Secured Private Data Sharing Based on Blockchain Method in Internet of Things

Subila Thankam T[1], Dr.B. Ben Sujitha[2]
[1]*PG Student, Department of CSE, Noorul Islam Centre for Higher Education, (Deemed to be University)*
[1]*Kumaracoil, Thuckalay, Kanyakumari District, Tamil Nadu, India*
[2]*Professor, Department of CSE, Noorul Islam Centre for Higher Education, (Deemed to be University)*
[2]*Kumaracoil, Thuckalay, Kanyakumari District, Tamil Nadu, India*

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices has significantly increased the volume of data generated, necessitating robust mechanisms for secure data sharing and privacy preservation. In this paper we introduced an advanced security framework incorporating Deniable Matchmaking Encryption (DME) to address the limitations identified previously. DME offers an additional layer of privacy by allowing users to plausibly deny the existence of encrypted data, thus mitigating the risks associated with coercive attacks. This novel approach integrates seamlessly with blockchain technology to ensure tamper-proof transaction logging and enhances user anonymity through advanced cryptographic techniques.**

***Index Terms*—Privacy; Data Sharing; Blockchain; IoT; Security; DME**

I. INTRODUCTION

The rapid expansion of Internet of Things (IoT) devices has ushered in an era of unprecedented data generation and connectivity, revolutionizing industries from healthcare to manufacturing. As these devices proliferate, the need for secure and private data handling mechanisms becomes paramount. Traditional approaches to data security often fall short in IoT environments due to the scale, diversity, and dynamism of connected devices. Ensuring confidentiality, integrity, and availability of data amidst these complexities requires innovative solutions that can mitigate evolving cyber threats while preserving user privacy. [1]

In response to these challenges, our research presents a sophisticated security framework designed to meet the unique demands of IoT ecosystems. The initial phase of our framework employed homomorphic encryption and ring signatures to secure data transmission and authenticate users, including bidders and sellers, anonymously. These insights prompted the evolution to our second phase, where we introduce Deniable Matchmaking Encryption (DME) as a pivotal enhancement. [2]

DME represents a cutting-edge cryptographic technique that not only enhances data security but also addresses privacy concerns by allowing users to plausibly deny the existence of encrypted data. This capability is crucial in safeguarding against coercive attacks and ensuring user autonomy in data sharing and transaction scenarios. Furthermore, our framework integrates seamlessly with blockchain technology, leveraging its inherent properties of transparency and immutability to establish tamper-proof transaction logs. By combining DME with blockchain, we augment the framework's ability to provide auditable records of data transactions while bolstering user anonymity. [3]

The architecture of our system is modular, comprising IoT devices for data collection, preprocessing modules, and specialized encryption mechanisms. This design not only secures data at every stage but also optimizes performance to accommodate the scalability demands of large-scale IoT deployments.[4]

By integrating advanced encryption techniques like DME with blockchain technology, our framework not only ensures secure and private data sharing but also lays the foundation for a more resilient and trustworthy IoT ecosystem. [5]. The DME encryption in our IoT security framework represents a cutting-edge solution to the challenges of privacy preservation and secure data sharing. Its innovative approach not only addresses current vulnerabilities in IoT security but also anticipates future needs for

robust, privacy-preserving technologies in the digital age.[6]

II. RELATED WORKS

Ying Gao et al [7] have used blockchain and proxy re-encryption (PRE) technologies to tackle these challenges. The blockchain authorizes all devices in the network to improve their credibility and authenticity. What's more, a blockchain-based data sharing framework that combines a PRE scheme is introduced for secure device-to-device communication in smart communities. A series of smart contracts are designed for flexible operations of searching and updating records on the blockchain.

Xiaofang L et al [8] have constructed a blockchain privacy protection scheme based on ring signature. This solution has built a privacy data storage protocol based on the ring signature on the elliptic curve, and used the complete anonymity of the ring signature to ensure the security of data and user identity privacy in blockchain applications. The correctness and safety proof analysis of the proposed scheme were also carried out.

