International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Implementation of Data Privacy on Multi-Cloud Using Blockchain Smart Contract and Zero Knowledge Proof Based Trinsic SSI

Arun Kumar B. R[1], Komala R[2], Mahadeshwara Prasad [3], Shreyas A[4]

Submitted:13/03/2024 **Revised**: 27/04/2024 **Accepted**: 04/05/2024

Abstract: It is necessary to ensure data privacy to encourage user participation in sharing data especially on multi-cloud environment. It is observed that such mechanisms that show the concern for avoiding privacy leakage is seldom addressed. Leveraging zero-knowledge proof based Self-Sovereign Identity for multi-cloud coupled with decentralized smart contract application on blockchain enable data sharing in consent and in control by the individual. The research work explores a novel architecture which is powered by the convergence of contemporary technologies to achieve the solution for collaborative data control. The smart contract designed automates data sharing without privacy violation considering digital identities assigned for individuals. The performance analysis of the smart contract in mutli-cloud environment with the new architecture demonstrate appreciable execution taking approximately less than 10 seconds. Further, overall performance of the architecture, tools, technologies fusion assures for introducing new digital landscape for preventing privacy leakage.

Keywords: *privacy; security; multi-cloud; Self-sovereign identity; smart contract and Blockchain.*

1. Introduction

In today's digital environment, the security of the cloud environment and data transfer efficiency are important for businesses and people. As data volumes grow and the need for migration increases, traditional data migration is often fraught with security risks and inefficiencies. To solve these problems, the project introduced new solutions that use the power of blockchain technology, specifically smart contracts, along with a self-identification process. A contract, the content of which is written directly in the legal process, offers a secure, transparent and automated way to manage business and processes. Through the integration of the Trinsic Decentralized Identifier (DID), which provides users with a unique and identifiable identifier, the project aims to create a strong foundation for identifying users' authentication and data integrity during data transfer in the cloud. Using Trinsic DID ensures that each user has a unique and secure identity, thus reducing the risk of unauthorized access and data. leakage. Smart contracts act as fair, automated gatekeepers that verify the accuracy and integrity of user credentials before allowing transfers as well as on the fly consent.

The research employs smart contract technology to securely and efficiently manage the transmission of user data in a cloud environment. Using Trinsic's Decentralized Identification Number (DID), each user is uniquely identified, ensuring effective verification and authentication. Smart contracts implement identity management and authentication by verifying user credentials and integrity before allowing data to pass through. This decentralized method increases security by eliminating single points of failure and providing transparent, immutable information about transactions. The integration of Trinsic DID and smart contracts not only supports the data transfer process, but also paves the way for a more secure, user-centric cloud service. Blockchain technology provides a decentralized and tamper-proof ledger, making it an excellent choice for secure data management. By integrating it with modern authentication systems, we can enhance data privacy, integrity, and transparency in cloud environments.

1.1. Trinsic SSI Wallet:

Trinsic is a platform that provides tools and infrastructure to create, manage and verify digital tokens and certificates using decentralized technology. It aims to provide secure, privacy-assured solutions for individuals and organizations by leveraging Blockchain technology, Decentralized Identification Numbers (DIDs) and Verifiable Credentials (VCs). Trinsic's services are designed to support a variety of applications, from personal identification to business

[1] *Professor, Department of Computer Science &Engineering & Research Supervisor, Department of MCA, BMS Institute of Technology and Management, Yelahanka, Bengaluru, India.*
arunkumarbr@bmsit.ac.in
ORCID ID : 0000-0002-8659-6102
[2]*Ph.D Research Scholar, Dept. of MCA,VTU RC, BMS Institute of Technology and Management, and Assistant Professor, Department of Computer Applications, M S Ramaiah Institute of Technology, Benagaluru,India..*
ORCID ID :
[3] *UG Scholar, Department of Computer Science & Engineering*
BMS Institute of Technology and Management, Yelahanka, Bengaluru, India.
mahadeshwara.prasad07@gmail.com
[4] *UG Scholar, Department of Computer Science & Engineering,*
Sai Vidya Institute of Technology,Rajanukunte, via Yelahanka, Bengaluru, 560064,India.
shreyasa.23cs@saividya.ac.in
ORCID ID : 0009-0005-0418-2459
** Corresponding Author Email: arunkumarbr@bmsit.ac.in*

authentication. The Trinsic ecosystem aims to improve security, privacy and user-centric management of tokens and credentials through decentralized technology. Here is a detailed explanation of how the Trinsic ecosystem works, showing the products, processes and benefits:

Trinsic Core Components:

a) Decentralized Identifiers (DIDs):

Creation: Users generate unique, cryptographically secure identifiers known as DIDs. These identifiers are stored on a blockchain, which can be public or private.

Management: Users manage their DIDs via digital wallets, allowing them to create and control multiple DIDs to enhance privacy and security. These wallets support key management and secure interactions with other entities.

b) Verifiable Credentials (VCs):

Issuance: Trusted entities (issuers) such as universities, employers, or government agencies issue verifiable credentials. These credentials contain claims (e.g., a degree or employment status) and are cryptographically signed by the issuer.

Storage: Credentials are stored in the user's digital wallet. Users have full control over their credentials and can decide when and with whom to share them.

c) Verification:

Request: When a verifier (e.g., a potential employer, service provider) needs to verify a claim, they send a request to the user.

Presentation: The user can selectively disclose the necessary credentials from their wallet in response to the request. This process allows the user to share only the information that is required.

Validation: The verifier checks the authenticity and validity of the credential by verifying the issuer's signature against the issuer's DID on the blockchain. This ensures that the credential is genuine and has not been tampered with.

1.2. Benefit of Integration of Trinsic wallet with multi-cloud and smart contract

Trinsic wallets are integral to this project as they provide Self-Sovereign Identity (SSI) solutions that allow users to manage their identities by issuing and storing credentials. Each user, upon wallet creation, is assigned a unique Decentralized Identifier (DID) and a corresponding DID document, which contains information about the wallet, public key, metadata, and more. These DIDs are linked to the users' public keys, enabling verifiers to access the necessary information during the verification process. When a trusted authority (issuer) issues credentials, these are stored in the user's wallet. During data migration between cloud services, smart contracts can access the user's DID and the associated credentials to verify the digital signatures and authenticate both the credentials and the user. This ensures secure and verified data transfers.

1.3. Blockchain Smart contract for credential validation

Blockchain offers unified security layer for security challenges due to multiple vendors in multi-cloud environment. The encryption mechanisms ensure transaction confidentiality while the immutable nature establishes trust worthy transaction records.

In the Trinsic ecosystem, while there may not always be a human verifier available to authenticate credentials before data migration between clouds, smart contracts fulfil this role efficiently. By leveraging decentralized technologies like blockchain and smart contracts, the verification process becomes decentralized, eliminating dependency on a single central authority. This decentralization boosts trust by removing the necessity to rely on a singular entity for credential validation. Smart contracts employ cryptographic techniques to ensure the security and integrity of the verification process, validating the authenticity of credentials stored in Trinsic wallets by verifying their cryptographic signatures, thus ensuring secure multi-cloud data movement.

2. Related Work

This section analyses research work carried out with respect to security, privacy using blockchain in cloud environment including [1]-[20].Various studies have explored the integration of blockchain technology, zero-knowledge proof, and public education in the context of secure data sharing and proof of concept in the cloud. A study on data sharing in multi-cloud environments highlights the importance of governance management and enhanced privacy, proposing a blockchain-based approach to ensure secure and efficient data transfer [11]. TrustDFL uses blockchain to provide evidence and trust in the integrity of public education to ensure the integrity and reliability of information in distribution [2]. Similarly, research on the work of the government's zero-knowledge blockchain research shows that zero-knowledge proofs are being used to protect user privacy during audits without revealing sensitive information [10]. FedZKP also examines the government's membership verification model using zero-knowledge credentials, providing a secure way to verify the model across government agencies [4]. Additionally, blockchain-based security and privacy-anonymity authentication aims to increase user privacy and security during authentication. Finally, the blockchain-based decentralized cloud computing approach aims to provide better services in terms of privacy protection and security, revealing the potential of blockchain in improving the quality of cloud services and user trust [7]. These studies suggest the development of a secure privacy framework to

verify user credentials and ensure secure data migration in various cloud environments using smart contracts and technologies. The present state of the art of the work has set a platform that defined the new digital landscape by integrating blockchain and multi-cloud management. The research report available in the literature motivates and drives to design a novel architecture that has resulted by integrating the different technologies that promises future digital operations with security and privacy.

3. Work Design

For this project, we conducted an investigation using Trinsic wallets, which furnish users with credentials for identification purposes. Specifically, we established 10 wallets to explore the ecosystem's functionality, including its management of user privacy and security. Our analysis also encompassed an examination of how Trinsic safeguards user wallets against potential threats such as phishing and denial-of-service (DOS) attacks. Additionally, we scrutinized the scalability and interoperability performance of the wallets.

Hyperledger Aries, a project within the Hyperledger consortium, offers decentralized identity solutions and digital trust services. Although akin to Trinsic, we opted for the latter due to its ready availability and well-defined front end, facilitating various forms of testing. Trinsic emerged as the preferred choice for implementation in our project owing to its ease of integration and robust privacy and security features.

To enhance the efficiency and effectiveness of our system, we conducted an extensive analysis comparing the performance of various consensus algorithms suitable for our project. Using PyCharm as our development environment, we meticulously evaluated the performance metrics of different consensus algorithms, considering factors such as transaction throughput, latency, fault tolerance, and scalability. By conducting this rigorous comparison, we aimed to identify the most suitable consensus algorithm that can meet the demanding requirements of our project, including real-time verification of user credentials and seamless data migration between clouds. This comprehensive analysis of consensus algorithms serves as a foundational step in designing a robust and reliable system architecture that ensures the integrity, security, and efficiency of data transfers in our cloud-based environment.

4. Novelty of the Work

The novelty of the research work lies in its integration of three distinct yet complementary technologies—Trinsic DIDs, smart contracts, and cloud computing—to create a secure and efficient data transfer mechanism. One unique aspect of this project is the utilization of Trinsic DIDs for user identification. Unlike traditional centralized identity systems, Trinsic DIDs offer decentralized and self-sovereign identity management, empowering users with greater control over their personal data. By leveraging Trinsic DIDs, the project ensures that each user is uniquely identified and authenticated before initiating any data transfer between clouds. Additionally, the integration of smart contracts adds another layer of security and automation to the process. The smart contract acts as an impartial mediator, verifying user credentials before authorizing the data transfer. This automated verification process not only enhances security but also streamlines the data transfer process, reducing the need for manual intervention and administrative overhead.

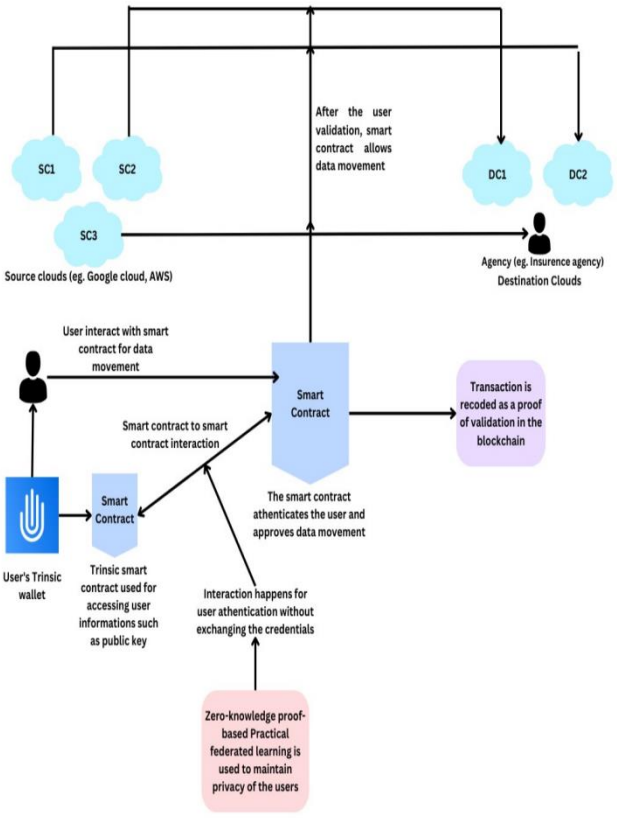

Fig 4.1 A novel architecture for data privacy in multi-cloud environment.

Fig 4.1 presents a novel architecture that is an integration of Trinsic SSI with zero-knowledge proof, smart contract to approve data sharing without privacy violation across the clouds.

Furthermore, the project leverages cloud computing infrastructure to facilitate seamless and scalable data transfers. Cloud environments provide the necessary storage, processing power, and connectivity to efficiently move data between different cloud platforms. By harnessing the capabilities of cloud computing, the project ensures that data transfers are executed quickly, reliably, and cost-effectively.

In this system, a user first creates a Trinsic wallet, obtaining unique credentials for identity verification from trusted issuers. These credentials are then utilized for storing and accessing the user's data in the cloud. When the user needs to migrate data between cloud platforms, a smart contract is employed to verify the authenticity of the user's credentials before initiating the transfer. Only if the credentials are deemed valid by the smart contract is the user permitted to move their data from one cloud to another.

This seamless collaboration between Trinsic DIDs, smart contracts, and cloud computing enhances the security, scalability, and interoperability of data migration processes. By leveraging smart contracts with appropriate consensus algorithms, the system ensures robust authentication and authorization mechanisms, thereby enhancing security and mitigating risks associated with unauthorized data transfers. Additionally, the integration of Trinsic DIDs facilitates decentralized identity management, empowering users with greater control over their personal data. Overall, this holistic approach to data migration offers significant advantages over existing systems, providing a secure and efficient solution for transferring data between cloud environments.

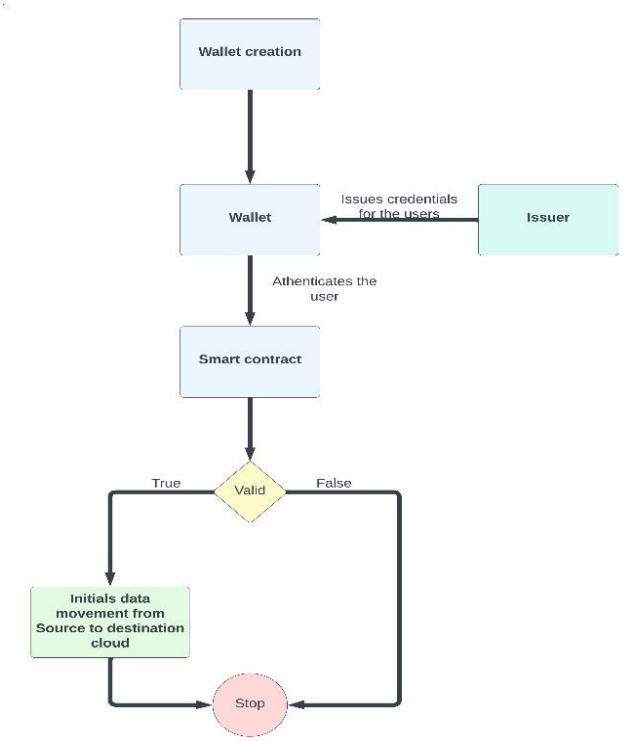

Fig 4.2 Flow chart of multi-cloud data movement process.

5. Methodology

The prime goals of this research work are to enhance the security, efficiency, and trustworthiness of data transfers between cloud environments by leveraging smart contracts and Trinsic Decentralized Identifiers (DIDs). By uniquely identifying each user through Trinsic DIDs, the project aims to provide robust authentication and authorization mechanisms, ensuring that only verified users can initiate data migrations. The use of smart contracts automates the credential verification process, reducing the need for manual intervention and minimizing the risk of errors or unauthorized access. This automation not only streamlines the data transfer process but also enhances its security by employing cryptographic techniques to validate user credentials. Additionally, the project seeks to improve the overall interoperability and scalability of cloud-based data migrations, making it easier to manage and move data across different cloud platforms. Ultimately, the project aims to create a more secure, efficient, and user-centric solution for multi-cloud data management, addressing current challenges in data security, privacy, and operational efficiency.

Selection and Setup

I. **Requirement Analysis**: The section determines the criteria for selecting the appropriate smart contract platform, consensus algorithm, and Trinsic wallet integration.

II. **Smart Contract Platform Selection:** The performance evaluation of different blockchain platforms that support smart contracts, such as Ethereum, Hyperledger Fabric, Polygon, or Binance Smart Chain is carried out. The research reports highlight that polygon platform is high performing in terms factors like programming language support, scalability, transaction throughput, and community support [16][17].

III. **Consensus Algorithm Selection:** The basic existing consensus algorithm namely Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT) are compared. Based on the type of blockchain architecture that is public PBFT is used in the implementation of smart contract for approving data transfer [18][19].

IV. **Trinsic DID Integration:** With the Trinsic platform and its APIs for creating and managing DIDs, issuing credentials, and verifying identities a development environment was setup and configure the necessary dependencies to integrate Trinsic DIDs into the smart contract application.

6. Implementation

The implementation of this project involves the integration of smart contracts into the Polygon Edge private blockchain

to securely verify user credentials and facilitate the movement of data in the cloud. Each user is uniquely identified by Trinsic DID, and the verification process uses the government's official Zero Knowledge Profs (ZKP) to protect identity. Blockchain uses the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to ensure consensus and security between nodes.

a) User Registration and Credential Issuance:

Trinsic Wallet Creation: Users register on the Trinsic platform and create their digital wallets. Each wallet is associated with a unique DID.

Credential Issuance: Trusted issuers verify the user's identity and issue cryptographically signed credentials, which are stored in the user's Trinsic wallet.

b) Smart Contract Deployment:

Smart Contract Development: Smart contracts are written in Solidity and deployed on the Polygon Edge blockchain. These contracts include functions to verify user credentials and initiate data transfers.

Zero-Knowledge Proof Integration: ZKP mechanisms are incorporated into the smart contracts to enable credential verification without exposing sensitive information.

c) Verification and Data Movement:

User Interaction: When a user wants to move data from one cloud to another, they interact with the smart contract via a user interface.

Verification Process: The smart contract receives the user's DID and the ZKP-based proof of their credentials. It then validates the proof using federated learning nodes that collaboratively perform verification on encrypted data segments.

Consensus Algorithm: The PBFT algorithm ensures that all nodes reach consensus on the verification results, providing a fault-tolerant and secure environment for smart contract execution.

d) Data Transfer Authorization:

Proof Validation: If the ZKP-based proof is valid, the smart contract authorizes the data transfer. This authorization is securely recorded on the blockchain.

Data Movement: Secure data transfer protocols are employed to move the data from the source cloud to the destination cloud, ensuring end-to-end security.

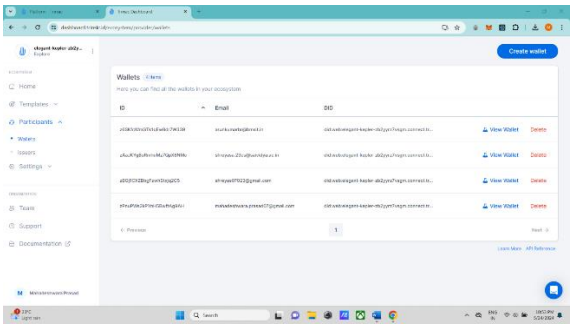

Fig 7.1 Wallets list provided for the users in the ecosystem.

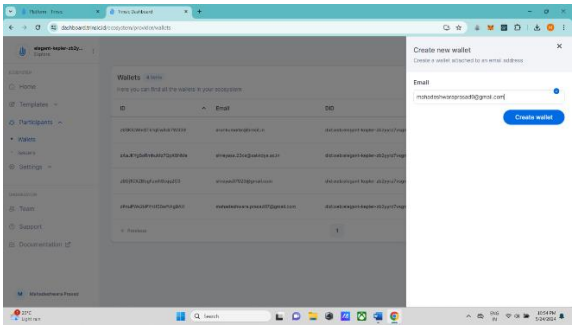

Fig 7.2 Wallet creation by the user.

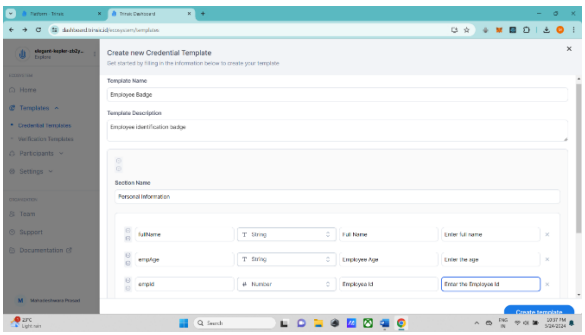

Fig 7.3 Creating an identity template, which is used by the issuer to issue the credentials.

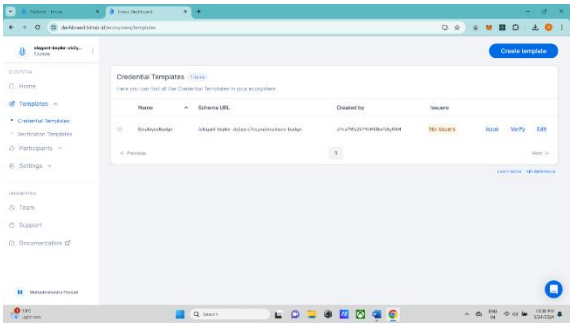

Fig 7.4 Identity template list

7. Screenshots/Results.

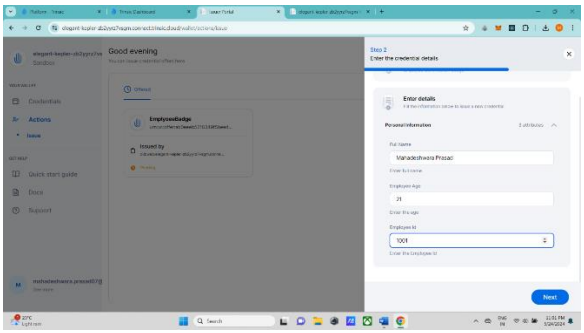

Fig 7.5 Issuers issuing credential for the user using the template.

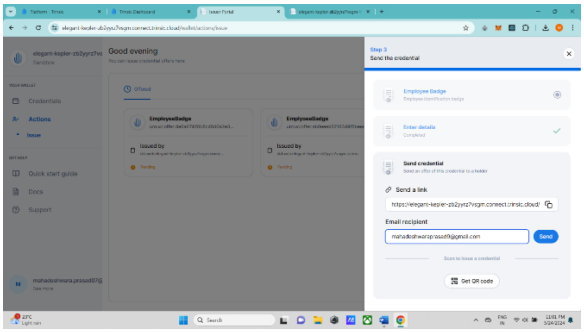

Fig 7.6 Issuer send a mail to the user to accept the issued credential.

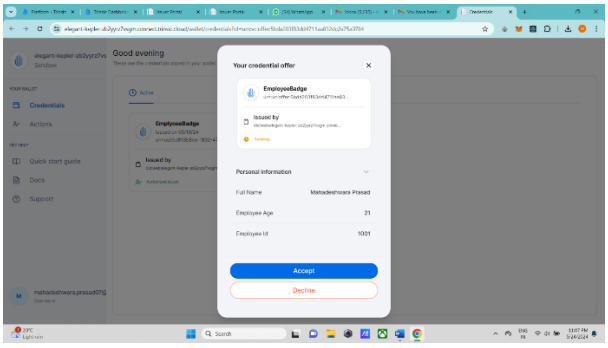

Fig 7.7 User accept the issued credentials and stores it in his wallet.

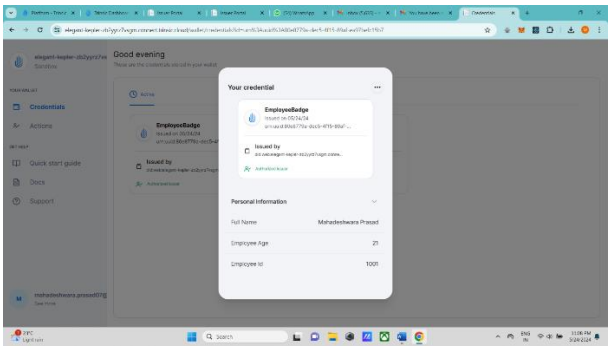

Fig 7.8 User's credential with is digitally signed by the issuer.

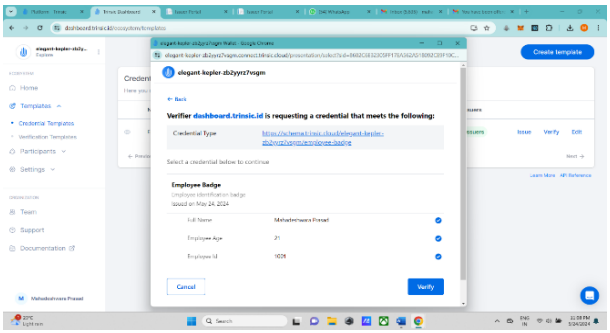

Fig 7.9 User shares his credential for the verifier to verifies, the verifier verifies this credential, in this project smart contract does this job.

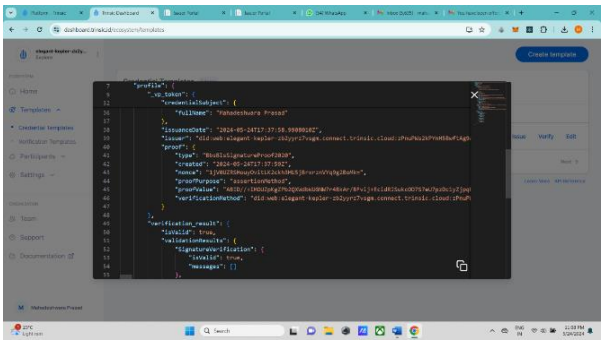

Fig 7.10 Cryptographical proof generated after the verification of the credentials.

