Server security in cloud computing by using Blockchain

[1]BUSHRA MUNEEB, [2]KEERTHANA, [3]D.ANJALI, [4]BHAVANI,[5]KAVYA

[1] Assistant Professor, Department of Artificial Intelligent &Machine Learning , Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5] B.Tech Students, Department of Artificial Intelligent &Machine Learning , Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

Cloud computing has revolutionized how data and applications are hosted, stored, and accessed. However, the centralized architecture of traditional cloud systems makes them vulnerable to cyber threats such as unauthorized access, data breaches, and insider attacks. This project, titled **"Server Security in Cloud Computing Using Blockchain"**, proposes a decentralized security framework where Blockchain technology is integrated with cloud servers to ensure immutability, transparency, and enhanced trust. By using a distributed ledger system, all server access events and data transactions are logged securely and can be verified without reliance on a central authority. Smart contracts are employed to automate access control, authentication, and auditing, making the server infrastructure more resilient to cyberattacks. The integration of blockchain offers a tamper-proof and trustless environment for critical cloud-based applications.

I.INTRODUCTION

As enterprises shift toward cloud computing for scalability and flexibility, securing server infrastructure becomes increasingly complex. Centralized cloud architectures, while efficient, present single points of failure and are susceptible to insider threats, hacking attempts, and data tampering. Conventional authentication methods and access control systems are no longer sufficient in ensuring the integrity and confidentiality of critical information in a shared cloud environment.

Blockchain technology, known for its decentralized, transparent, and tamper-proof nature, provides a promising solution to address these issues. In this project, we propose a blockchain-based server security model where each server access, configuration change, or data transaction is recorded on an immutable blockchain ledger. This ensures traceability and accountability while eliminating reliance on centralized security mechanisms. By combining smart contracts for automated access control and real-time logging on blockchain, the system enhances cloud server security in a robust and

scalable manner**.**

II.LITERATURE SURVEY

1. Xia et al. (2017) proposed a blockchain-based data sharing scheme in cloud storage, demonstrating how blockchain can ensure integrity and traceability in decentralized systems. They emphasized the role of smart contracts in policy enforcement.
2. Zyskind et al. (2015) developed a secure personal data management system using blockchain. Their research showed how blockchain could be used for decentralized identity verification and user-centric data access in cloud-based applications.
3. Al-Bassam (2018) suggested the use of blockchain for decentralized logging in distributed systems. Their model showed how logs could be made tamper-proof and more reliable compared to traditional server-based logging systems.
4. Kshetri (2018) presented a comprehensive review of blockchain's role in cybersecurity and its potential to disrupt traditional security models in cloud infrastructure. It highlighted blockchain's ability to enhance trust and decentralization.
5. Zhang and Lin (2019) discussed blockchain-based access control models for cloud environments. Their study evaluated the feasibility of smart contracts in controlling and auditing data access across multiple users.
6. Ouaddah et al. (2017) proposed FairAccess, a blockchain-based access control protocol for IoT and cloud. It introduced the concept of decentralized authorization tokens, which can also apply to server access control.
7. Singh & Kim (2020) developed a blockchain framework for securing multi-cloud environments. Their system supported role-based access controls and blockchain-based auditing.
8. Yuan et al. (2021) used blockchain to secure cloud logging and auditing, showing a drastic improvement in log integrity and incident traceability.
9. Rahman et al. (2019) focused on integrating blockchain into cloud security for small businesses, proposing a lightweight architecture with Ethereum smart contracts for logging user activity.
10. Moinet et al. (2017) emphasized blockchain's resistance to insider threats, one of the biggest challenges in cloud environments. Their decentralized models reduce the risk of rogue admins altering logs or bypassing access controls.

III.EXISTING SYSTEM

Current server security systems in cloud computing rely heavily on centralized access control, password-based authentication, and manual logging systems. While service providers use encryption, firewalls, intrusion detection systems (IDS), and multi-factor authentication (MFA), these measures are not always sufficient to prevent sophisticated attacks such as privilege escalation, insider threats, and log tampering. Centralized logging servers are themselves vulnerable to being modified or deleted by attackers. Moreover, cloud clients must trust the provider's infrastructure, which may lead to concerns about data transparency and accountability, especially in multi-tenant or public cloud environments.

IV.PROPOSED SYSTEM

The proposed system introduces Blockchain-based server security in cloud computing environments to eliminate single points of failure and establish trust without intermediaries. Each server access attempt, file upload, system command, or authentication event is logged into a decentralized blockchain ledger, making it immutable and verifiable. Smart contracts define rules for access control, ensuring that only authorized users or services can interact with the cloud server. The use of public key cryptography and digital signatures enhances authentication and non-repudiation. In case of any breach attempt, the blockchain provides forensic evidence of who accessed what, when, and how. The architecture is designed to be cloud-agnostic and can integrate with platforms like AWS, Azure, or Google Cloud. This system significantly enhances auditability, trust, and accountability in managing cloud servers.

V.SYSTEM ARCHITECTURE

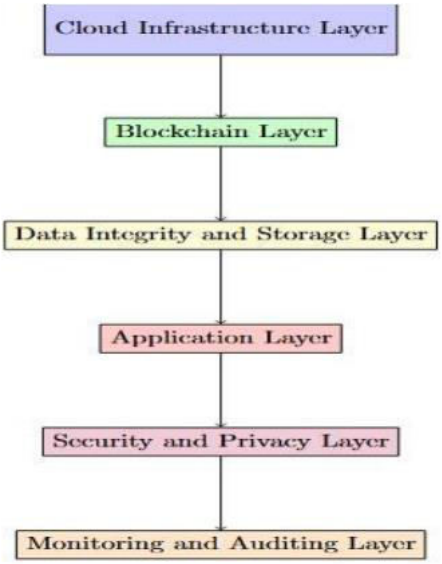

Fig 5.1 System Architecture

The system architecture integrates cloud infrastructure, blockchain networks, and smart contracts to ensure secure, decentralized, and immutable server access control and logging

