



International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 3, May - June 2026

Impact Factor: 9.971



Blockchain-Enhanced Privacy-Preserving Security Protocol for Cloud

B.Ratnamala¹, N.Pradeepthi², K. Jahnavi³, K.Varsha⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India¹

Students, Department of CSE Guru Nanak Institute of Technology, Hyderabad, Telangana, India^{2,3,4}

ABSTRACT: A Cloud computing has become an important technology for storing and sharing large amounts of data in various applications such as healthcare, Industrial IoT, Digital Twin systems, and enterprise environments. Although cloud services provide flexibility and scalability, they also introduce major security and privacy challenges such as unauthorized access, data tampering, replay attacks, and privacy leakage. Traditional cloud security mechanisms are not sufficient to ensure secure communication, authentication, and integrity verification in distributed cloud environments. This project proposes a Blockchain-Enhanced Privacy-Preserving Security Protocol for Cloud Environment to provide secure data sharing and authentication in cloud-assisted systems. The proposed framework integrates blockchain technology with AES-256 encryption and SHA-256 hashing algorithms to ensure confidentiality, integrity, authentication, and transparency. Blockchain is used to maintain immutable transaction records and verify the integrity of uploaded files through secure hash values. The system includes modules such as Cloud Server, Data Owner, Data User, and Trace Authority. Data Owners upload encrypted files to the cloud, authorized users request and access files securely, and the Trace Authority verifies data integrity using blockchain records. The proposed protocol protects the system against replay attacks, impersonation attacks, offline password guessing attacks, and unauthorized access attempts. Experimental analysis demonstrates that the system achieves improved security, privacy preservation, and efficient communication with reduced computation overhead compared to existing cloud security frameworks.

I. INTRODUCTION

To provide a secure and privacy-preserving cloud environment for storing and sharing sensitive data. To design a blockchain-enhanced security protocol that ensures confidentiality, integrity, authentication, and secure communication in cloud-assisted systems. To integrate blockchain technology for maintaining immutable transaction records and transparent integrity verification of uploaded data. To use AES-256 encryption and SHA-256 hashing algorithms for protecting confidential files and preventing unauthorized modifications. To prevent major security threats such as replay attacks, impersonation attacks, offline password guessing attacks, and unauthorized access in cloud environments. To support secure communication among Cloud Server, Data Owner, Data User, and Trace Authority with efficient authentication mechanisms. To improve trust management, scalability, and privacy preservation in Digital Twin and Industrial IoT cloud applications while reducing communication and computational overhead.

SCOPE OF THE PROJECT

The project focuses on developing a secure and privacy-preserving cloud environment using blockchain technology for protecting sensitive data and communication. The system is designed to provide secure storage, authentication, and data sharing in cloud-assisted Digital Twin and Industrial IoT applications. By integrating blockchain with AES-256 encryption and SHA-256 hashing algorithms, the framework ensures confidentiality, integrity, transparency, and secure access control for cloud data.

The scope of the project includes secure communication among Cloud Server, Data Owner, Data User, and Trace Authority through authentication and verification mechanisms. Blockchain technology is used to maintain immutable transaction records and verify the integrity of uploaded files using secure hash values. The system also supports encrypted file storage, secure key sharing, and privacy-preserving access to cloud resources without exposing sensitive information to unauthorized users.

II. LITERATURE SURVEY

Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain, S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, 2023, The authors proposed a blockchain-based privacy-preserving communication scheme for cloud-assisted Digital Twin (DT) environments. The framework was designed to provide secure communication between cloud servers, digital twins, and users while preserving data privacy. Blockchain technology was used to maintain immutable transaction records and ensure integrity verification. The scheme also employed authentication and session key establishment mechanisms to prevent unauthorized access and replay attacks. Formal security verification using BAN logic and AVISPA tools demonstrated the reliability of the protocol. Experimental analysis showed that the proposed system achieved efficient communication with lower computational overhead compared to traditional DT security frameworks. The study highlighted the importance of blockchain integration in improving transparency, trust management, and secure cloud communication.