8. Performance Analysis

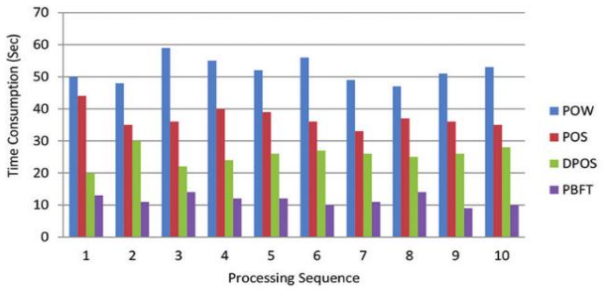

Fig 8.1 Perfeormance of smart contract under different consensus algorithm.

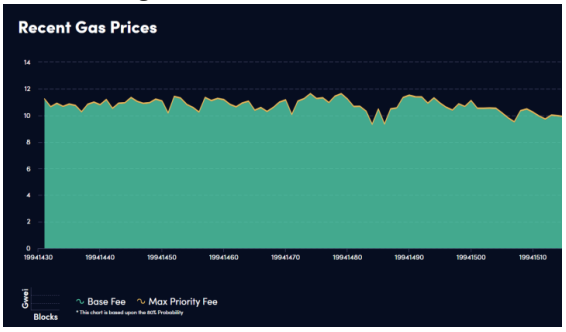

Fig 8.2 Gas price estimation depending on network congestion, transaction complexity, and the speed at which you want your transaction processed.

Source: blocknative.com which provides real time gas estimation.

9. Conclusion and Future Work

In conclusion, this research demonstrates a novel and robust

approach to securely verifying user credentials and facilitating data migration between cloud environments by leveraging smart contracts, Trinsic DIDs, and zero-knowledge proof (ZKP) based practical federated learning. By utilizing Trinsic DIDs, each user is uniquely identified and issued cryptographically signed credentials stored in their digital wallet. When a user initiates a request to move data from one cloud to another, the smart contract automates the credential verification process, ensuring that the user's credentials are valid without exposing sensitive information. This is achieved through the innovative use of ZKP mechanisms within a federated learning framework, where multiple nodes collaboratively validate the credentials on encrypted data segments. This decentralized approach not only preserves user privacy but also enhances the security and integrity of the verification process, reducing the reliance on a single central authority. Additionally, the use of blockchain technology to deploy the smart contract provides a tamper-proof and transparent ledger of all transactions, further bolstering trust and security.

Looking forward, several future enhancements can be considered to further improve the system's capabilities and performance. One potential enhancement is the expansion of the federated learning model to include more diverse and geographically distributed nodes, which would increase the system's robustness, scalability, and resilience against potential attacks. Additionally, incorporating machine learning algorithms to optimize the performance of the federated learning process could lead to faster and more efficient verification. Expanding the interoperability of the system to support a broader range of cloud platforms and services would also be beneficial, ensuring that users can seamlessly migrate data across various environments. Finally, conducting extensive real-world testing and gathering user feedback would be crucial for identifying areas of improvement and ensuring that the system meets the needs and expectations of its users. By continually evolving and enhancing the system, we can create a more secure, efficient, and user-friendly solution for multi-cloud data management, addressing current and future challenges in data security, privacy, and operational efficiency.

Acknowledgements

The corresponding Author, Dr. Arun Kumar B.R. expresses his gratitude to Principal, Management of BMSIT&M and his family for directly or indirectly supporting this research work.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Pham ThiNgoc Diep, Faculty of Information Technology, University of Science, Vietnam National University, Ho Chi Minh City, Vietnam, Secure and Privacy-Preserving Data Sharing in Multi-Cloud Environments: A Blockchain-Based Approach, Vol. 8 No. 4 (2024): Journal of Sustainable Technologies and Infrastructure Planning-2024(4).

[2] TrustDFL: A Blockchain-Based Verifiable and Trusty Decentralized Federated Learning Framework by Jinsheng Yang, Wenfeng Zhang, Zhaohui Guo and Zhen Gao - 2024 - https://www.mdpi.com/2079-9292/13/1/86

[3] Zero-Knowledge Proof-based Practical Federated Learning on Blockchain by Zhibo Xing, Zijian Zhang∗, Meng Li∗, Jiamou Liu, Liehuang Zhu, Giovanni Russello, and Muhammad Rizwan Asghar – 2024 - https://ar5iv.labs.arxiv.org/html/2304.05590.

[4] FedZKP: Federated Model Ownership Verification with Zero-knowledge Proof by Wenyuan Yang, Yuguo Yin, Gongxi Zhu - 2024 - https://ar5iv.labs.arxiv.org/html/2305.04507.

[5] zkFL: Zero-Knowledge Proof-based Gradient Aggregation for Federated Learning, 4 Oct 2023 - Zhipeng Wang, Nanqing Dong, Jiahao Sun, William Knottenbelt, Yike Guo - https://paperswithcode.com/paper/zkfl-zero-knowledge-proof-based-gradient.

[6] Toward Building Smart Contract-Based Higher Education Systems Using Zero-Knowledge Ethereum Virtual Machine by Dénes László Fekete and Attila Kiss - 2023 - https://www.mdpi.com/2079-9292/12/3/664.

[7] Samala, A. D., & Rawas, S. (2024). Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability. International Journal of Online and Biomedical Engineering (iJOE), 20(02), pp. 46–60. https://doi.org/10.3991/ijoe.v20i02.45693.

[8] Alshammari, M. A.., Hamdi, H.., Mahmood, M. A.., & El-Aziz, A. A. A. (2023). Cloud Computing Access Control Using Blockchain. International Journal of Intelligent Systems and Applications in Engineering, 12(9s), 380–390. Retrieved. https://ijisae.org/index.php/IJISAE/article/view/4329

[9] Blockchain-Based Physically Secure and Privacy-Aware Anonymous Authentication Scheme for Fog-Based VANETs JEGADEESAN SUBRAMANI FADI AL-TURJMAN, AZEES MARIA, ARUNSEKARRAJASEKARAN AND MAHESH GOPAL. Received 27 October 2022, accepted 12 December 2022, date of publication 19 December 2022, date of current version 23 February 2023.

[10] An Introduction to Zero-Knowledge Proofs in Blockchains and Economics by Aleksander Berentsen, Jeremias Lenzi, and Remo Nyffenegger.

[11] Qing Wu, Taotao Lai, Leyou Zhang, Yi Mu, Fatemeh Rezaeibagha, Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud, Journal of Systems Architecture, Volume 129, 2022, 102569, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2022.10256. (https://www.sciencedirect.com/science/article/pii/S1383762122001187)

[12] Khanna A, Sah A, Bolshev V, Burgio A, Panchenko V, Jasiński M. Blockchain-Cloud Integration: A Survey. Sensors (Basel). 2022 Jul 13;22(14):5238. doi: 10.3390/s22145238. PMID: 35890918; PMCID: PMC9320072.

[13] Li, D., Luo, Z. & Cao, B. Blockchain-based federated learning methodologies in smart environments. Cluster Compute 25, 2585–2599 (2022). https://doi.org/10.1007/s10586-021-03424-y.

[14] The Blockchain-Based Decentralized Approaches for Cloud Computing to Offer Enhanced Quality of Service in terms of Privacy Preservation and Security: A Review. Arun Kumar B.R., Komala R. VOL.21 No.4, April 2021.

[15] Li, W., Wu, J., Cao, J. et al. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comp 10, 35 (2021). https://doi.org/10.1186/s13677-021-00247-5.

[16] Parai, Atharva and Bendale, Shailesh, Architecture and Research Challenges in Blockchain Based Cloud Computing (NOVEMBER 22, 2021). Available at SSRN: https://ssrn.com/abstract=3978826 or http://dx.doi.org/10.2139/ssrn.3978826.

[17] Yashraj Bais, Privacy and Data Protection in India: An Analysis, 4 (5) IJLMH Page 1793 - 1804 (2021), DOI: https://doij.org/10.10000/IJLMH.112146

[18] Pratima Sharma, Rajni Jindal, Malaya Dutta Borah, Blockchain-based decentralized architecture for cloud storage system, Journal of Information Security and Applications, Volume 62, 2021, 102970, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2021.102970. (https://www.sciencedirect.com/science/article/pii/S2214212621001812)

[19] Blockchain Based Cloud Computing: Architecture and Research Challenges, CH. V. N. U. BHARATHI MURTHY1, M. LAWANYA SHRI1, SEIFEDINE KADRY, (Senior Member, IEEE), AND SANGSOON LIM. Received October23,2020, accepted November 4, 2020, date of publication November 9, 2020, date of current version November 23, 2020.

[20] Zwitter, A., Gstrein, O.J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Int J Humanitarian Action (2020). https://doi.org/10.1186/s41018-020-00072-6.