International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

A Centralized Cloud Security Storage System Using Blockchain Technique

K.A.S.L.U. Maheswari[1], Gugulothu Mythili[2], Jitta Rithika Reddy[3], Kolipaka Vineeth Nihal[4]
[1,2,3,4]IV year Students, dept.ofAIML, Malla Reddy EngineeringCollege, Hyderabad,Telangana,India

Abstract- This study introduces a Blockchain-Based Zero Trust Network Access (ZTNA) solution that is designed to solve security problems caused by the centralised design of cloud storage systems, like data leaks, unauthorised access, and reliance on third-party providers. It uses blockchain, specifically Ethereum, along with the Zero Trust approach of "never trust, always verify" to create a secure, transparent, and unchangeable access control system. Smart contracts written in Solidity automate authentication, permission checks, and access validation, while AES encryption ensures strong protection for sensitive information in the cloud. The system sorts files into public and private groups based on user roles, and all access requests, permission changes, and activity logs are permanently stored on the blockchain, making it easier to keep track of who did what and when. The system's lack of central control reduces the risk of failures, increases dependability, and builds confidence among users. The system is meant to be scalable, work with mixed cloud setups, and could be linked to future security tools like advanced threat detection systems. In general, this solution offers a secure, checkable, and reliable platform for managing valuable digital assets in today's environment.

Keywords – Zero Trust Network Access, Blockchain, Security, Decentralized Identity, Access Control, Data Encryption.

I. INTRODUCTION

The old "castle-and-moat" security model is no longer effective in today's digital environment because of the widespread use of cloud computing, remote work, and distributed systems. These traditional methods assume that people inside the organisation can be trusted, which leads to vulnerabilities like insider threats, misuse of credentials, and attacks that move laterally through the network. As cyber threats become more complex, organisations need better, more flexible and adaptable security strategies to protect sensitive data and systems. To tackle these issues, the Zero Trust Network Access (ZTNA) model has become a modern security approach that treats every access request as potentially risky. It checks authentication, permission, and validation continuously, no matter where the user is, what device they're using, or which network they're on. This limits implicit trust and greatly lowers the chances of unauthorised access. However, many ZTNA systems still depend on central identity providers and policy enforcement servers.

These central parts can become weak points that attackers can exploit. If they are compromised, they might expose sensitive data, break services, and harm the security setup.This project overcomes these issues by combining blockchain with the ZTNA architecture to decentralise identity management, access control, and activity tracking. Using Ethereum's distributed blockchain and Solidity-based smart contracts, trust is shared across a peer-to-peer network instead of relying on a single central authority. The decentralised approach ensures that access rights, authentication records, and system logs are stored in a way that cannot be altered, which improves reliability, reduces risks from central failures, and boosts overall security. The blockchain layer also gives secure audit trails, allowing organisations to track access activities accurately and meet legal requirements.

The proposed system is scalable, robust, and verifiable, making it suitable for modern network security. It follows the principle of least privilege, giving access only when certain conditions are met, which lowers exposure to cyber threats. Encryption ensures data confidentiality, while smart contracts automate tasks, reducing the need for manual work and human mistakes.In total, combining Zero Trust with blockchain technology improves transparency, accountability, and efficiency. This approach marks a significant improvement in building secure, decentralised access control systems that protect sensitive digital assets while keeping trust, compliance, and security intact in more complex cloud and remote work environments.Making security systems easy to use is crucial for their adoption, especially in places where both technical and non-technical users access digital resources. Traditional security tools often involve complicated setups, centralised control, and manual enforcement, increasing workloads and reducing efficiency. In contrast, the Blockchain-Based ZTNA system is designed to be user-friendly while maintaining strong security.

By combining blockchain and automated smart contracts, it simplifies authentication, access control, and monitoring without needing advanced technical skills. Using decentralised identity verification and automated policy enforcement reduces the need for manual decisions, allowing users to securely access resources with less setup while still meeting strict security requirements. Classifying files into public and private groups makes it easier for administrators to manage permissions while ensuring appropriate access control and data protection. Immutable blockchain logs give clear visibility into access activities, making auditing and problem-solving straightforward without the need for complex tools. The system has a simple interface, letting users upload, check, and access data with minimal effort. Automation through smart contracts ensures consistent enforcement of rules, reducing human errors and delays. The decentralised architecture also improves reliability and availability by removing single points of failure, ensuring continuous access even if parts of the system fail. Overall, the blockchain-based ZTNA system balances high security with ease of use through automation, transparency, and shared trust, making it suitable for real-world use in cloud and distributed environments where secure and convenient access is essential.

II. LITERATURE REVIEW

The BeyondCorp project [1] by Google changed how businesses protect their networks by moving away from the old idea of securing everything around a company's network. Instead, it checks each user and device carefully before letting them access company resources. It doesn't assume everyone inside the network is safe. This approach removes the need for traditional tools like VPNs and firewalls and uses smart methods to check who is accessing what and under what conditions. It focuses on checking user identities, making sure devices are safe, and keeping track of access requests in real time [2]. The guide helps organizations change from old, fixed security methods to more flexible, smart security setups. It also explains how to mix Zero Trust with current systems by improving identity management and access rules. These best practices have made real-world use of ZTNA more practical and easier to set up. A. Dorri et.al, [3] can improve access control systems by removing the need for a single trusted authority. Blockchain uses unchangeable records and shared agreement methods to make sure all access actions are clear and can't be changed. Comparisons with traditional access models like RBAC and ABAC suggest that blockchain improves tracking and responsibility. But there are still problems like slow processing, high costs, and privacy issues. Overall, blockchain supports new access control systems like ZTNA by offering decentralized trust.

L. Zhang, M. Zhou, and Y. Wang [4] proposed a useful way to manage access control in blockchain networks. These self-running programs enforce rules automatically, without needing people or third-party help. Frameworks built with Solidity on Ethereum allow administrators to set and update user roles and permissions in a way that can't be changed. Studies show smart contracts reduce errors and help keep track of user actions. But they need to be designed and tested carefully to stop possible security problems. J. Park and R. Sandhu [5] design a system using blockchain allow decisions based on user, environment, and resource attributes like role, time, device health, and network conditions. K. Cameron and M. Sporny [6], developed DID and SSI frameworks change how digital identities are managed and checked. Instead of relying on one central authority, users control their own credentials, which are kept secure on a shared network. S. Singh and D. Sharma [7] shows that every user action or data change can be recorded on the blockchain to keep everything clear and traceable. These logs provide real proof during audits or investigations. The distributed nature of blockchain also removes single points of failure found in traditional logging systems. F. Antonopoulos and G. Wood [8] combining it with decentralized file systems like IPFS. In these setups, only metadata or file hashes are stored on the blockchain, and large files are kept off-chain. This keeps data secure while allowing more storage and efficiency. Smart contracts are used to manage access and verify data.

The literature review shows a growing need for better security solutions because traditional perimeter-based network security models have limitations. This is particularly true in cloud-centric and remote working environments. Zero Trust Network Access (ZTNA) has become an effective method that focuses on continuous authentication and tight access control to reduce insider threats and unauthorized access. However, many current ZTNA systems depend on centralized identity and policy management systems. This reliance can create single points of failure and increase vulnerability to cyberattacks. Recent research suggests that combining blockchain technology with ZTNA can help solve these problems by decentralizing identity verification, ensuring tamper-proof logging, and improving transparency in access control. Using smart contracts also boosts automation, lowers administrative tasks, and strengthens policy enforcement. Overall, the reviewed literature points out that blockchain-based ZTNA frameworks offer a promising way to create secure, transparent, scalable, and resilient network access control systems for today's digital environments.

III METHODOLOGY

The methodology of this project outlines a clear approach for designing and implementing a secure Blockchain-Based Zero Trust Network Access (ZTNA) system that protects sensitive data in cloud and distributed environments. The proposed framework combines blockchain technology, encryption methods, and Zero Trust security principles to guarantee safe data storage, controlled access, and clear activity monitoring. By decentralizing identity management and access control with smart contracts, the system removes single points of failure and builds trust, integrity, and accountability. The methodology emphasizes secure data encryption, blockchain-based storage, attribute-driven access control, continuous verification, and immutable logging to create a reliable, scalable, and user-friendly security setup appropriate for modern digital infrastructures. Additionally, the framework includes automated authentication processes, secure data transmission methods, and real-time access validation to improve overall system security.

