Leveraging Blockchain for Safe Cloud Data Storage

[1] B.Rani , Assistant professor, Department of CSE ,Malla Reddy Engineering college,Hyderabad,Telangana- 50100 rani@mrec.ac.in

[2] Venkata Anupama Chitturi Assistant Professor, Department of CSE, Malla Reddy Engineering College, Hyderabad, Telangana-50100 **anupama@mrec.ac.in**

[3] K Uma Keerthi , Assistant Professor Department of IT, Malla Reddy University umakeerthikurada@gmail.com

[4] Narayanam Satish Kumar, Assistant Professor, Department of CSE, Malla Reddy Engineering College, Hyderabad, Telangana -50100, satishkumar@mrec.ac.in

[5] T.Nagarjuna Reddy, Assistant Professor, Department of IT, Malla Reddy Engineering College, Hyderabad, Telangana 50100, nagarjuna@mrec.ac.in

[6] B.Anusha, Assistant Professor, Department of IT, Malla Reddy Engineering College, Hyderabad, Telangana -50100. anisha20@mrec.ac.in

ABSTRACT:Ensuring the security and integrity of sensitive data kept on cloud servers has become a crucial problem due to the rapid rise of cloud computing. Conventional approaches mostly use encryption techniques to protect data while it is being transmitted and stored. To stop unwanted changes or attacks on cloud data, encryption might not be enough on its own. In this research, we suggest a novel method to improve data security in cloud storage systems by fusing blockchain technology with encryption. To make sure that only authorized users can access the original material, the system encrypts the data before transferring it to the cloud. Every data block also generates a distinct blockchain hash, which is then recorded in a blockchain ledger. As a fingerprint, this hash serves as thedata, guaranteeing its accuracy. The hash value will change, indicating a change to the server, if attackers edit or tamper with the data. A decentralized, unchangeable record of data transactions is provided by the blockchain method, which makes it visible and impenetrable. An extra degree of security is added by this blockchain connection, which not only makes data more resistant to unwanted changes but also makes it easier to identify attacks in real time. We show the benefits of the suggested approach in terms of data integrity, transparency, and tamper-proof capabilities and compare its efficacy to more conventional encryption-based techniques. According to our findings, using blockchain technology in cloud data storage provides a reliable and expandable way to protect private information in a digital world that is becoming more and more insecure.

KEYWORDS:Data Security, Network Attacks, Block chain, Flask Web Application, RSAEncryption.

I. INTRODUCTION

Blockchain is an innovation that keeps track of the public ledger, or decentralized database, of all the various processes that are carried out and the inputs that are shared. By agreeing, most parties validate the transaction that took place. The data cannot be removed once it has been entered into the program. Every single transaction ever made in the system is documented by this method of recording. The most well-known and widely used technology is the digital currency, which is intrinsically linked. Since it allows multibillion-dollar transactions on a global scale without governmental interference, it has also been one of the most talked-about phenomena in recent years. As a result, there are many regulatory issues involving both the national government and other financial firms. However,Verification that funds have been transferred to a recipient anywhere in the globe is available. We can conclude that because we live in such a digital age, we must rely on other parties to handle security and privacy concerns. But the truth is that this additional source might also be controlled or compromised. The transaction mechanism between two people and two businesses is currently mostly centralized and managed by a third party, which is where blockchain computing enters the picture. In order for transactions to be accomplished, a third party is always involved when we do digital payments. Additionally, a bank or finance firm may levy additional fees. Comparable Similar trends are also observed in other fields, such as applications, games, and music. With the introduction of technology known as blockchain, this problem has been solved. This the technological primary goal is to establish a decentralized system in which a third party is not involved

in any transactions or data.

