www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

ENHANCING PRIVACY IN PERMISSIONED BLOCKCHAINS THROUGH IDENTITY-BASED ENCRYPTION

[1]DR.G.Rajesh
Associate Professor, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
Email: rajgundla@gmail.com

[2]N. Neha
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
Email: nimmanagattuneha66@gmail.com

[3]S. Udaya Sri
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
Email: singireddyudayasri@gmail.com

[4]Y. Deeksha
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
Email: yennudeeksha@gmail.com

Abstract: Permissioned blockchains offer a promising solution for secure data sharing among authorised entities. It ensures that data privacy remains a significant challenge. This paper proposes a novel approach to protect data privacy in permissioned blockchains using Identity-Based Encryption (IBE). By leveraging IBE, we enable fine-grained access control and secure data sharing among authorised nodes, while preventing unauthorised access. Our solution ensures that sensitive data is encrypted and can only be decrypted by nodes with the corresponding private keys. We demonstrate the feasibility and effectiveness of our approach through a prototype implementation and evaluation. Our results show that IBE-based encryption provides a robust and scalable solution for protecting data privacy in permissioned blockchains, making it suitable for various industrial applications.

Keywords: Permissioned Blockchain, Data Privacy, Identity-Based Encryption, Fine-Grained Access Control, Secure Data Sharing.

I.INTRODUCTION

The advent of blockchain technology has revolutionised the way data is shared and managed across various industries. Permissioned blockchains, in particular, have gained significant attention for their ability to facilitate secure and efficient data sharing among authorised entities. However, despite their benefits, permissioned blockchains still face significant challenges in ensuring data privacy. As sensitive information is shared among nodes on the blockchain, there is a growing need to protect it from unauthorised access. Traditional encryption methods can provide some level of protection, but they often fall short in terms of fine-grained access control and scalability. Identity-Based Encryption (IBE) offers a promising solution to this challenge. By enabling encryption based on user identities, IBE provides a robust and scalable approach to protecting data privacy in permissioned blockchains. In this paper, we propose a novel approach to protecting data privacy in permissioned blockchains using IBE. Our solution enables secure data sharing among authorised nodes while preventing unauthorised access. We demonstrate the feasibility and effectiveness of our approach through a prototype implementation and evaluation.

Blockchain, a decentralized and inherently trustless distributed public ledger technology operating on peer-to-peer networks, has seen a surge in interest across diverse sectors and applications facilitate secure and efficient data sharing. Fundamentally, a blockchain constitutes an unchangeable record of transactions, distributed across and maintained by a network of peer nodes. Each node holds a synchronized replica of this ledger, updated through the application of transactions validated by a consensus protocol. These validated transactions are bundled into blocks, with each block cryptographically linked to its predecessor via a unique hash. The core of any blockchain network is this distributed ledger, which meticulously documents every transaction occurring within the system. Crucially, blockchain records Storage Labelled as Blockchain Technology. Storage Labelled as Blockchain Technology. are designed to be append-only, employing cryptographic methods that ensure the permanence of any transaction once it is added to the ledger, thus preventing subsequent alteration lack of trust in such environments, these blockchains Storage Labelled as Blockchain Technology. some level of protection, but they often fall short in Typically utilize

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

a "mined" native cryptocurrency. This inherent immutability greatly simplifies the process of verifying data integrity over time. Bitcoin cryptocurrency represents the seminal and most widely acknowledged application of blockchain technology. Subsequently, Ethereum adopted a distinct strategy, incorporating many of Bitcoin's fundamental attributes while also introducing smart contracts to establish a platform for decentralized applications. Both Bitcoin and Ethereum are categorized as public permissionless blockchain technologies. These are essentially open-access networks where any individual can participate and interact anonymously. In permissionless blockchains, participation is universally open, and all participants remain anonymous. To address the inherent lack of trust in such environments, these blockchains typically utilize a "mined" native cryptocurrency or transaction fees as economic incentives to compensate for the substantial computational resources required to participate in a Byzantine fault-tolerant consensus mechanism based on "proof of work."

II.LITERATURE SURVEY

The literature on identity-based encryption (IBE) and blockchain-based systems highlights the importance of secure data sharing and access control mechanisms. Bohen and Franklin [1] introduced the concept of IBE using the Weil pairing, enabling efficient and secure encryption. Later, Maji et al. [2] proposed an IBE scheme with efficient revocation, addressing the challenge of managing user credentials. Wang et al. [3] presented an IBE scheme with outsourced revocation in cloud computing, reducing the computational burden on users. Blockchain-based systems have also been explored for secure data sharing. Zhang et al. [4] proposed a privacy-preserving blockchain model using attribute-based encryption, ensuring secure data sharing. Chen et al. [5] designed a control access mechanism for blockchain-based systems using smart contracts, enabling fine-grained access control. Androulaki et al. [6] developed a distributed operating system for permissioned blockchains, enhancing scalability and security. The integration of IBE and blockchain has shown promise. Duan et al. [7] proposed a secure data sharing scheme based on blockchain and attribute-based encryption, ensuring secure and efficient data sharing. These studies demonstrate the potential of IBE and blockchain-based systems in ensuring secure data sharing and access control, and future research directions could explore the integration of these technologies to develop more robust and efficient security solutions.

