Bharat Bhushan, Mohd Abdul Ahad, Blockchain based solutions to secure IoT: Background, integration trends and a way forward, Journal of Network and Computer Applications, Volume 181, 2021, 103050, ISSN 1084-8045.
[5] Dhar, Suparna, Bose, Indranil, Securing IoT Devices Using Zero Trust and Blockchain, 2021/01/02, 1091-9392.
[6] Issa, Wael and Moustafa, Nour and Turnbull, Benjamin and Sohrabi, Nasrin and Tari, Zahir, Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey, September 2023, volume 55, 0360-0300
[7] Sarthak Gupta, Virain Malhotra, Shailendra Narayan Singh, Securing IoT- Driven Remote Healthcare Data Through Blockchain, Advances in Data and Information, Sciences, 2020, Volume 94, ISBN : 978-981-15-0693-2.
[8] El-Masri, Mazen, Hussain, Eiman Mutwali Abdelmageed, Blockchain as a mean to secure Internet of Things ecosystems – a systematic literature review, volume 34, 2021, ISSN 1741-0398
[9] Alfandi Omar, Khanji Salam, Ahmad Liza, and Khattak Asad. 2021. A survey on boosting IoT security and privacy through blockchain. Cluster Computing 24, 1 (2021), 37–55.
[10] Naz, Muqaddas & Javaid, Nadeem & Iqbal, Sohail. (2019). Research Based Data Rights Management Using Blockchain Over Ethereum Network.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY