Enhancing Secure Communications In The Cloud Through Block Chain Assisted -CP-DABE

R.Gopi[1], Jayasanthiya S[2], Kamali R[3], Kaviya B[4]
[1]HOD, Dept of CSE
[2, 3, 4]Dept of CSE
[1, 2, 3, 4] Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu, India.

Abstract- *As cloud computing becomes increasingly integral to modern data management and communication, ensuring secure and fine-grained access control remains a pressing challenge. This paper proposes a novel framework that enhances cloud communication security by integrating Blockchain-assisted Ciphertext-Policy Decentralized Attribute-Based Encryption (CP-DABE). The proposed model leverages the decentralized nature of blockchain to eliminate reliance on a single trusted authority, thus enhancing trust, auditability, and resistance to key escrow and collusion attacks. CP-DABE enables fine-grained access control based on user attributes, while blockchain ensures transparent and tamper-proof management of attribute authorities and access policies. Our solution supports scalable, decentralized key distribution, and secure data sharing in dynamic cloud environments. Experimental analysis demonstrates that the system achieves robust security with minimal performance overhead, making it a practical and effective approach for secure, decentralized cloud communication.*

Keywords- Fine-grained access control, CP-DABE, Collusion attacks ,Decentralized key distribution, Robust security.

I. INTRODUCTION

Cloud computing has revolutionized the way individuals and organizations store, process, and share data by offering scalable, flexible, and cost-effective infrastructure. However, the convenience of the cloud also brings significant security and privacy concerns, particularly when it comes to sensitive data and communication across untrusted or distributed environments. Traditional encryption methods often fall short in providing fine-grained access control, scalability, and resistance to insider threats, especially when centralized authorities are involved.

To address these challenges, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has emerged as a promising solution, allowing data owners to define access policies over encrypted data. However, conventional CP-ABE schemes typically rely on a single trusted authority, making them vulnerable to single points of failure, key escrow problems, and scalability limitations.

To overcome these issues, this work introduces an enhanced approach: Blockchain-Assisted Ciphertext-Policy Decentralized Attribute-Based Encryption (CP-DABE). By integrating blockchain technology with CP-DABE, we harness the decentralized, immutable, and transparent nature of blockchain to distribute trust among multiple attribute authorities and ensure secure, verifiable key distribution and access control. The blockchain acts as a tamper-resistant ledger that records attribute issuance, revocation, and policy enforcement, thereby eliminating the need for centralized control and improving system resilience.

The widespread adoption of cloud computing has brought unparalleled flexibility and scalability to data storage and processing. However, as more individuals and organizations migrate their sensitive data to the cloud, concerns surrounding data confidentiality, integrity, and secure access control have grown significantly. Traditional security models often rely on centralized entities to manage encryption keys and enforce access policies, making the entire system vulnerable to single points of failure, insider threats, and unauthorized access. These limitations highlight the need for a more robust and decentralized approach to cloud security that can ensure fine-grained data access without sacrificing performance or trust.

This paper presents the design, implementation, and evaluation of a blockchain-assisted CP-DABE scheme tailored for secure communications in cloud environments. The proposed framework ensures fine-grained, decentralized access control while preserving data confidentiality and integrity, even in dynamic and adversarial settings. Throughsecurity analysis and performance evaluation, we demonstrate that our approach achieves enhanced privacy, reduced risk of key compromise, and improved scalability for cloud-based applications.

II. RELATED WORK

The development of secure communication frameworks in the cloud has significantly evolved with the introduction of advanced cryptographic techniques and distributed ledger technologies. Numerous research efforts have examined the integration of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with blockchain to overcome traditional challenges in data security, access control, and trust management in cloud environments.

2.1 Enhancing Cloud Data Security Using CP-DABE

Attribute-Based Encryption in Cloud Security Attribute-Based Encryption (ABE) schemes, especially CP-ABE, have gained prominence for enforcing fine-grained access control. In CP-ABE, the data owner defines an access policy, and only users whose attributes satisfy this policy can decrypt the data. Research by Bethencourt et al. (2007) laid the foundational framework for CP-ABE, while later enhancements focused on reducing computational complexity and supporting multi-authority systems.

2.2 Blockchain Integration in Cloud Communication

Blockchain Integration in Cloud Communication Blockchain offers a tamper-proof, decentralized platform that enhances trust, transparency, and immutability. Its integration with CP-ABE addresses key management issues, ensuring verifiable access rights and auditability. Several studies have proposed blockchain-based access control frameworks, highlighting their resilience against internal and external attacks.

2.3Limitations and Challenges in Traditional CP-ABE Schemes

Limitations in Traditional CP-ABE Schemes Despite its advantages, traditional CP-ABE suffers from limitations such as heavy computation on user devices, single-point trust assumptions, and scalability issues. Efforts have been made to offload computation to the cloud, but this introduces trust issues. Hybrid frameworks that utilize edge computing or proxy re-encryption mechanisms have shown promise in mitigating these challenges.

2.4 Decentralized Access Control Models Using Blockchain and Smart Contracts

Decentralized Access Control Models Decentralized models leveraging blockchain and smart contracts offer automated enforcement of access policies without centralized authorities. Recent work explores combining smart contracts with CP-ABE to manage attribute keys and revocation lists in a transparent and verifiable manner.

2.5 Enhanced Key Management in Secure Communication Using Blockchain

Enhanced Key Management Using Blockchain Effective key distribution and revocation remain critical in secure communication. Blockchain-based key management systems (KMS) have been proposed to maintain the integrity and availability of cryptographic keys, allowing secure updates, revocations, and auditing. These systems improve resilience and reduce reliance on central trusted entities.

III. PROPOSED SYSTEM

This section outlines the architecture and functioning of the proposed secure cloud communication system that leverages blockchain technology to enhance Ciphertext-Policy Decentralized Attribute-Based Encryption (CP-DABE). The proposed system ensures fine-grained access control, user privacy, and traceability without relying on a centralized authority.

3.1 System Architecture

The proposed system architecture is composed of five primary entities: Data Owners (DOs), Data Users (DUs), Attribute Authorities (AAs), Cloud Service Provider (CSP), and a Blockchain Network. Data Owners are responsible for encrypting sensitive data and uploading it to the cloud, while Data Users request access to that encrypted data based on their attributes. Multiple Attribute Authorities operate independently to issue keys based on verified attributes without relying on a centralized entity. The Cloud Service Provider stores the encrypted data but is not trusted with decryption capabilities. A permissioned blockchain serves as the backbone for storing public parameters, credential issuance logs, and transaction metadata, thereby enabling trust and transparency across the system.

3.2 CP-DABE Integration

To enable fine-grained access control, the proposed system adopts Ciphertext-Policy Decentralized Attribute-Based Encryption. In this model, the Data Owner defines an access policy and embeds it within the ciphertext. Only Data Users whose attribute sets satisfy the embedded policy can decrypt the data. Unlike traditional CP-ABE schemes, CP-DABE allows for the involvement of multiple independent Attribute Authorities, thereby eliminating the risk of a single

point of failure and enhancing system robustness. Each user can obtain attribute keys from different authorities, supporting a fully decentralized trust model

3.3 Blockchain-Assisted Key Management

Blockchain plays a vital role in the secure and transparent management of attribute keys. Each Attribute Authority registers its public keys and credentials on the blockchain, which serves as an immutable and verifiable ledger. Attribute issuance, revocation, and verification are all governed by smart contracts deployed on the blockchain. This ensures that Data Users and Data Owners can verify the authenticity of attribute keys without needing to directly trust any single authority. Moreover, the decentralized ledger prevents issues such as duplicate attribute issuance and collusion between malicious authorities.

3.4 Data Encryption and Upload

In the data encryption phase, the Data Owner first defines an access control policy over a set of attributes. The data is then encrypted using the CP-DABE encryption algorithm, which binds the policy to the ciphertext. The encrypted data is uploaded to the Cloud Service Provider, ensuring that the CSP cannot read or misuse the content. Additionally, a hash of the policy, along with relevant metadata such as timestamps and Data Owner identifiers, is recorded on the blockchain. This step ensures tamper-evident logging and traceability for future access audits.

3.5 Data Access and Decryption

When a Data User wishes to access encrypted data, they query the blockchain to retrieve the relevant access policy and verify its integrity. If their attribute set matches the required policy, they can use the attribute keys obtained from the respective Attribute Authorities to decrypt the data. The decryption process is enabled only after the smart contract validates the authenticity and freshness of the user's credentials. Once decryption is successful, an audit log of the access event is automatically written to the blockchain, ensuring transparency and accountability in data access.