Blockchain Data-Based Cloud Data Integrity Protection Mechanism P. Wei, D. Wang, Y. Zhao, et al, 2020 This research introduced a blockchain-based cloud data integrity protection mechanism for secure cloud storage systems. The scheme utilized blockchain technology and Merkle hash trees to verify the integrity of outsourced cloud data. Smart contracts were integrated to automate integrity verification and maintain transparency between cloud servers and users. The framework improved trust management by preventing unauthorized modification of stored data. Experimental results demonstrated efficient integrity verification and reduced risk of data tampering in distributed cloud environments. The paper also discussed the suitability of blockchain for Industrial IoT and enterprise cloud systems requiring secure audit mechanisms and Secure cloud data integrity verification ,detection of unauthorized data modification.

Blockchain-Based Trust Mechanism for Industrial IoT, S. Vairavasundaram, K. Kotecha, et al, 2023 This paper proposed a blockchain-based trust management framework for Industrial IoT systems integrated with Digital Twin technology. The authors used Proof of Authority (PoA) consensus mechanisms to improve trust, reduce energy consumption, and enhance security in cloud-assisted IoT applications. The framework ensured secure communication between IoT devices, cloud servers, and digital twins through decentralized verification. Blockchain records were used to maintain transparency and prevent malicious activities. Performance analysis showed improved efficiency and reliability compared to centralized trust management systems.

Secure Mutual Authentication Scheme for Meta verse Environments Using Block chain, J. Ryu, H. Kim, Y. Park, 2022, The paper presented a blockchain-enabled mutual authentication scheme for secure communication in metaverse and cloud environments. The proposed protocol established secure session keys and protected users from impersonation, replay, and password guessing attacks. Blockchain technology was utilized to store authentication records and maintain decentralized trust. The scheme also focused on reducing communication overhead while preserving privacy in cloud-assisted virtual environments. Security analysis proved the robustness of the protocol under various attack scenarios. However, the system has certain limitations. Blockchain synchronization can be complex and may increase management difficulty in distributed environments. The initial deployment and maintenance cost of blockchain infrastructure is relatively high. In addition, the framework has limited support for very large-scale cloud integration and may face scalability challenges in extensive IoT and enterprise deployments.

SPDT: Secure and Privacy-Preserving Scheme for Digital Twin-Based Traffic Control, C. Lai, M. Wang, D. Zheng, 2024, This work proposed a secure and privacy-preserving framework for Digital Twin-based intelligent traffic systems using blockchain technology. The scheme used group signatures and attribute-based access control mechanisms to provide secure communication and privacy protection among vehicles, cloud servers, and traffic management systems. Blockchain technology was integrated to maintain immutable transaction records and improve trust management among all participating entities. Experimental analysis showed that the framework achieved reduced communication latency and efficient access control in smart transportation environments. The study highlighted the importance of combining blockchain and Digital Twin technologies for secure large-scale IoT applications. The system provides secure traffic data communication, blockchain-enabled trust management, efficient attribute-based access control, and reduced communication overhead. However, the framework also faces certain limitations such as complex access policy management, high computational cost in large-scale networks, and limited adaptability to heterogeneous IoT devices.

Blockchain-Enhanced Privacy-Preserving Security Protocol for Cloud Environment Proposed System, 2026,The proposed system introduces a blockchain-enhanced privacy-preserving security protocol for secure cloud environments integrated with Digital Twin and IoT applications. The framework combines blockchain technology, AES-256 encryption, and SHA-256 hashing algorithms to provide confidentiality, integrity, authentication, and secure data sharing. Block chain is used to store immutable hash records of uploaded files and maintain transparent transaction logs for integrity verification .The protocol supports multiple entities such as Cloud Server, Data Owner, Data User, and Trace Authority. Data Owners upload encrypted files to the cloud, while authorized users can securely access files using secret keys.The system is designed to resist replay attacks, impersonation attacks, offline password guessing attacks, and unauthorized access attempts. Experimental results indicate improved security, reduced communication overhead, and efficient authentication compared to traditional cloud security protocols.