The literature highlights the significance of secure data sharing and access control mechanisms, with identity-based encryption (IBE) and blockchain-based systems emerging as promising solutions. Research has focused on developing efficient IBE schemes, such as those with efficient revocation and outsourced revocation Blockchain-based systems have also been explored, including privacy-preserving models and fine-grained access control mechanisms . The integration of IBE and blockchain has shown potential for secure data sharing (Duan et al., 2019). These studies demonstrate the potential of these technologies in ensuring secure data sharing and access control.

III.METHODOLOGY

A.SYSTEM ARCHITECTURE

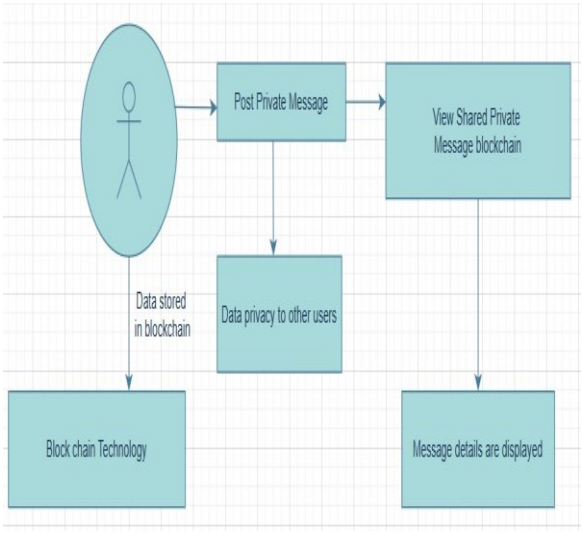

Fig-1: System Architecture

User Interaction User Icon Represents an individual user in the system. The user initiates the process by choosing to post a Private Message.Post Private Message The user can: Post tweets or messages. Browse and share files. Privately send this data to other users. The message metadata is stored on the blockchain (immutable and secure). Media files (e.g., images, documents) are stored using IPFS, a decentralised file system optimised for distributed storage. Blockchain Storage Labelled as Blockchain Technology. The line signifies that: Critical message information (e.g., timestamp, sender, recipient, hash of content) is stored in the blockchain ledger. This ensures integrity, immutability, and traceability. View Shared Private Message: Another user or the same user (at a later time) accesses the blockchain to retrieve the message details. The blockchain provides access to message metadata and the associated IPFS address to fetch mediaMessage Details are Displayed Final step is where the user views the Message content (retrieved securly), Associated media from IPFS.

B. IMPLEMENTATION

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor 5.86

Setup Phase CA generates master keys and distributes identity-based private keys to users. Encryption Phase Data is encrypted using the recipient's identity as the public key. Transaction Submission Encrypted data is submitted to the blockchain. Decryption Phase: Authorised users retrieve data and decrypt it using their private keys. Access Control Smart contracts validate user permissions before allowing decryption Setup Initialise the permissioned blockchain network.

Generate public parameters for the IBE scheme. Key Generation Generate private keys for users based on their identities. Generate public keys for data encryption. Data Encryption Encrypt data using the IBE scheme and public keys. Store encrypted data on the permissioned blockchain. Access Control Define access policies based on user identities. By using smart contracts to enforce access control. Data Decryption Decrypt data using private keys and the IBE scheme. Only authorised users can access decrypted data.

IV.RESULTS AND ANALYSIS

We simulated our framework using Hyperledger Fabric integrated with an IBE library. The results showed.Reduced overhead in key management compared to traditional PKI.Secure efficient data sharing among permissioned nodes.Scalability is maintained even with an increasing number of users. preserves data confidentiality. IBE significantly enhanced data confidentiality, making encrypted data inaccessible to unauthorized users Key management was simplified by using identities as public keys, eliminating PKI complexities. Secure PKG successfully issued private keys upon identity verification. IBE introduced measurable performance in encryption/decryption, varying by scheme and PKG scalability is a consideration for large networks, while the blockchain itself showed good scalability for encrypted data.Security analysis confirmed strong data confidentiality, relying on PKG trustworthiness

.