Mengyuan Li et al [9] have proposed a novel searchable attribute cryptographic access control mechanism that facilitates trusted cloud data sharing. Users can use keywords to efficiently search for specific data and decrypt content keys when their properties are consistent with access policies. in this way Cloud service providers will not be able to access any data privacy-related informationEnsuring the security and trustworthiness of data sharing as well as the protection of user data privacy. our simulation results show that our approach outperforms existing studies in terms of time overhead. compared to traditional access control schemes.

Wei Yang et al[10] have proposed a secure and efficient data sharing scheme for IoT. First, the scheme integrates blockchain with the distributed database, utilizing smart contracts to ensure secure data storage, querying, and sharing in IoT. Second, they incorporated a reputation mechanism into the data sharing process. This allows IoT users to receive reputation feedback from their partners based on their behaviours, which is dynamically updated as a reputation score on the blockchain by smart contracts. Therefore, honest users get more opportunities to share data, while malicious users are held accountable and revoked from the IoT system. They also harness advanced cryptographic techniques to ensure the submission of reputation feedback does not disclose the user's private information, preventing vindictive actions from malicious users.

Abdullah Aljumah et al[11] have Proposed a BCT-based lightweight IoT information exchange security architecture for data exchange. The proposed technique uses a dual chain methodology, namely transaction and data BCT working together to provide distributed storage and tamper-proofing of data. Moreover, Transaction BCT is enhanced by a consensus algorithm using a practical Byzantine fault-tolerant (PBFT) mechanism. The proposed algorithm can increase data registering efficiency, transactions, and privacy protection BCT. It is deduced that local dominance can be avoided using the dynamic game strategy of node cooperation. Furthermore, by reporting the node's global reputation value, the status of the unknown node may be approximated. The high-trust measure is utilized to adjust the weight of the affected node in the combined node-set, leading to the Bayesian equilibrium.

III. PROPOSED METHODOLOGY

The proposed system aims to address the limitations of the existing system by integrating Deniable Matchmaking Encryption (DME) and optimizing other critical aspects to enhance security, efficiency, and scalability in IoT data sharing. This proposed system builds on the foundation established in existing method, focusing on overcoming computational overhead, improving key management, and ensuring scalability and usability. The proposed enhancements are designed to create a more robust, flexible, and user-friendly system for secure IoT data transactions.

A. Integration of Deniable Matchmaking Encryption (DME)

Deniable Matchmaking Encryption (DME) is introduced to provide an additional layer of security and privacy. DME allows users to plausibly deny the existence of certain encrypted data, protecting against coercion attacks. This method ensures that even if an adversary forces users to reveal their encryption keys, they can deny the presence of specific sensitive data.

DME will be seamlessly integrated with existing cryptographic mechanisms to enhance overall system security without compromising performance.

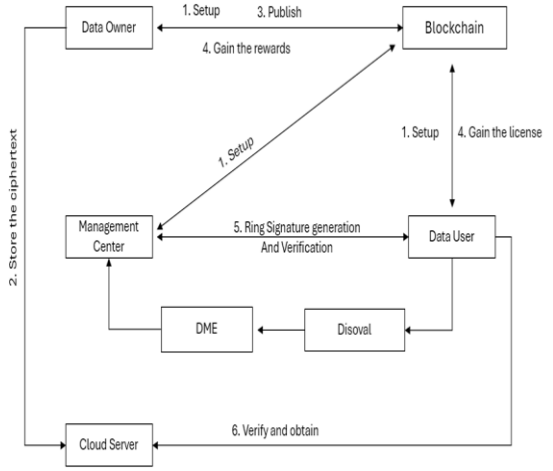

Fig.1. The Proposed Architecture

a. Data Owner

- Description: The Data Owner is an entity or individual who generates and controls access to data. They are responsible for creating, managing, and providing permissions for their data.
- Role: Initiates data sharing requests, manages access controls, and interacts with the system to protect and share data securely.

b. Blockchain

- Description: Blockchain is a decentralized ledger technology that records transactions in a secure and immutable manner. It provides transparency, data integrity, and tamper-proof records.
- Role: Stores and manages transaction logs, maintains decentralized security controls, and facilitates secure data sharing and verification processes.

