International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Cloud Chain: Integrating Ethereum Blockchain for Secure & Scalable Cloud Services

Ms. J. Rekha
Assistant Professor,
Dept of CSE(DS) , CMR Technical Campus
Hyderabad, Telangana,
India
mrreo10@gmail.com

Ms. N. Soujanya
Assistant Professor,
Dept of CSE(DS), CMR Technical Campus Hyderabad,
Telangana, India
noundlasoujanya516@gmail.com

R. Sai Deepthi
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana,
India
saideepthirayini@gmail.com

S. Praveen Kumar
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
somanaboinapraveenkumar@gmail.com

K. Poojitha
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
poojithaapooja1216@gmail.com

M. Suresh
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
malothsuresh289@gmail.com

How to Cite this Article:
Soujanya, N., Deepthi, R. S., Kumar, S. P., Poojitha, K. & Suresh, M. (2026). Cloud Chain: Integrating Ethereum Blockchain for Secure & Scalable Cloud Services. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.305

https://doi.org/10.55041/ijcope.v2i4.305

ABSTRACT— Cloud computing has revolutionized the way organizations and individuals store, process, and manage data by offering scalable and cost-effective solutions over the internet. However, despite its widespread adoption, cloud computing faces critical challenges related to data security, privacy, trust, and centralized control. Centralized cloud architectures are highly susceptible to cyber-attacks, unauthorized access, and data breaches, which can compromise sensitive information. To address these issues, this project proposes a blockchain-integrated cloud system called Cloud Chain, which leverages Ethereum blockchain technology to enhance security and trust in cloud environments.The proposed system utilizes smart contracts to automate access control and ensure secure data transactions. Blockchain provides an immutable and decentralized ledger, making it nearly impossible to alter stored data without detection. This system enables secure file storage, transparent data access, and efficient verification mechanisms. By integrating blockchain with cloud computing, the project enhances data integrity, reduces dependency on centralized authorities, and improves overall system reliability. The experimental results demonstrate that the proposed system provides a more secure and scalable solution compared to traditional cloud systems.

INTRODUCTION

Cloud computing has become a fundamental technology in modern IT infrastructure, enabling organizations to store large volumes of data and access computing resources on demand. It eliminates the need for physical hardware and reduces operational costs. Despite these advantages, traditional cloud systems rely on centralized architectures where data is managed by third-party service providers. This centralization creates vulnerabilities such as data breaches, insider threats, and lack of transparency. Users must trust service providers to handle their data securely, which is not always guaranteed.

Blockchain technology introduces a decentralized approach that addresses these limitations by distributing data across multiple nodes and maintaining a transparent and immutable ledger. Ethereum blockchain, in particular, provides support for smart contracts, which are self-executing programs that enforce predefined rules without requiring intermediaries. By integrating blockchain with cloud computing, it becomes possible to enhance security, transparency, and trust.

In this project, a hybrid system is developed where cloud computing handles data storage and scalability, while blockchain ensures security and access control. This combination creates a more robust and efficient system capable of addressing modern cloud security challenges.

I. PROBLEM DEFINITION

Cloud computing systems are designed to provide efficient data storage and services to a large number of users. However, their centralized nature introduces several security and trust-related challenges. Sensitive data stored in the cloud is vulnerable to unauthorized access, data tampering, and cyber-attacks. In addition, users have limited control over their data once it is stored in the cloud, leading to concerns about privacy and data misuse.

Traditional security mechanisms such as encryption and authentication provide some level of protection but are not sufficient to address all threats, especially insider attacks and system vulnerabilities. Furthermore, the lack of transparency in cloud operations makes it difficult to track data access and modifications.

Therefore, there is a need for a secure and transparent system that ensures data integrity, prevents unauthorized access, and eliminates reliance on centralized authorities. This project aims to solve these problems by integrating blockchain technology into cloud computing, thereby providing a decentralized and secure environment for data storage and access.

1.2 PROJECT FEATURES

The proposed Cloud Chain system incorporates advanced features that significantly improve cloud security and performance. The system ensures secure file storage by encrypting data before uploading it to the cloud, thereby preventing unauthorized access. It uses blockchain technology to maintain a tamper-proof record of all transactions, ensuring data integrity and transparency. Smart contracts are implemented to automate access control, allowing only authorized users to access specific data based on predefined conditions.