Using decentralized blockchain infrastructure also ensures tamper-proof record keeping, increased system resilience, and better auditability of user activities. This approach not only cuts down on administrative work but also boosts operational efficiency by limiting manual tasks while keeping strict security standards. Overall, the methodology aims to offer a strong, transparent, and flexible security solution that can tackle new cyber threats in dynamic cloud-based and distributed computing environments. The proposed system consists of System Initialization and User Authentication, Data Encryption and Secure Upload, Blockchain Integration and Immutable Storage, Attribute-Based Access Control Implementation, Zero Trust Verification and Access Decision, Data Retrieval, Decryption, and Logging, and Monitoring, Auditability, and Security Enhancement

The proposed Blockchain-Based Zero Trust Network Access (ZTNA) system uses a structured method to ensure secure data storage, controlled access, and clear monitoring in cloud and distributed environments. The system combines blockchain technology, AES encryption, Attribute-Based Access Control (ABAC), and Zero Trust principles to remove centralized weaknesses and improve security. Data is encrypted before it is stored, and blockchain maintains unchangeable records of transactions, access permissions, and activity logs. Smart contracts handle authentication and access control decisions automatically, making sure every request is checked before access is given. By decentralizing identity management and requiring ongoing verification, the method guarantees confidentiality, integrity, accountability, and resilience. Overall, the approach offers a flexible, secure, and clear framework for modern network access management.

IV. RESULTS AND DISCUSSION

The results of the proposed Blockchain-Based Zero Trust Network Access (ZTNA) system show that the framework effectively guarantees secure, transparent, and reliable file storage and access control. The successful integration of AES encryption, SHA-256 hashing, blockchain-based logging, and Attribute-Based Access Control (ABAC) confirms that the system keeps data confidential, intact, and accessible only to authorized users throughout the data lifecycle. During testing, all core functions—such as user registration, authentication, encrypted file upload, access request verification, decryption, and file download—worked successfully. Each transaction was recorded on the Ethereum blockchain, creating unchangeable and verifiable logs. The generated hash values stayed consistent, confirming that stored data was not altered. This validated the system's integrity mechanism. The access control system worked as intended, providing file access only when user attributes matched predefined policies. Unauthorized users were denied access, showing effective enforcement of Zero Trust principles. The decentralized design removed the need for a central authority, eliminating single points of failure and improving system reliability. From a security standpoint, the system showed significant advancement over traditional centralized models. Even in situations where blockchain data was accessed, encrypted files remained unreadable without the correct AES key, ensuring confidentiality. The unchangeable logging feature improved auditability and transparency, allowing administrators to track user activities accurately.

Table 4.1: Performance Comparison

System	Security level	Transparency	Reliability	Remarks
Traditional Access Control	Moderate	Low	Medium	Centralized
Centralized ZTNA	Good	Moderate	Moderate	Possible Single Point of Failure
Block chain based ZTNA	High	High	High	Decentralized, Tamper Proof Logging

From Table 4.1, it compares traditional access control systems, centralized ZTNA solutions, and the proposed blockchain-based ZTNA system regarding security level, transparency, reliability, and overall effectiveness. Traditional access control systems offer moderate security, but they have low transparency and face higher risks from centralized management. Centralized ZTNA enhances security and transparency somewhat, but it still has potential single-point failures. In contrast, the blockchain-based ZTNA system provides higher security, improved transparency, and better reliability. It does this by using decentralized architecture and tamper-proof logging, making it a more secure and trustworthy solution for managing modern data access.

From Fig. 4.1, This graph shows the performance metrics of the proposed Blockchain-Based ZTNA system across key factors like authentication speed, system reliability, auditability, and scalability. The results indicate strong overall performance, with auditability scoring the highest because of the logging capabilities of blockchain technology. System reliability and scalability also show good performance, reflecting the strength of the decentralized architecture. While authentication speed is slightly lower than the other metrics, it remains efficient while ensuring strict security verification. This highlights the balance between security and performance in the proposed system.