c. Data User

- Description: The Data User is an individual or system that accesses or utilizes the data provided by the Data Owner. They may request access to the data based on predefined permissions.
- Role: Consumes or processes the data for various purposes while complying with access permissions and security protocols.

d. Management Centre

- Description: The Management Centre oversees and coordinates the interactions between different components of the system. It is responsible for policy enforcement, monitoring, and managing user access and data sharing processes.
- Role: Provides administrative control, manages data access requests, and ensures compliance with security and privacy policies.

e. Deniable Match-Making Encryption (DME)

- Description: Deniable Match-Making Encryption is a cryptographic technique that allows users to securely share data while being able to plausibly deny the existence of the data. It is designed to protect data from coercive attacks.
- Role: Encrypts data in a manner that allows the owner to deny its existence if necessary, enhancing privacy and security during data sharing.

f. Disovial Algorithm

- Description: The Disovial Algorithm is a specific algorithm used within the system for data processing, encryption, or access control. It is involved in managing how data is shared or protected within the framework.
- Role: Executes specific tasks related to data processing or security, such as encrypting, decrypting, or validating data transactions. [12]

g. Cloud Server

- Description: The Cloud Server provides storage and computational resources for the system. It hosts data, performs computations, and supports the operations of the blockchain and other components.
- Role: Stores data, executes processing tasks, and interacts with other components to facilitate secure data access and management.

A. Optimization of Computational Efficiency

To address the high computational overhead associated with homomorphic encryption, the proposed system will implement several optimization strategies:

- Algorithmic Improvements: Refining and optimizing the homomorphic encryption algorithms to reduce complexity and enhance performance.
- Hardware Acceleration: Utilizing specialized cryptographic processors and hardware accelerators to offload intensive computations from IoT devices, thereby improving efficiency.

- Selective Encryption: Implementing selective encryption techniques where only critical data is encrypted homomorphically, while less sensitive data uses lighter encryption methods.

B. Enhanced User Authentication Mechanisms

The proposed system will strengthen user authentication by incorporating multi-factor authentication (MFA) mechanisms, including:

- Biometric Authentication: Adding biometric verification methods such as fingerprint or facial recognition to enhance security.
- Behavioral Analytics: Employing machine learning techniques to analyze user behavior and detect anomalies, providing an additional layer of security.
- User-Friendly Interfaces: Designing intuitive and user-friendly interfaces to simplify the authentication process, making it accessible and straightforward for users.[13]

C. Secure and Efficient Data Sharing Protocols

The proposed system will develop advanced data sharing protocols leveraging DME and other cryptographic techniques:

- Dynamic Protocol Design: Creating protocols that adapt to different data sensitivity levels and usage scenarios, ensuring optimal security and efficiency.
- Regulatory Compliance: Ensuring that the new data sharing protocols comply with international data protection regulations and standards, providing a trustworthy and legally compliant system.
- Decentralized Data Management: Implementing decentralized data management to reduce single points of failure and enhance data availability and security.[14]

D. Expanded Smart Contract Functionality

The smart contracts used in the system will be enhanced to support more complex and customizable reward distribution mechanisms:

- Advanced Smart Contracts: Developing smart contracts that can handle diverse reward scenarios, including conditional rewards based on data usage and contributions.
- Blockchain Integration: Ensuring seamless integration of smart contracts with the blockchain to maintain transparency, immutability, and security.
- Automated Reward Distribution: Implementing automated processes to distribute rewards fairly and transparently based on predefined criteria, encouraging user participation and data sharing.

The proposed system aims to significantly enhance the security, efficiency, and scalability of IoT data sharing by integrating Deniable Matchmaking Encryption and optimizing various aspects of the existing system. By addressing the limitations identified in existing method, the proposed enhancements will create a more robust, flexible, and user-friendly platform. These improvements will ensure secure, efficient, and privacy-preserving data transactions, paving the way for a scalable and trustworthy IoT data sharing ecosystem.[15]

IV. RESULTS AND DISCUSSION

A. Summary of Results

The implementation of the proposed system involves several key modules that work together to provide enhanced security and privacy in IoT data sharing. The primary modules in the system are as follows:

- Login/Signup Module
- NFT Upload Module
- Initiate Transaction Module
- Publish for Reward Module
- Result of Publication Module

The aim is to evaluate the effectiveness of the proposed security framework incorporating Deniable Matchmaking Encryption (DME) in addressing the challenges associated with data privacy, security, and operational efficiency in IoT environments. The discussion also explores the broader impact of the system, potential areas for improvement, and future research directions. our proposed security framework effectively addresses the key challenges associated with IoT data security and privacy. The integration of DME and blockchain technology provides a robust solution that enhances both user privacy and data integrity.