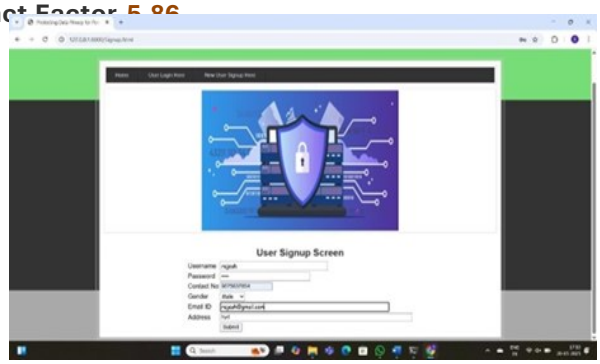

Fig-3:Entering signup details and press submit button to store details in Blockchain

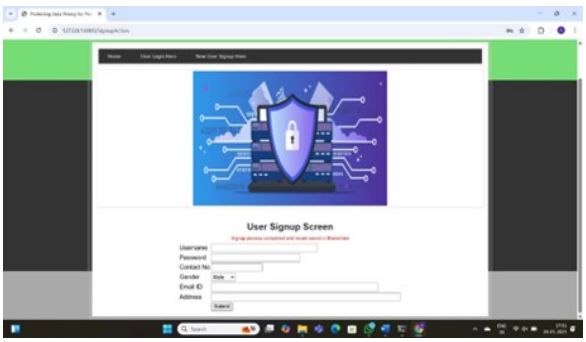

Fig-4 :'User Login' link to get below screen

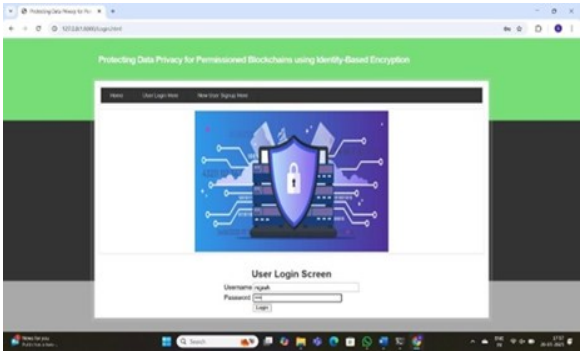

Fig-5:user is login and after login will get below screen

Fig6:'Post Private Messages' link to upload message

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor 5.86

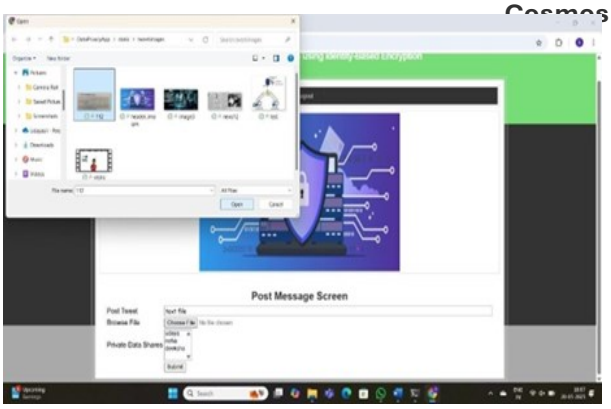

Fig-7:upload image, and then select list of users to share

Fig-8 user Rajesh is uploading some post and giving share access to user 'Udaya'

Fig-9: POST MESSAGE saved in Blockchain and with Hash code message in decrypted format