3.6 Security and Efficiency Considerations

The proposed system offers several security and performance advantages. Fine-grained access control is achieved through CP-DABE, supporting complex access policies and multiple authorities. Decentralization eliminates the need for a single trusted entity, while blockchain ensures transparency and traceability in credential management and data access. The use of smart contracts prevents unauthorized access and attribute mismanagement. Furthermore, the system design minimizes blockchain overhead by storing only metadata on-chain, while encrypted data remains off-chain in the cloud, thereby improving scalability and operational efficiency.

IV. SYSTEM DESIGN

This section delves deeper into the detailed design and implementation of the proposed system, which integrates blockchain technology with Ciphertext-Policy Decentralized Attribute-Based Encryption (CP-DABE). The aim is to offer a secure, decentralized approach to cloud communications, ensuring privacy, fine-grained access control, and accountability in the management and access of sensitive data.

4.1 System Architecture Overview

The architecture of the proposed system is composed of several interacting components designed to work in a decentralized and secure environment. These components include Data Owners, Data Users, Attribute Authorities, Cloud Service Providers, and a Blockchain Network. The Data Owners encrypt their data using the CP-DABE scheme and upload it to the cloud. Data Users, based on their attributes, request access to encrypted data. Attribute Authorities are responsible for issuing and managing the attributes that determine access rights. The Cloud Service Provider hosts the encrypted data but does not have access to the plaintext. Blockchain acts as a decentralized ledger to securely store keys, policies, and access logs, ensuring transparency and integrity across the system. The overall system design emphasizes decentralization, ensuring that no single entity has full control over access rights or data, thereby enhancing the security and trustworthiness of the system..

4.2 Blockchain-Integrated Key Management

In the proposed system, blockchain technology plays a pivotal role in the management of attribute keys and policy information. Attribute Authorities register their public parameters, including the public keys for encrypting and decrypting attribute-based data, on the blockchain. This decentralized approach allows Data Users to independently verify the authenticity and validity of the attribute keys they receive. Blockchain guarantees that any updates, revocations, or alterations to the attribute keys or policies are transparent, auditable, and tamper-resistant. Smart contracts are used to automate the processes of key issuance, verification, and revocation, ensuring that access control policies are enforced without the need for manual intervention. By storing policy-related metadata and credentials on the blockchain, the system

eliminates the risks associated with centralized management systems and enhances accountability.

4.3 Secure Data Upload and Storage

Data Owners initiate the secure data upload process by first defining an access control policy based on a set of attributes that represent the conditions for granting access to their data. This policy is integrated into the encryption process using the CP-DABE scheme. The data is then encrypted using the policy and uploaded to the Cloud Service Provider. Importantly, the cloud service provider stores the encrypted data without having access to its plaintext form, preserving confidentiality. To further enhance security, a hash of the access control policy and relevant metadata is recorded on the blockchain, ensuring that the integrity of the policy can be verified at any point in the future. This step guarantees that data access is governed by the correct policy, which cannot be altered without detection.

4.4 Data Access and Decryption Process

When a Data User seeks to access the encrypted data, they first query the blockchain to retrieve the policy hash and metadata associated with the data. The system then checks whether the user's attributes match the policy specified by the Data Owner. If the attributes satisfy the conditions of the policy, the user is granted access to the decryption keys issued by the Attribute Authorities. Decryption is performed using the CP-DABE decryption algorithm, which ensures that only authorized users with the appropriate attributes can decrypt the data. Smart contracts on the blockchain validate the authenticity of the attribute keys before allowing the decryption process to proceed, ensuring that no unauthorized access can occur. Furthermore, each decryption attempt is logged on the blockchain, creating a permanent, auditable record of all access events.