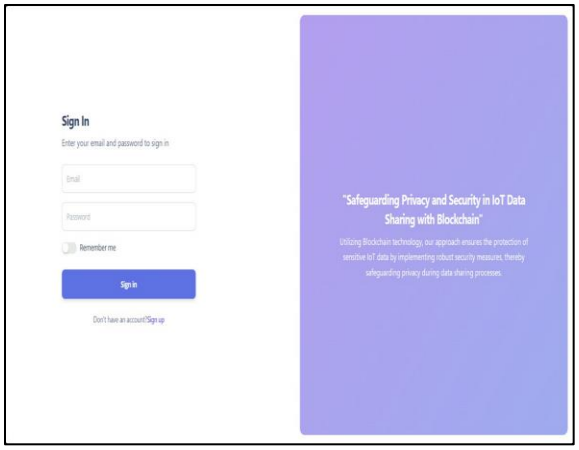

Fig 2 Sign-In Page

This is where users enter their unique identifier, which may be a username, email address, or another piece of information associated with their account. Users input their secret password in this field, serving as a second factor for authentication. Passwords are typically hidden to protect them from being visible. After entering the required credentials, users click the "Sign-In" or "Log In" button to submit their information and initiate the authentication process.

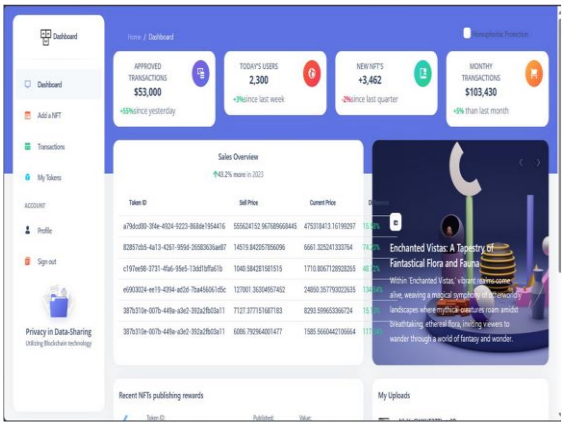

Fig 3 Dashboard

Users often have the ability to customize dashboards to suit their specific needs and preferences. This may include selecting the KPIs to display, arranging visual elements, and adjusting settings for a personalized experience. Many dashboards support interactivity, enabling users to drill down into specific data points, filter information based on criteria, or toggle between different views. Interactive elements enhance the user's ability to explore and analyse data.

Choose a blockchain platform that supports NFTs. Ethereum, Finance Smart Chain, and Flow are examples of popular blockchains for NFTs. If you don't have a cryptocurrency wallet, create one. This wallet will be used to store your NFTs. Ensure that it is compatible with the blockchain platform you've chosen. Choose a minting platform or marketplace where you can create and publish your NFT. Platforms like Open Sea (for Ethereum), Rarible, or Mintable offer minting services. Connect your wallet to the chosen platform.

V. CONCLUSION

The rapid expansion of the Internet of Things (IoT) has brought about unprecedented opportunities and challenges in data generation, transmission, and security. This research aimed to address these challenges by developing an advanced security framework that leverages Deniable Matchmaking Encryption (DME) and blockchain technology to enhance data privacy, security, and operational efficiency within IoT environments. we introduced DME to provide an additional layer of privacy and security, allowing users to plausibly deny the existence of encrypted data and mitigating risks associated with coercive attacks. The integration of DME with blockchain technology further enhanced the system's robustness by ensuring tamper-proof transaction logs and transparent, immutable data exchanges. Our research represents a significant advancement in IoT security, providing a comprehensive and scalable solution to modern data privacy challenges. By integrating state-of-the-art encryption methods with blockchain technology, our framework sets a new standard for secure and efficient data management in IoT ecosystems.