With the use of distributed agreement, this technology allows us to trace each transaction that has been completed in the past as well as the present. This can be confirmed later. Even so, the confidentiality of the third party's complex and digital assets is maintained. Distributed arbitration and confidentiality are two of the main characteristics of the technology known as blockchain. With the aid of a decentralized database solution, blockchain makes it possible to continuously expand the data records that are contributed by the various nodes. Every completed transaction is entered onto a public ledger. Blockchain-based technologies offer a decentralized solution that eliminates the need for third-party mediation. Every node involved in the Blockchain receives information about every transaction that is completed on it.Relative to a centralized transactions that requires a third party to mediate, this aspect of the blockchain system makes it more transparent. The transaction is also more secure for other nodes because every node in the Blockchain is anonymous. the digital currency was the very first blockchain app for technology to be released. Bitcoin is a distributed system that facilitates the buying and selling of products through digital payments [2]. Even while this technology appears to be very suitable for carrying out transactions using cryptocurrency, it still has certain limitations and technical problems that need careful consideration and resolution. To keep the nodes safe from attacks and to maintain a high level of security, the Blockchain requires that they be kept private.

II. LITERATURE WORK

K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, in their paper “Blockchain-enhanced data sharing with traceable and direct revocation in IIoT,” discuss a blockchain-based mechanism to enhance data sharing security in the Industrial Internet of Things (IIoT). The authors employ smart contracts to provide access traceability and direct revocation of data sharing permissions, ensuring a high level of security. This approach improves data integrity and auditability. However, it introduces high storage overhead and scalability concerns, as the blockchain ledger grows significantly over time [3]. A. F. S. Devaraj, M. Elhoseny, S. Dhanasekaran, E. L. Lydia, and K. Shankar propose a hybrid approach in their work “Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy-efficient load balancing in cloud computing environments.” The study integrates the Firefly Algorithm (FA) with Multi-Objective Particle Swarm Optimization (MOPSO) to enhance resource utilization and ensure energy-efficient task scheduling in cloud environments. The proposed method reduces energy consumption and improves system performance. However, it increases computational complexity and requires fine-tuning of multiple parameters to achieve optimal performance [4]. N. Krishnaraj, M. Elhoseny, E. L. Lydia, K. Shankar, and Omar Alabas, in their research titled “An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment,” develop a novel indexing model to facilitate efficient image retrieval in cloud storage. Their method leverages a radix trie-based approach for semantic indexing, significantly improving search speed and scalability. While their approach enhances retrieval efficiency, it suffers from high memory consumption and preprocessing overhead, which may limit its applicability in resource-constrained environments [5]. P. K. Premkamal, S. K. Pasupuleti, A. K. Singh, and P. J. A. Alphonse present an enhanced security model in “Enhanced attribute-based access control with secure deduplication for big data storage in cloud.” The study introduces an attribute-based encryption (ABE) mechanism combined with secure deduplication techniques to optimize data security while reducing redundancy. This approach strengthens access control and minimizes storage costs. However, it introduces significant computational overhead and challenges in key management, which could hinder its practical deployment [6]. Q. He and H. He, in their work “A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining,” propose a hybrid security model that integrates encryption techniques with data mining to detect anomalies in cloud environments. Their method ensures real-time threat detection and improves data confidentiality. However, it requires substantial computational resources and raises potential data privacy concerns due to extensive mining of user information [7]. V. S. Lakshmi, S. Deepthi, and P. P. Deepthi, in their paper “Collusion-resistant secret sharing scheme for secure data storage and processing over cloud,” introduce a secret-sharing scheme to prevent collusion attacks in cloud storage. Their approach enhances data confidentiality and prevents unauthorized access by malicious insiders. However, their method increases computational complexity and may require additional storage overhead for secure key management [8]. L. Zhou, X. Li, K. H. Yeh, C. Su, and W. Chiu, in “Lightweight IoT-based authentication scheme in cloud computing circumstance,” propose a lightweight authentication mechanism for IoT-based cloud computing environments. Their approach minimizes computational overhead while ensuring secure access control for IoT devices. Although their model enhances authentication efficiency, it may not be resilient against sophisticated cyber-attacks due to its lightweight nature [9].