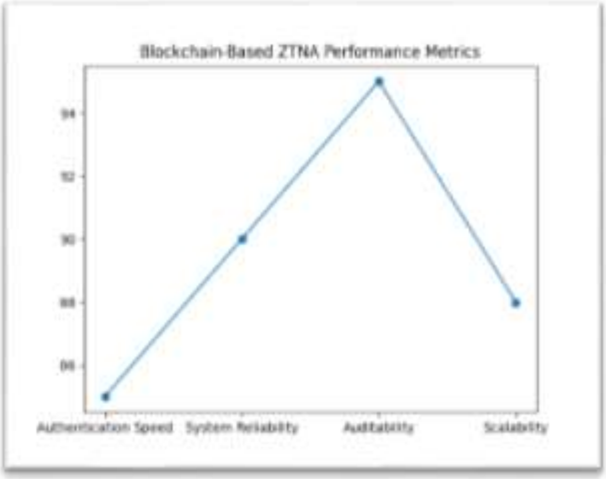
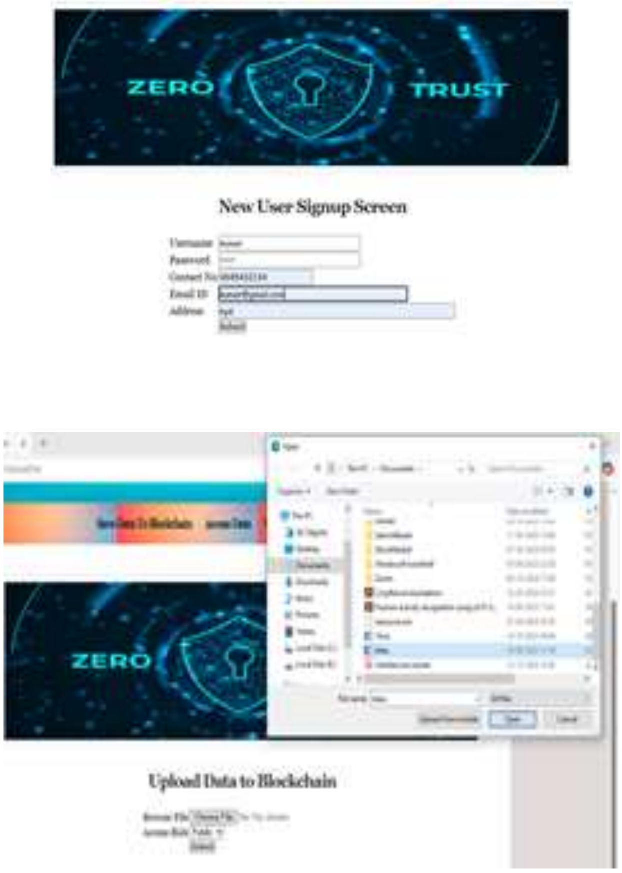


Fig 4.1: Blockchain-Based Performance Metrics



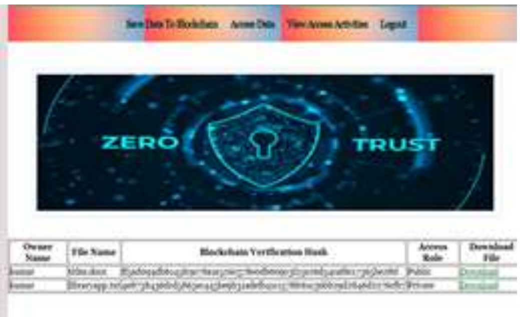
New User Signup Screen

Username	kumar
Password	[illegible]
Contact No	[illegible]
Email ID	kumar@gmail.com
Address	hyd

Upload Data to Blockchain

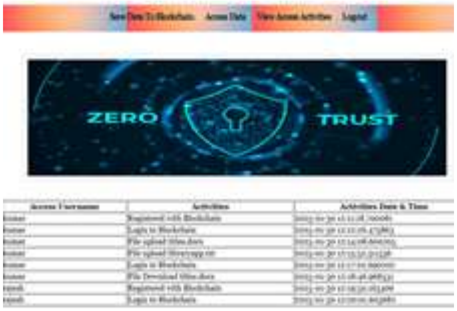
Browse File	Choose File No file chosen
Access Role	Public