VI.IMPLEMENTATION

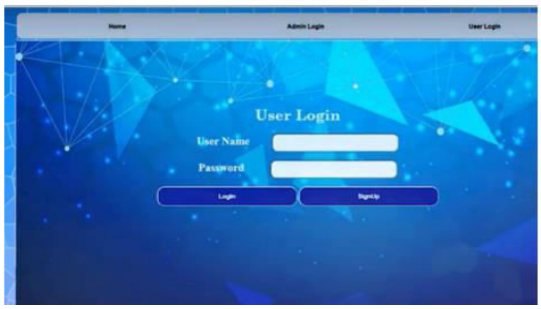

Fig 6.1 User Login

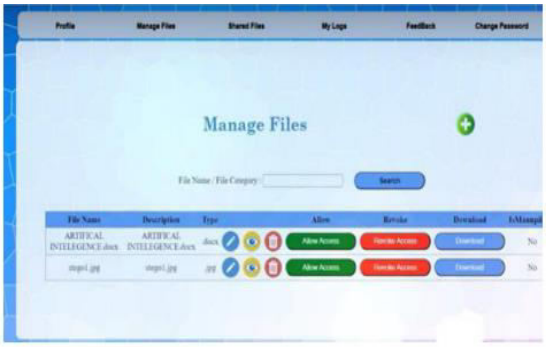

Fig6.2 :ManageFiles

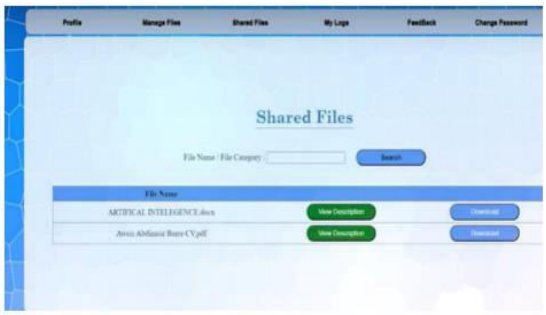

Fig 6.3 Fig3: Shared Files

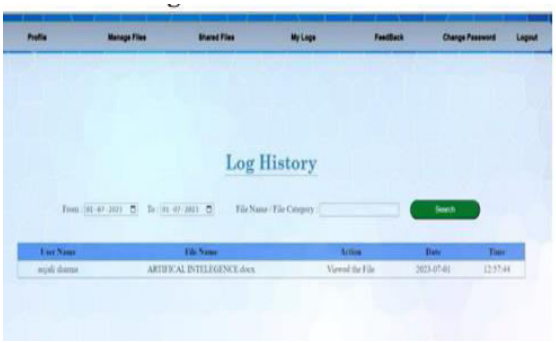

Fig 6.4 Log History

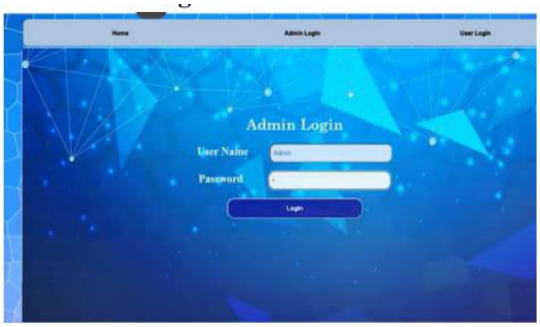

Fig 6.5 Admin Login

VII.CONCLUSION

The Server Security in Cloud Computing Using Blockchain project presents a forward-looking approach to overcoming the inherent limitations of centralized security architectures in cloud environments. By utilizing blockchain's core features—decentralization, immutability, transparency, and distributed consensus—this system ensures that all access logs and server interactions are verifiable and tamper-proof. Smart contracts automate and enforce access policies, reducing human error and insider threats.

As data breaches, system compromises, and unauthorized accesses continue to rise, traditional security mechanisms must evolve. This project demonstrates how blockchain can serve not only as a data integrity layer but also as a foundation for building trustless and secure cloud ecosystems. With further research and optimization, blockchain-based server security can be seamlessly integrated into enterprise-grade cloud infrastructure,

enhancing digital trust and resilience in the next generation of cloud computing.

VIII.FUTURE SCOPE

- The integration of blockchain in cloud server security opens new avenues for innovation and enhancement:
- AI-Powered Intrusion Detection: Combining blockchain with AI-based threat prediction models to detect abnormal access patterns in real time.
- Decentralized Identity (DID): Implementation of blockchain-based identity management to completely eliminate password-based authentication.
- Cross-cloud Security Ledger: A unified blockchain ledger that spans across multiple cloud providers for unified access tracking and auditing.
- Integration with IoT and Edge Devices: Securing cloud-connected IoT servers using lightweight blockchain nodes.
- Zero Trust Architecture (ZTA): Developing a blockchain-enhanced ZTA model where every request is validated and logged immutably.
- Federated Smart Contracts: Enable inter-organization policies in hybrid cloud environments using collaborative blockchain contracts.

IX.REFERENCES

1. Xia, Q., et al. (2017). A Blockchain-Based Data Sharing Scheme for Cloud Storage. IEEE Access.
2. Zyskind, G., et al. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE S&P.
3. Al-Bassam, M. (2018). Scalable Secure Logging for Distributed Systems. arXiv.
4. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. IJIM.
5. Zhang, Y., & Lin, X. (2019). Blockchain-Based Access Control for Cloud Data. Future Generation Computer Systems.
6. Ouaddah, A., et al. (2017). FairAccess: Blockchain-based access control framework. Journal of Internet Services and Applications.
7. Singh, S., & Kim, S. (2020). Security and Privacy of Blockchain in Multi-Cloud Computing. IEEE Access.
8. Yuan, Y., et al. (2021). Cloud Audit Logs via Blockchain. Springer.
9. Rahman, M., et al. (2019). Lightweight Blockchain Framework for Small Business Cloud Security. ACM.