III. **METHODOLOGY**

The proposed system utilizes blockchain technology to enhance data security, prevent unauthorized modifications, and ensure data integrity. The methodology is divided into two primary modules: Owner Module and User Module, both of which integrate blockchain functionalities for secure data storage and retrieval.

In the Owner Module, the owner registers by providing necessary details and then logs into the system using a secure username and password. Once authenticated, the owner can upload files, which are encrypted using RSA before being stored in the application. Blockchain technology, specifically Hyperledger, is employed to generate a unique hash value for each file, ensuring tamper-proof storage. The owner can share files with registered users and track key requests. When a user requests access, the owner can approve or deny the request. If approved, the system sends the encryption key and blockchain hash via email. The blockchain verification mechanism ensures that the data remains unchanged by validating the hash before allowing download. Any discrepancy in hash values indicates data tampering, preventing unauthorized access.

In the User Module, users register and authenticate through the system. Once logged in, they can view all encrypted files and request access. Upon approval from the owner, the system sends the necessary decryption keys and blockchain hash to the user's email. Before downloading, the system verifies the blockchain hash against the stored hash in the ledger. If the hash matches, the user is granted access to download and decrypt the file. If verification fails, it indicates unauthorized modifications by a third party, and the system blocks the download, ensuring data security.

By incorporating Hyperledger into the data security mechanism, the system achieves enhanced integrity, transparency, and resistance to tampering. Blockchain ensures a decentralized approach, eliminating the need for a central authority and reducing risks associated with single-point failures. The use of RSA encryption and blockchain verification together strengthens data security, preventing unauthorized access and ensuring confidentiality.

.