Fig 4.2. User Signup and data uploading to blockchain



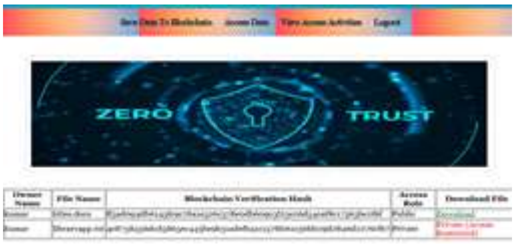
Owner Name	File Name	Blockchain Verification Hash	Access Role	Download File
kumar	[illegible]	[illegible]	Public	Download
kumar	[illegible]	[illegible]	Private	Download

Fig 4.5: Details of Uploaded



Access Username	Activities	Activities Date & Time
kumar	Registered with Blockchain	[illegible]
kumar	Login to Blockchain	[illegible]
kumar	File upload [illegible]	[illegible]
kumar	File upload [illegible]	[illegible]
kumar	Login to Blockchain	[illegible]
kumar	File Download [illegible]	[illegible]
[illegible]	Registered with Blockchain	[illegible]
[illegible]	Login to Blockchain	[illegible]

File View Access Activities



Owner Name	File Name	Blockchain Verification Hash	Access Role	Download File
kumar	[illegible]	[illegible]	Public	Download
kumar	[illegible]	[illegible]	Private	[illegible]

Fig4.7: Final Result

V. CONCLUSION

The combination of Blockchain technology with Zero Trust Network Access (ZTNA) significantly enhances network security by addressing the limitations of traditional centralized security systems. Unlike conventional ZTNA frameworks that depend on centralized identity providers and policy servers, the blockchain-based approach decentralizes trust, removing single points of failure and improving system resilience. Smart contracts enable automated, real-time access control decisions based on continuous verification of user identity, device status, and access context, ensuring compliance with the Zero Trust principle of “never trust, always verify.” This automation reduces administrative workload while maintaining consistent and adaptive security enforcement. Furthermore, the immutable nature of blockchain ensures transparent and tamper-proof recording of authentication activities, access permissions, and policy updates, supporting strong auditability and regulatory compliance. The decentralized architecture enhances reliability, prevents unauthorized data modification, and enables seamless integration with both cloud-based and on-premises infrastructures. Overall, the Blockchain-based ZTNA system provides a secure, scalable, and future-ready solution for access management, strengthening data protection and helping organizations effectively address evolving cybersecurity challenges. The proposed Blockchain-based Zero Trust Network Access (ZTNA) system provides a secure and transparent framework for access control, but there is still scope for future improvement. Enhancing blockchain performance through efficient consensus mechanisms can improve scalability and reduce latency. Integrating AI and machine learning can enable adaptive access control, threat prediction, and automated security responses. Improving interoperability with cloud platforms, IoT devices, and privacy-preserving technologies will further strengthen usability and data protection. Overall, these advancements can make the blockchain-enabled ZTNA system more efficient, intelligent, and suitable for evolving cybersecurity needs.

REFERENCES

1. [Kindy, S., & Habib, S. (2020). Blockchain-based Zero Trust Architecture for Secure Network Access Control. IEEE International Conference on Communications (ICC), 1-6.
2. Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1-34.
3. Rose, S., et al. (2020). Zero Trust Architecture. NIST Special Publication 800-207, National Institute of Standards and Technology.
4. Cachin, C., & Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild. arXiv preprint arXiv:1707.01873.
5. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A Survey on the Security of Blockchain Systems. Future Generation Computer Systems, 107, 841-853.
6. Saberi, S., et al. (2019). Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. International Journal of Production Research, 57(7), 2117-2135.
7. Kim, H. M., & Laskowski, M. (2018). A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. IEEE Software, 35(3), 34-39.
8. Joshi, A., & Aghila, G. (2021). Blockchain-Based Decentralized Access Control in Cloud Computing. Journal of Network and Computer Applications, 168, 102742.