The decentralized architecture of the system eliminates the need for a single controlling authority, reducing the risk of system failures and attacks. Additionally, the system is designed to be scalable, allowing it to handle large volumes of data efficiently. It also provides real-time verification of data access and maintains detailed logs for auditing purposes, thereby enhancing accountability and trust among users.

Related Work

Several research studies have explored the integration of advanced technologies to improve cloud security. Traditional approaches include the use of encryption algorithms, authentication protocols, and intrusion detection systems. While these methods provide a certain level of protection, they are often insufficient to handle sophisticated cyber threats.

Recent research has focused on the use of blockchain technology to enhance data security and transparency. Blockchain-based systems have been proposed for secure data sharing, decentralized storage, and identity

management. These systems leverage the immutability and transparency of blockchain to prevent data tampering and unauthorized access.

However, many existing solutions face challenges related to scalability, high computational costs, and limited integration with cloud platforms. Some systems also lack efficient mechanisms for managing access control using smart contracts. This project builds upon existing research by developing a more efficient and scalable system that integrates Ethereum blockchain with cloud computing, thereby addressing the limitations of previous approaches.

II. METHODOLOGY

1. Data Collection and Upload

Users upload data to the cloud system through a secure interface after authentication.

2. Data Encryption and Storage

The uploaded data is encrypted and stored in the cloud to ensure confidentiality and security.

3. Block chain Integration

File metadata is stored on the Ethereum blockchain to maintain a secure and tamper-proof record.

4. Smart Contract-Based Access Control

Smart contracts are used to verify user permissions and control access to data automatically.

5. Data Access and Verification

When a user requests data, the blockchain verifies the request, and only authorized users can access and decrypt the data.

III. PROPOSED SYSTEM

The proposed system combines cloud computing with blockchain technology to create a secure and decentralized platform. It integrates cloud storage for handling large data and Ethereum blockchain for maintaining secure and immutable records. Smart contracts play a key role in automating access control and ensuring that all transactions are secure and transparent. Unlike traditional systems, this approach eliminates the need for centralized control, thereby reducing the risk of data breaches and unauthorized access. The system enhances trust among users by providing a transparent and tamper-proof environment.

IV. IMPLEMENTATION DETAILS

The implementation of the proposed system involves both frontend and backend technologies along with blockchain integration. The frontend is developed using HTML, CSS, and JavaScript to provide a user-friendly interface. The backend is implemented using programming languages such as Python or Node.js to handle server-side operations. Ethereum blockchain is used to deploy smart contracts, and tools like MetaMask and Ganache are utilized for blockchain interaction and testing. The system allows users to upload files, manage access permissions, and retrieve data securely through a simple interface.

4.1 ALGORITHMS USED

4.1.1 ELLIPTIC CURVE CRYPTOGRAPHY(ECC)

Elliptic Curve Cryptography (ECC) is a modern encryption algorithm used to provide strong security with smaller key sizes. It is based on mathematical properties of elliptic curves and is widely used for secure data transmission. In this project, ECC is used to generate public and private keys for encrypting and decrypting user data. When a user uploads a file, the data is encrypted using the public key, and only the corresponding private key can decrypt it. This ensures confidentiality and prevents unauthorized users from accessing sensitive information. Due to its efficiency and high level of security, ECC is highly suitable for cloud-based applications.

4.1.2 SECURE HASH ALGORITHM(SHA-256)

SHA-256 is a cryptographic hashing algorithm that generates a unique fixed-length hash value for any input data. It is widely used in blockchain technology to ensure data integrity. In this project, SHA-256 is used to generate hash values for files stored in the system.

Instead of storing actual data on the blockchain, only hash values are stored, which act as unique identifiers. If any modification occurs in the data, the hash value changes, making it easy to detect tampering. This mechanism ensures that the data remains secure and unchanged.

4.1.3 ETHEREUM SMART CONTRACTS

Smart contracts are self-executing programs that run on the Ethereum blockchain. They automatically enforce predefined rules and conditions. In this project, smart contracts are used to manage user registration, file storage, and access control. When a user performs an action, such as uploading or accessing data, the smart contract verifies the conditions and executes automatically. This improves security, transparency, and reduces manual intervention.