I. ARCHITECTURE &WORKFLOW

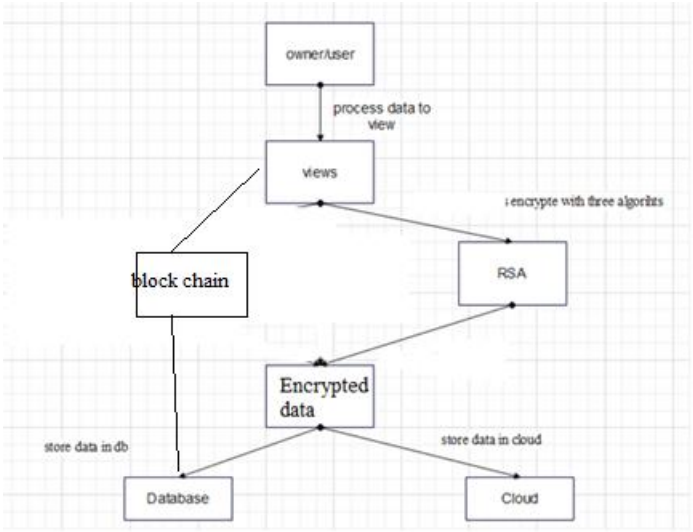

Fig.5:Architecture

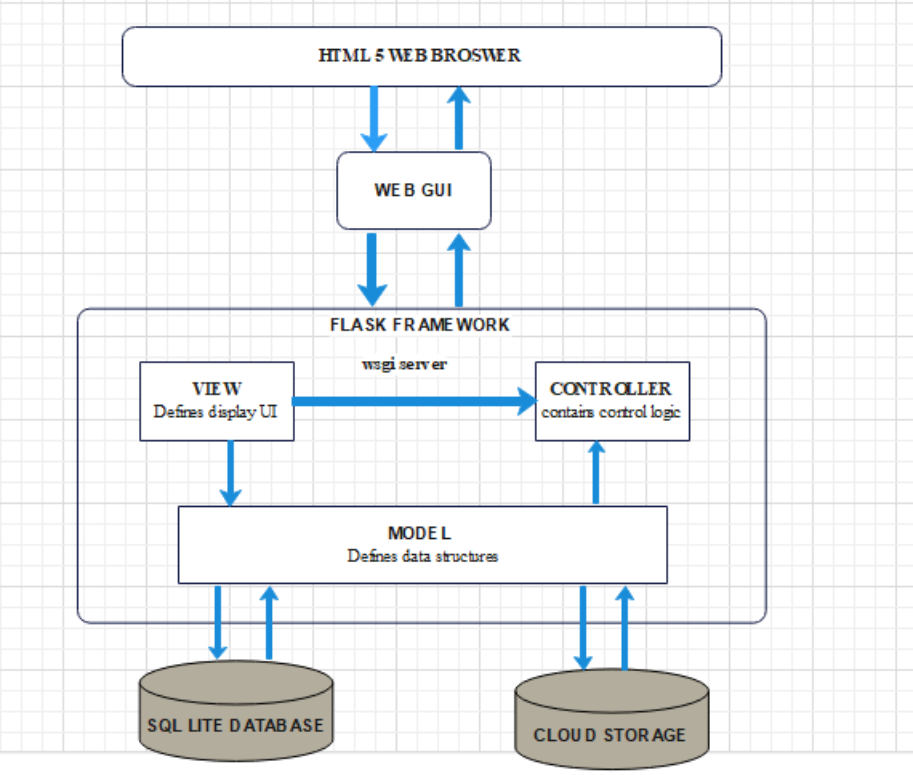

Fig ;6 Flask Frame work structure

IV. EXPERIMENTALRESULTS

Feature	AES (Advanced Encryption Standard)	RSA (Rivest-Shamir-Adleman)	ECC (Elliptic Curve Cryptography)	SHA-256 (Hashing)	Combined Encryption + Blockchain
Security Strength	Strong symmetric encryption	Strong asymmetric encryption	High security with smaller keys	One-way secure hashing	Enhanced security via immutability and decentralization
Key Size	128/192/256-bit	1024/2048/4096-bit	256-bit (equivalent to 3072-bit RSA)	Fixed 256-bit	Uses both encryption and blockchain hashing
Encryption Speed	Fast	Slower due to key size	Faster than RSA	Very fast	Blockchain adds some processing overhead
Computational Cost	Low	High	Moderate	Low	Moderate (due to blockchain verification)
Tamper Resistance	Encryption only, no tracking	Encryption only, no tracking	Encryption only, no tracking	Cannot be reversed	Blockchain ensures tamper-proof logs
Key Management	Symmetric key sharing required	Complex key management	More efficient key management	No keys needed	Decentralized key validation with blockchain
Attack Resistance	Vulnerable if key is exposed	Susceptible to quantum attacks	More resistant to quantum attacks	Secure against brute force	Resistant to data tampering and key compromise
Data Integrity	No built-in integrity check	No built-in integrity check	No built-in integrity check	Ensures integrity	Blockchain ledger ensures data integrity
Single Point of Failure	Possible if encryption key is lost	Possible if private key is compromised	Less vulnerable due to smaller keys	Not applicable	Eliminates single point of failure through decentralization

Table: from above table various encryption methods are compared and which shows combined model for encryption and block chain can increase data protection

Immutability: Blockchain ensures that once data is encrypted and stored, it cannot be altered without detection.

Tamper Detection: Any unauthorized modification is immediately identifiable through blockchain hash verification.

Decentralized Security: Unlike traditional encryption that relies on a single trusted entity, blockchain distributes trust across a network.

Better Key Management: Blockchain can be used to securely store and share encryption keys without central authority reliance.

Quantum Resistance: While traditional encryption may be vulnerable to quantum attacks, blockchain can add an extra layer of security by ensuring historical data integrity.

This combined approach leverages both strong encryption for confidentiality and blockchain for integrity, making it a superior security model for sensitive data storage and transmission. Let me know if you need further refinements.