Blockchain-Based Data Security Framework for Cloud Storage Systems,M. Al-Bassam, A. Z. Al-Hamadi, et al,2022,This paper proposed a blockchain-based security framework to enhance data protection in cloud storage environments. The system integrates blockchain technology with cryptographic hashing techniques to ensure data integrity, transparency, and tamper resistance. Each data transaction and storage operation is recorded in a distributed ledger, which prevents unauthorized modifications and improves trust between users and cloud service providers. The framework also includes authentication mechanisms to verify user identity before granting access to cloud resources. Experimental results show that the system improves security and reliability in cloud storage while maintaining acceptable performance overhead. The study emphasizes that blockchain can significantly enhance trust and accountability in cloud-based systems.

Lightweight Blockchain-Based Security Protocol for Cloud and IoT Environments,S. Patel, R. Sharma, K. Mehta,2023, This work introduced a lightweight blockchain-based security protocol designed for cloud and IoT environments. The proposed system focuses on reducing computational overhead while maintaining strong security features such as authentication, data integrity, and access control. The framework uses blockchain for secure logging of transactions and AES-based encryption for protecting sensitive data. A simplified consensus mechanism is adopted to improve efficiency and reduce latency in cloud communication. The experimental evaluation demonstrates that the system performs efficiently in IoT-based cloud applications with improved response time and reduced energy consumption. The study highlights the suitability of lightweight blockchain models for resource-constrained environments.

III. EXISTING SYSTEM

In existing system it was by utilizing block chain technology and "elliptic curve cryptography (ECC)" to realize secure communication among legitimate users and conquer security flaws. The suggested framework's informal analysis ensures that the protocol is resilient to various security assaults, Using the ROR model and BAN logic, we also demonstrate that the existing scheme can assure "mutual authentication" and "'session key security' (Every time has same for long minutes. The computational and communication efficiency of the work is demonstrated by analyzing the presented work with the pre-existing authentication schemes. Another problem with this approach is the privacy of user data.

Disadvantages of Existing System

- Less Security and privacy for data.
- Takes more cost for storing data.
- The users can attack without authentication a data.

IV. PROPOSED SYSTEM

The proposed two-factor authentication protocol for DT environments that utilizes the block chain technology. We have a security offline password-guessing. The A suitable method for identifying the authenticity of a user is the usage of the user's comes a OTP through OTP information as an additional factor in an authentication system. The proposed framework assures data verification by utilizing block chain technology. Once Ur has received the requested data from Si, Ur can check the of data using the hash values stored in the block chain.The data we have converted in a three peers network to form a block chain.

Advantages of Proposed System:

- High Security and privacy for data.
- Takes less cost for storing data.
- The Project we have access control and authentication.

V. SYSTEM ARCHITECTURE

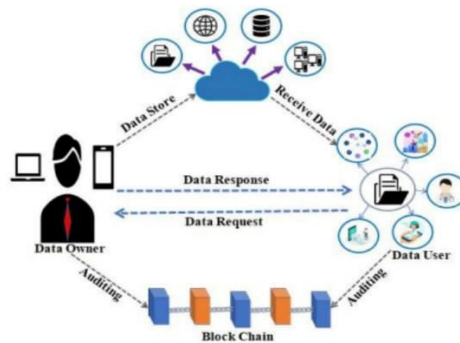


Fig 1.1 System Architecture

In this project, the Data Owner registers, logs in, uploads text files, and shares access keys with users. The Data User registers, logs in, requests permission, searches, and downloads data. The Trace Authority monitors and traces blockchain activities and data transactions. The Cloud Server maintains blockchain records, stores user and owner details, and manages all blockchain-based activities securely.

VI. METHODOLOGY

Modules Name:

- User Interface Desian
- Cloud Server
- Data Owner
- Data User
- Trace Authority

1) User Interface Design. In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must have their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2) Cloud Server: This is the first module of this project and he will be the Cloud server and has control over all the thing. In this module. Cloud server can a blockchain record data has stored in the database. Cloud server can have all data owner details. Cloud server can have a data user details Cloud server can have a blockchain activity data

3) Data Owner: This is the second module of this project. In this module data owner should be register then login. Data owner will upload the files stored in the database. Data owner will be see all the data request. Data owner should view all the request, from the users. Data owner should share the key to the user.

4) Data User: This is the third module of this project. In this module user need to register and then login. Then data user can search the files based on the file name. Data user can be see the responses from the user keys in database, After the keys it was download data.