REFERENCES

[1] Madhu, B., Chari, M. V. G., Vankdothu, R., Silivery, A. K., & Aerranagula, V., “Intrusion detection models for IOT networks via deep learning approaches”, Measurement Sensors, 25, 100641. https://doi.org/10.1016/j.measen.2022.100641,2023.

[2] Sohail, S., Fan, Z., Gu, X., & Sabrina, F, “Multi-tiered Artificial Neural Networks model for intrusion detection in smart homes”, Intelligent Systems with Applications, 16, 200152. https://doi.org/10.1016/j.iswa.2022.200152, 2022.

[3] Wang, M.; Yang, N.; Weng, N. “Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System”, Electronics 2023, 12, 2100. https://doi.org/10.3390/ electronics12092100, 2023.

[4] Yoo, S., Kim, S., Kim, S., & Kang, B. B, “AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification”, Information Sciences, 546, pp: 420435.https://doi.org/10.1016/j.ins.2020.08.082 ,2021.

[5] Bukhari, O., Agarwal, P., Koundal, D., & Zafar, S, “Anomaly detection using ensemble techniques for boosting the security of intrusion detection system”, Procedia Computer Science, 218, 1003–1013. https://doi.org/10.1016/j.procs.2023.01.080,2023 .

[6] Xu, L.; Xu, K.; Qin, Y.; Li, Y.; Huang, X.; Lin, Z.; Ye, N.; Ji, X, “TGAN-AD: Transformer-Based GAN for Anomaly Detection of Time Series Data”, Appl. Sci. 2022, 12, 8085. https://doi.org/10.3390/ app12168085,2022.

[7] Ying Gao; Yijian Chen; Hongliang Lin; Joel J. P. C. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities", IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Canada, 2020.

[8] XIAOFANG LI, YURONG MEI, JING GONG, FENG XIANG and ZHIXIN SUN, "A Blockchain Privacy Protection Scheme Based on Ring Signature", IEEE Access,Special Section on Blockchain technology: Principles and Applications, Vol-8,2020.

[9] Mengyuan Li,Shaoyong Guo,Wenjing Li,Ao Xiong,Xiaoming Zhou,Jun Qi,Feng Qi,Dong Wang,Da Li, "Secure and trusted sharing mechanism of private data for Internet of Things", Elsevier,High-Confidence Computing, In Press, 2024.

[10] Wei Yang,Chengqi Hou,Zhiming Zhang,Xinlong Wang,Shaolong Chen, "Secure and Efficient Data Sharing for IoT Based on Blockchain and Reputation Mechanism",IEEE Internet of Things Journal, Volume-11,No-11,2024.

[11] Abdullah Aljumah and Tariq Ahamed Ahanger, "Blockchain-Based Information Sharing Security for the Internet of Things", MDPI, Mathematics 2023, 11(9), 2157; https://doi.org/10.3390/math11092157.

[12] Poongodi, M., & Hamdi, M, “Intrusion detection system using distributed multilevel discriminator in GAN for IoT system”, Transactions on Emerging Telecommunications Technologies, 34(11). https://doi.org/10.1002/ett.4815,2023.

[13] Abbas, A., Khan, M. A., Latif, S., Ajaz, M., Shah, A. A., & Ahmad, J, “A new Ensemble-Based intrusion detection system for internet of things”, Arabian Journal for Science and Engineering, 47(2), 1805–1819. https://doi.org/10.1007/s13369-021-06086-5,2021.

[14] St´ephane Gaıffas and Ibrahim Merad, “WildWood: a new Random Forest algorithm”, IEEE Transactions on Information Theory, Volume 69, Issue: 10, 2023.

[15] Matías Gabriel Rojas, Ana Carolina Olivera, Pablo Javier Vidal, “Optimising Multilayer Perceptron weights and biases through a Cellular Genetic Algorithm for medical data classification”, Array, Elsevier, 14 (2022) 100173,2022.