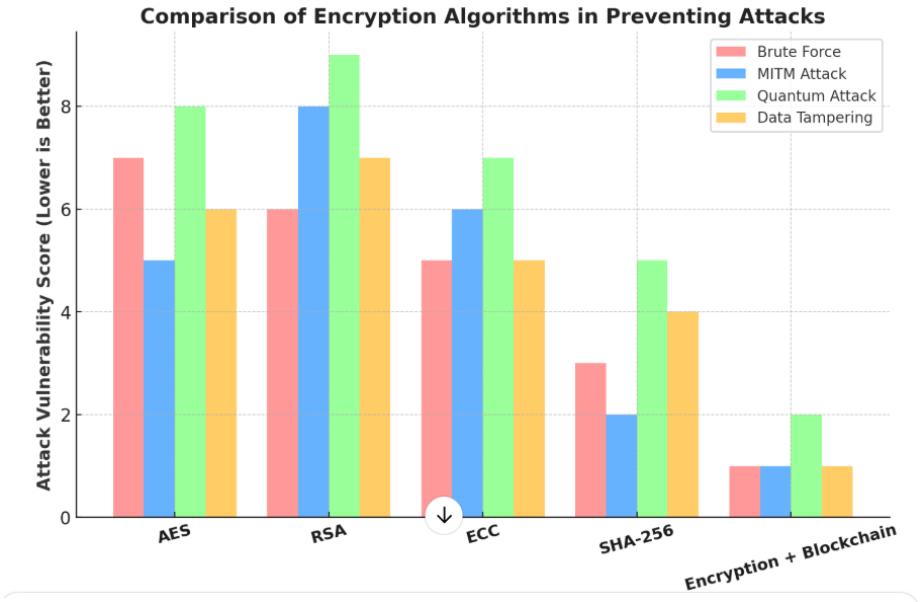

Fig this graph shows various attacks under different algorithms in which block chained combined methods has less attacks.

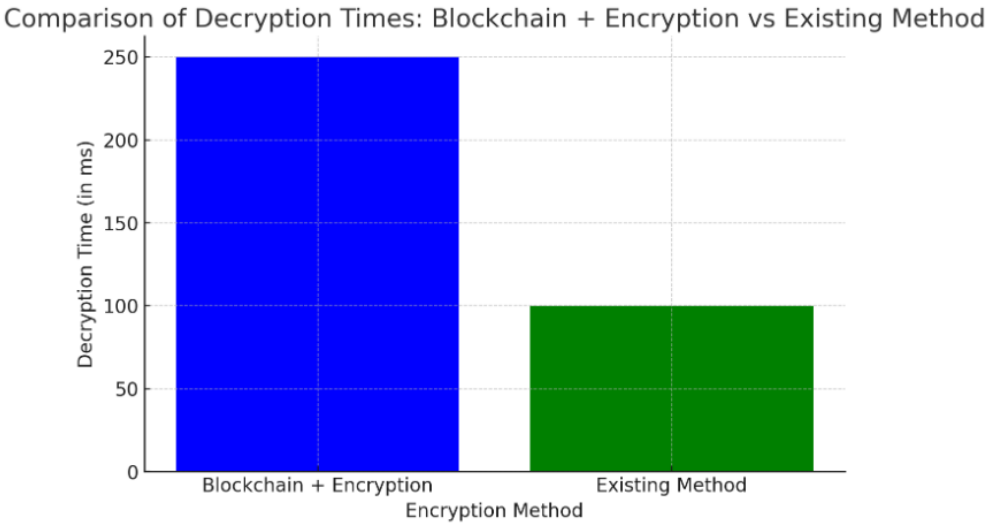

Fig:comparison graph showing the decryption times for the "Blockchain + Encryption" method and the "Existing Method." As expected, the blockchain-based method tends to take more time due to the additional computational overhead, such as consensus mechanisms and the complexity of managing blockchain data.