4.5 Privacy and Security Enhancements

The integration of blockchain with CP-DABE provides several privacy and security enhancements. First, the use of CP-DABE enables fine-grained control over who can access data, as the data owner can specify complex access policies based on multiple attributes. Second, blockchain technology ensures that all interactions—such as key issuance, policy updates, and data access—are transparent and auditable. This transparency discourages malicious activities, as all actions are recorded immutably on the blockchain. Third, the decentralized nature of the system mitigates the risks associated with a single point of failure, as no single authority has full control over the keys or data. Finally, the use of smart contracts guarantees that policies are enforced automatically, reducing the potential for human error or malicious interference

4.6 Performance and Scalability Considerations

In terms of performance and scalability, the proposed system is designed to handle large-scale cloud environments efficiently. While the blockchain provides enhanced security and transparency, it is also optimized to store only essential metadata—such as policy hashes, transaction logs, and public keys—rather than large volumes of data. This reduces the computational burden on the blockchain and minimizes network congestion. Additionally, the use of decentralized Attribute Authorities ensures that the system can scale by distributing the key management process, allowing for seamless integration of new authorities and users. The use of off-chain storage for the encrypted data further optimizes the system's performance, ensuring that it can handle large datasets without compromising security or efficiency.

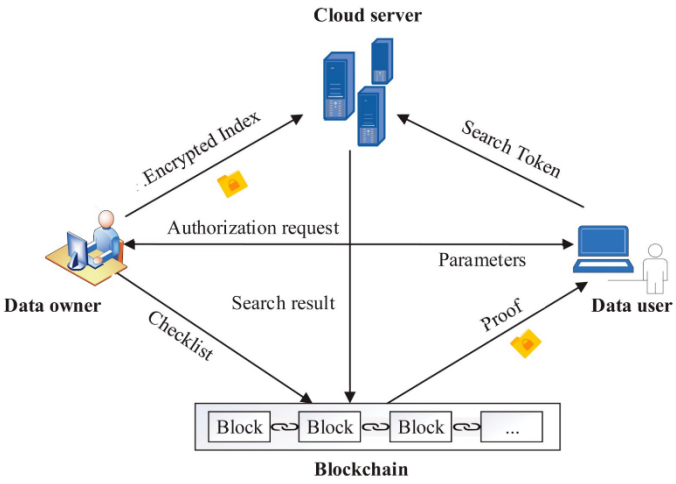

Fig 4.1 System Architecture

V. CONCLUSION

This research introduces a secure, decentralized framework that combines Blockchain technology with Ciphertext-Policy Decentralized Attribute-Based Encryption (CP-DABE) to enhance communication security in cloud environments. The proposed system addresses major limitations of existing cloud security solutions, particularly those that depend heavily on centralized authorities for key management and access control. By adopting a decentralized model, the system distributes trust among multiple Attribute Authorities, significantly reducing risks related to single points of failure and centralized attacks.

Through CP-DABE, the system enables fine-grained access control by allowing data owners to define encryption

policies based on user attributes. Only users possessing the correct set of attributes can decrypt the data, ensuring that sensitive information remains confidential and is accessed only by authorized parties. This capability is crucial in modern cloud systems where users vary in roles, privileges, and responsibilities. Additionally, decentralized attribute management strengthens the system's scalability, flexibility, and resistance to collusion attacks.

The incorporation of blockchain further enhances the system's security, transparency, and accountability. Blockchain serves as an immutable ledger that stores public keys, attribute credentials, access policies, and user interactions. Smart contracts are used to automate key operations such as attribute issuance, revocation, and policy enforcement, eliminating the need for manual intervention and ensuring consistent, rule-based execution. This ensures that access decisions are verifiable and traceable, fostering greater trust among cloud users.

In conclusion, the Blockchain-Assisted CP-DABE framework represents a significant step toward building secure, privacy-preserving, and transparent cloud environments. It effectively combines the strengths of decentralized encryption and blockchain to achieve robust access control, data confidentiality, and verifiable user behavior. This work lays the foundation for future improvements, including real-time performance optimization, support for dynamic attributes, and integration with emerging technologies such as edge computing and cross-chain blockchain platforms.

REFERENCES

[1] S. Yaji, K. Bangera, and B. Neelima, ''Privacy preserving in blockchainbased on partial homomorphic encryption system for ai applications,'' inProc. IEEE 25th Int. Conf. High Perform. Comput. Workshops (HiPCW),Dec. 2018, pp. 81–85.

[2] P. P. Nayudu and K. R. Sekhar, ''Accountable specific attribute-basedencryption scheme for cloud access control,'' Int. J. Syst. Assurance Eng.Manage., vol. 2022, pp. 1–10, Jul. 2022.