4.1.4 INTERPLANETARY FILE SYSTEM(IPFS)

IPFS is a decentralized storage system used to store large files securely. Instead of storing files directly on the blockchain, they are stored in IPFS and only the file hash is stored on the blockchain. This reduces storage cost and improves efficiency. IPFS distributes data across multiple nodes, ensuring high availability and reliability. In this project, it is used for secure and efficient file storage.

4.1.5 PROOF OF WORK(POW)

Proof of Work (PoW) is a consensus algorithm used in blockchain to validate transactions. It ensures that all transactions are verified before being added to the blockchain. In this project, PoW helps maintain the security and integrity of the system by preventing unauthorized changes and malicious activities. It ensures that the blockchain remains trustworthy and tamper-proof.

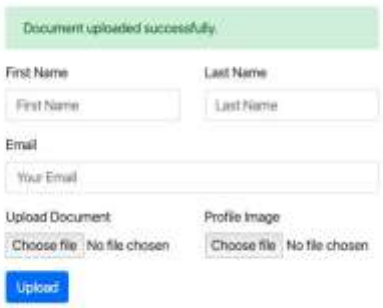
V. EXPERIMENTAL RESULTS AND DISCUSSION

The following screenshots represent the execution and performance of the proposed Cloud Chain system. These figures demonstrate the working of different modules such as user authentication, file upload, encryption, blockchain storage, and secure data retrieval. The results clearly show how the system ensures data security, integrity, and transparency using blockchain technology..

System Interface – Home Page:

The above figure shows the main interface of the system where users can perform operations such as registration, login, file upload, and file access.

Fig. 1.File Upload



In this figure, the user uploads a file to the system. The file is encrypted using Elliptic Curve Cryptography (ECC) before being stored.

Fig. 2. Final Output Page

The above figure shows the blockchain transaction where the file metadata and hash value are stored. The blockchain ensures immutability, meaning the data cannot be altered

once it is stored. This guarantees data integrity and transparency.

VI. CONCLUSION

This project presents a secure and scalable cloud computing system by integrating Ethereum blockchain technology. The proposed system addresses key challenges in traditional cloud environments, including data security, transparency, and trust. By utilizing blockchain and smart contracts, the system ensures secure data storage, controlled access, and tamper-proof records.

The results demonstrate that the integration of blockchain significantly improves the security and reliability of cloud systems. This project highlights the potential of combining emerging technologies to create advanced solutions for modern computing challenges.

VII. FUTURE SCOPE

The proposed system can be further enhanced by integrating advanced technologies such as artificial intelligence and machine learning for real-time threat detection and predictive analysis. Future improvements may include support for multiple blockchain platforms, enabling greater flexibility and interoperability. The system can also be optimized to reduce transaction costs and improve scalability for handling large-scale applications.

Additionally, the integration of real-time monitoring and automated response systems can further enhance security. These advancements will make the system more robust, efficient, and suitable for practical deployment in various industries.

VIII.ACKNOWLEDGMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **Ms. J. Rekha** Designation for his/her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him/her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) coordinators **N. Soujanya, Shafana Bakshi,**
for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Murali**, Head, Department of Computer Science and Engineering (Data Science) for providing encouragement and support for completing this project successfully.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to **Sri. Ch. Gopal Reddy**, Chairman, **Smt. C. Vasantha Latha**, Secretary and
Sri. C. Abhinav Reddy, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

The guidance and support received from all the members of CMR Technical Campus who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

IX. REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"
https://bitcoin.org/bitcoin.pdf

[2] Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger"
https://ethereum.github.io/yellowpaper/paper.pdf

[3] Juan Benet, "IPFS: Content Addressed, Versioned, P2P File System"
https://arxiv.org/abs/1407.3561

[4] Z. Zheng et al., "An Overview of Blockchain Technology"
https://ieeexplore.ieee.org/document/8048631

[5]N. Koblitz, "Elliptic Curve Cryptography"
https://doi.org/10.1090/S0025-5718-1987-0866113-5

[6] Christidis & Devetsikiotis, "Blockchains and Smart Contracts for IoT"
https://ieeexplore.ieee.org/document/7467408

[7] Blockchain Applications Beyond Cryptocurrency
https://arxiv.org/abs/1801.03528

[8] Blockchain Technology Survey (IEEE Big Data)
https://ieeexplore.ieee.org/document/8029379

X. GITHUB REPOSITORY LINK

https://github.com/saideepthirayini/A15-IOMP.git