CONCLUSIONS

The integration of blockchain technology with encryption in cloud data storage provides a significantly higher level of security compared to traditional encryption methods alone. By encrypting data and utilizing blockchain's decentralized, immutable ledger, the system ensures that data remains protected from tampering and unauthorized changes. The hash value tied to each data block guarantees data integrity and allows for real-time detection of any alteration. Furthermore, the transparency and auditability provided by blockchain make it easier to trace and identify potential security threats, thus enhancing overall security. This hybrid approach delivers a more robust, tamper-proof solution, addressing both data confidentiality and integrity. Despite encryption being effective for protecting data in transit and storage, blockchain adds an additional layer that safeguards against any unauthorized alterations. The method's resilience to cyber-attacks and data breaches demonstrates its effectiveness in an increasingly digital and insecure environment. The study confirms that blockchain and encryption together provide a scalable and reliable security solution. However, the downside is the increased time required for decryption due to the blockchain integration, which could impact performance in real-time applications. Overall, this combined approach is an innovative step towards securing sensitive data in cloud storage systems.

VI Future Scope

The hybrid method of blockchain and encryption holds great promise for enhancing data security in cloud environments, but there is significant room for further research and development. Future efforts could focus on optimizing the decryption process to reduce time delays, making the method more suitable for real-time applications without compromising security. Additionally, researchers could explore the potential for combining this approach with other advanced security technologies such as AI-based threat detection or multi-factor authentication to further strengthen data protection. Cloud service providers could adopt this technique more widely, but they will need to address concerns related to the computational overhead and scalability. Future work could aim to develop lightweight blockchain protocols that maintain high levels of security while minimizing resource consumption. Furthermore, the system's ability to handle large-scale data storage needs in a decentralized environment could be explored, ensuring that it remains efficient as the amount of stored data grows. Additionally, integrating quantum-resistant encryption methods with blockchain could be an important avenue to explore in anticipation of future advancements in quantum computing. Real-world pilot implementations of this hybrid system across various industries could provide further insights into its practical viability and help refine the model for broader adoption.

REFERENCES

[1]Blanco-Novoa O et al (2018) A practical evaluation of commercial industrial augmented reality systems in an industry 4.0 shipyard. IEEE Access 6:8201–82182.

[2] Fraga-Lamas P et al (2018) A review on industrial augmented reality systems for the industry4.0 shipyard. IEEE Access 6:13358–13375

[3] K. Yu, L.Tan, M. Aloqaily, H. Yang and Y. Jararweh, “Blockchain-enhanced data sharing with traceable and direct revocation in IIoT,” IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7669–7678, 2021.

[4] A. F. S. Devaraj, M. Elhoseny, S. Dhanasekaran, E. L. Lydia and K. Shankar, “Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy efficient load balancing in cloud computing environments,” Journal of Parallel and Distributed Computing, vol. 142, no. 4, pp. 36–45, 2020.

[5] N. Krishnaraj, M. Elhoseny, E. L. Lydia, K. Shankar and Omar ALDabbas, “An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment,” Software: Practice and Experience, vol. 51, no. 3, pp. 489–502, 2021.

[6] P. K. Premkamal, S. K. Pasupuleti, A. K. Singh and P. J. A. Alphonse, “Enhanced attribute-basedaccess controlwith securededuplication forbig datastorage in cloud,” Peer-to-Peer Networking and Applications, vol. 14, no. 1, pp. 102–120, 2021.

[7] Q. He and H.He, “A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining,” Sustainability, vol. 13, no. 1, pp. 101, 2021.

[8] V. S. Lakshmi, S. Deepthi and P. P. Deepthi, “Collusion resistant secret sharing scheme for secure data storage and processing over cloud,” Journal of Information Security and Applications, vol. 60, no. 9, pp. 102869, 2021.

[9] L. Zhou, X. Li, K. H. Yeh, C. Su and W.Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance,” Future Generation Computer Systems, vol. 91, no. 6, pp. 244–251, 2019.