5) Trace Authority: This is the fourth module of this project. In this module user need to login. Trace authority can trace a data in a block chain using a hash values. If the hash values match the data has shows in block chain.

VII. ANALYSIS AND DISCUSSION

The proposed system, Blockchain-Enhanced Privacy-Preserving Security Protocol for Cloud Environment is analysed in terms of security, efficiency, scalability, and practicality. The results obtained from implementation and experimental evaluation indicate that the system successfully addresses major limitations of existing searchable encryption techniques.

1. Security Analysis

The proposed system provides a strong and improved security framework compared to traditional cloud-based encryption schemes. It ensures privacy preservation by preventing unauthorized access to sensitive information stored in the cloud. The use of trapdoor encryption plays a crucial role in securing keyword searches, as it ensures that the cloud server cannot identify or infer the actual keywords used during the search process. This eliminates the risk of keyword leakage during query processing. Additionally, the integration of aggregate keys simplifies access control by allowing multiple encrypted files to be accessed using a single compact key, thereby reducing the complexity of key distribution and management. Overall, the system strengthens confidentiality, integrity, and access control while reducing vulnerabilities present in conventional searchable encryption systems

2. Performance and Efficiency

The performance of the proposed system is significantly improved due to the use of Key-Aggregate Searchable Encryption (KASE). Instead of managing multiple encryption keys for different files, the system uses a single aggregate key, which reduces both storage overhead and key management complexity. This makes the system more efficient, especially in environments where a large number of files are stored and shared. Keyword search operations are performed directly over encrypted data, eliminating the need for decryption before searching. This not only improves processing efficiency but also reduces computation time. As a result, the system achieves faster search responses and optimized resource utilization in cloud environments..

3. Scalability Analysis

The proposed cloud-based architecture is designed to support scalability and high-performance operations in large-scale environments. It can efficiently handle multiple users, large datasets, and concurrent search requests without significant degradation in performance. The system is suitable for modern applications such as IoT networks, enterprise data sharing platforms, and Digital Twin environments where data volume and user interactions continuously increase. The modular structure of the system ensures that additional users and data can be integrated easily without affecting the overall performance. This makes the system highly adaptable and future-ready for expanding cloud infrastructures.

4. Usability and Practical Implementation

From the results, the system provides a user-friendly interface to ensure ease of access for different types of users, including administrators, data owners, and authorized users. It provides essential functionalities such as secure user registration, file upload, keyword-based search, and secure file download. The admin approval mechanism ensures that only verified users can access the system, enhancing security and control. Data owners can easily upload encrypted files and manage access permissions, while users can efficiently search and retrieve required documents without dealing with complex cryptographic operations. This simplicity in design improves usability and makes the system practical for real-world deployment.

5. Comparison with Existing Systems

When compared with traditional searchable encryption systems, the proposed scheme offers significant improvements in security, efficiency, and usability. Unlike existing methods, the proposed system eliminates keyword privacy leakage by using secure trapdoor mechanisms that prevent the cloud server from learning search queries. It also provides stronger resistance against attacks such as keyword guessing and unauthorized access. Furthermore, the system reduces cryptographic overhead by using aggregate keys, which simplifies key management and improves operational efficiency. It also supports secure delegation of search capabilities, allowing users to safely outsource search operations to the cloud without compromising data privacy. Overall, the proposed system delivers a more secure, efficient, and scalable solution for cloud-based data management.

6. Discussion

Overall, the proposed Blockchain-Enhanced Privacy-Preserving Security Protocol for Cloud Environment provides a strong and efficient solution for securing cloud data. The system improves security by using encryption and blockchain technology to protect data from unauthorized access and tampering. It ensures data integrity through SHA-256 hashing and maintains confidentiality using AES-256 encryption. The use of blockchain helps in providing transparent and tamper-proof verification of cloud transactions, which increases trust in the system.