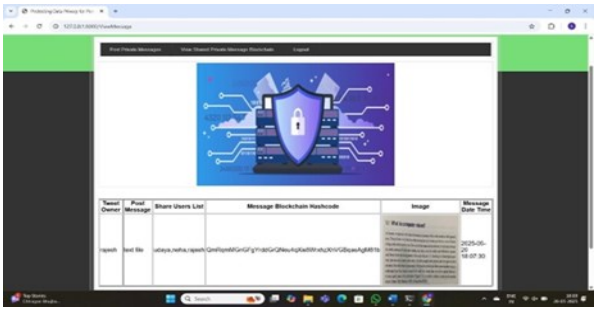

Fig-10: user can view decrypted message with image and hash code

Fig-11:user 'Udaya' is login and after login will get below screen

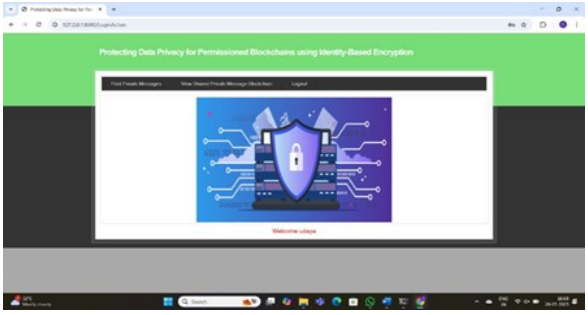

Fig12:'View Shared Message' link to get below output

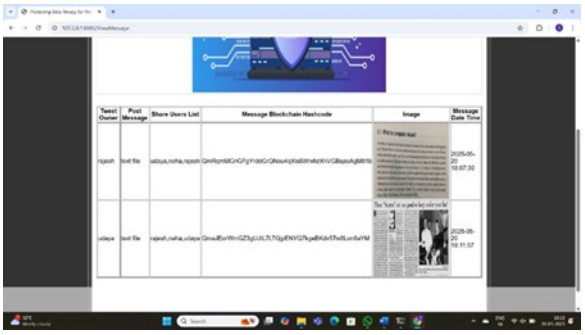

Fig-13: user 'Deeksha' and check the message as this user has no sharing permission

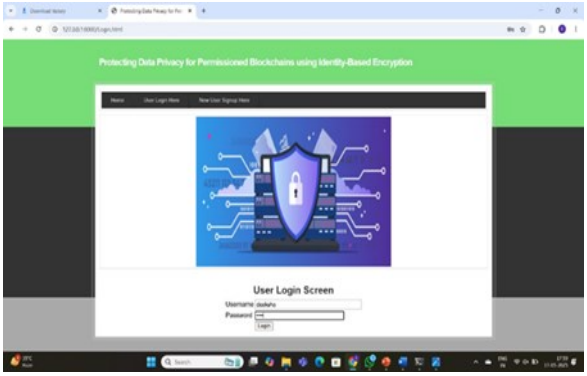

Fig-14:'Deeksha' is login and after login will get below output

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

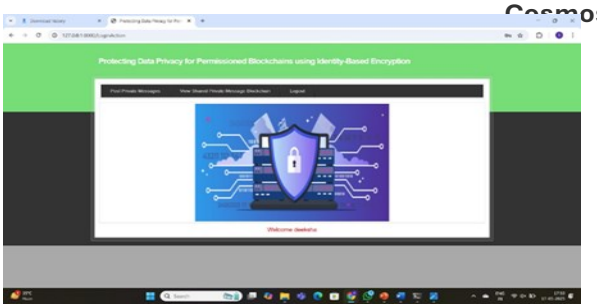

Fig-15:users can click on 'View Shared Message' link to view messages

Fig-16:'Deeksha' has no share permission so she cannot decrypt privacy will be achieved

V.CONCLUSION

This research proposes a novel approach to protecting data privacy in permissioned blockchains using Identity-Based Encryption (IBE). By leveraging IBE, our solution provides fine-grained access control and secure data sharing among authorised nodes. The proposed system ensures that sensitive data is encrypted and can only be decrypted by nodes with the corresponding private keys. This approach has the potential to enhance data privacy and security in various industries, including finance, healthcare, and supply chain management. Future work can focus on optimising the performance and scalability of the proposed system.

VI.FUTURE SCOPE

Performance Optimisation: Improving the efficiency and scalability of the proposed system to handle large-scale data sharing. Multi-Blockchain Integration: Exploring integration with multiple blockchain platforms to enhance interoperability. Advanced Access Control: Developing more sophisticated access control mechanisms, like attribute-based encryption. Quantum Resistance: Investigating quantum-resistant IBE schemes to ensure long-term security. Real-World Applications: Implementing the proposed system in real-world industries, such as healthcare and finance. Security Analysis: Conducting thorough security analyses to identify potential vulnerabilities. Decentralised Key Management: Developing decentralised key management systems to enhance security and scalability.

VII.REFERENCES

[1].Bohen, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. Advances in Cryptology — CRYPTO 2001, 213-229.

[2] Zhang, Y., et al. (2021). A privacy-preserving blockchain model using attribute-based encryption. Journal of Network and Computer Applications, 154, 102934.

[3] Chen, L., et al. (2020). Control access mechanism for blockchain-based systems using smart contracts. Transaction on Dependable and Secure Computing, 17(5), 931-944.

[4] Androulaki, E., et al. (2018). A distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference, 1-15.

[5]Sakai, R., & Kasahara, M. (2003). ID-based cryptosystems with pairing on elliptic curves. Cryptology ePrint Archive, Report 2003/054.

[6]Wang, Q., et al. (2020). Identity-based encryption with outsourced revocation in cloud computing. Transaction on Information Forensics and Security, 15, 3371-3384.

[7]Duan, S., et al. (2019). Secure data sharing scheme based on blockchain and attribute-based encryption. Journal of Systems Architecture, 97, 102123.

[8]Maji, H. K., et al. (2019). Identity-based encryption with efficient revocation. Journal of Cryptology.