[3] Y. Yang, M. Hu, Y. Cheng, X. Liu, and W. Ma, ''Keyword search-able encryption scheme based on blockchain in cloud environment,''in Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock), Oct. 2020,pp. 1–4.

[4] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, ''Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks forcloud storage,'' IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1335–1348,Oct. 2021.

[5] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, ''BC-SABE: Blockchain-aided searchable attribute-based encryption forcloud-IoT,'' IEEE Internet Things J., vol. 7, Sep. 2020.

[6] S. Tahir and M. Rajarajan, ''Privacy-preserving searchable encryptionframework for permissioned blockchain networks,'' in Proc. IEEEInt. Conf. Internet Things (iThings) IEEE Green Comput. Commun.(GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE SmartData (SmartData), Jul. 2018.

[7] S. Jiang, J. Cao, J. A. McCann, Y. Yang, Y. Liu, X. Wang, and Y. Deng,''Privacy-preserving and efficient multi-keyword search over encrypteddata on blockchain,'' in Proc. IEEE Int. Conf. Blockchain (Blockchain),Jul. 2019.

[8] X. Yan, X. Yuan, Q. Ye, and Y. Tang, ''Blockchain-based search-able encryption scheme with fair payment,'' IEEE Access, vol. 8,pp. 109687–109706, 2020.

[9] B. Chen, D. He, N. Kumar, H. Wang, and K. R. Choo, ''A blockchain-based proxy re-encryption with equality test for vehicular communicationsystems,'' IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2048–2059,Jul. 2021.

[10] J. Han, Z. Li, J. Liu, H. Wang, M. Xian, Y. Zhang, and Y. Chen, ''Attribute-based access control meets blockchain-enabled searchable encryption:A flexible and privacy-preserving framework for multi-user search,''Electronics, vol. 11, no. 16, p. 2536, Aug. 2022.

[11] S. Wang, X. Wang, and Y. Zhang, ''A secure cloud storage framework with access control based on blockchain,'' IEEE Access, vol. 7,pp. 112713–112725, 2019.

[12] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, ''An integratedarchitecture for maintaining security in cloud computing based onblockchain,'' IEEE Access, vol. 9, pp. 69513–69526, 2021.

[13] M. Whaiduzzaman, Md. J. N. Mahi, A. Barros, Md. I. Khalil, C. Fidge,and R. Buyya, ''BFIM: Performance measurement of a blockchain basedhierarchical tree layered fog-IoT microservice architecture,'' IEEE Access,vol. 9, pp. 106655–106674, 2021.

[14] Y. Sun, X. Li, F. Lv, and B. Hu, ''Research on logistics informationblockchain data query algorithm based on searchable encryption,'' IEEEAccess, vol. 9, pp. 20968–20976, 2021.

[15] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, ''Flexibleand efficient blockchain-based ABE scheme with multi-authority formedical on demand in telemedicine system,'' IEEE Access, vol. 7,pp. 88012–88025, 2019.

[16] S. Alqahtani and M. Demirbas, ''Bottlenecks in blockchain consensprotocols,'' in Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS),Aug. 2021, pp. 1–8.

[17] S. Liu, J. Yu, L. Chen, and B. Chai, ‘‘Blockchain-assisted comprehensivekey management in CP-ABE for cloud-stored data,’’ IEEE Trans. Netw.Service Manage., vol 20, no. 2, pp. 1745–1758, Jun. 2023.
[18] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, 321–334.
[19] Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. IEEE INFOCOM, 1–9.
[20] Wang, H., Liu, D., & Wu, J. (2017). Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. IEEE Transactions on Cloud Computing, 5(4), 720–732.
[21] Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. IEEE Cloud, 268–275.
[22] Liu, Y., Yang, K., & Wang, X. (2019). Blockchain-based access control model for electronic health records in cloud environments. Journal of Medical Systems, 43(1), 27.
[23] Mollah, M. B., Zhao, J., &Niyato, D. (2021). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, 8(1), 18–43.
[24] Xu& Zhang, Z. (2019). Blockchain-based access control system for the internet of things. IEEE Access, 7, 129433–129444.
[25] Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2013). Secure deduplication with efficient and reliable convergent key management. IEEE Transactions on Parallel and Distributed