VIII. CONCLUSION

In this article, we examined various design flaws and vulnerabilities of the scheme suggested in [7] in opposition to numerous cryptographic attacks, like user impersonation, KSST IA, and offline password guessing attacks. By utilizing blockchain technology, we proposed an enhanced three-factor-based privacy-preserving authentication framework for the DT environment. The informal security analysis of the proposed scheme shows the efficiency and enhanced security against various wicked attacks. The mutual authentication and session key security is also ensured by performing the formal analysis of the proposed work using both the ROR Model and BAN logic. Moreover, compared to the competing existing works, the proposed method offers reduced computation costs, comparable communication costs, and superior security. Therefore, the proposed work is suitable for the DT environment.

IX. FUTURE ENHANCEMENT

In future, we would like to enhance the proposed scheme with more efficiency in terms of communication, computational and storage costs while keeping the same security level. In addition, we would also like to develop a complete testbed experiment for practical aspects of the proposed scheme.

REFERENCES

1. M.Grieves and J. Vickers, "Digital twini Mitigating unpredictable, undesirable emergent behavior in complex systems, " in Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Cham, Switzerland: Springer, 2017, pp. 85-113.
2. B.Piasek, J. Vickers, D.Lowry, S. Scotti, J. Stewart, and A. Calomino, "Materials, structures, mechanical systems, and manufacturing roadmap, " NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.
3. H. Laaki, Y. Miche, and K. Tammi, "Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery" IEEE Access, vol. 7, pp.20325-2033b, 2019.
4. H. Wang and J. Zhang, "Blockchain based data integrity verification for large-scale Iot data," IEEE Access, vol. 7, pp. 164996-165006, 2019.
5. P. Wei, D. Wang, Y.Zhao, S.K.S. Tyagi, and N. Kumar, "Blockchain datarbased cloud data integrity protection mechanism Future Gener. Comput.Syst, vol. 102, pp.902-911, Jan. 2020.
6. B. Liu, X.L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data, " in Proc. IEEE Int. Conf. Web Services (ICWS), Tum. 2017, pp. 468-475.
7. S.Son, D. Kwon, J.Lee, s. Yu, N.-S. Tho, and Y. Park, "On the design of a privacy preserving communication scheme for cloud-based digital twin environments using blockchain, "IEEE Access, val. 10, pp.75365-75375, 2022.
8. T.Y. Wu, Y.-Q.Lee, c-M. Chen, Y. Tian, and N. A. AL-Ndbhan, "An ehanced pairing-based authentication scheme for smart grid communications,:" J, Ambient Intell. Humanized Compute vol. 2021, pp. 1-13, Jan. 2021.
9. Is. Khalon, s. ML M.Rolnmwaon, M. Alrulbaian, and A Mlamri, "Privacy reserved, proueble secure, mutually authenticated key agreement pratacadl for healthcare in a smart city environment, " IEEE Access, vol. 7, pp.47962-47971, 2019.
10. A.Sengupta, A. Singh, P. Kumar, and T. Dhar, "A secure and improved two factor authentication scheme using alliptic curve and bilinear pairing for cyber physical systems, "Multimedia Tools Appl., vol. 16, pp. 1-24, Jul. 2022.
11. H.S.Grover and D. Kumar, "Cryptanalysis and improvement of a three factor user authentication scheme for smart grid environment, " J. Reliable Intell. Emviron, vol. 6, no. 4, pp.249-260, Dec. 2020.
12. M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three factor user authentication scheme for renewable-energy-based smart grid environment, " IEEE Trans. Ind Informat., vol. 13, no. 6, pp. 3144-3153, Dec. 2017.
13. D.Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home, " J. Inf. Secure. Appl., vol. 58, May 2021, Art. no. 102787.[14] M. Shuai, N. Yu, H. Wang, and L. Xiong,

“Anonymous authentication scheme for smart home environment with provable security, " Comput. Secur, vol. 86, pp. 132-146, Sep.2019.

14. Y. Chen, I. Martinez, P. Castillejo, and L. López, “A bilinear map pairing based authentication scheme for smart grid communications: Pauth, "" IEEE Access, vol. 7, pp. 22633-22643, 2019.
15. S. Roy, S. Chatterjee, A. K. Das, S. Chatopadhyay, N. Kumar, and A V. Vasilakos, “On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services, " IEEE Access, vol. 5, pp. 25808-25825, 2017



International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 9.971