IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Dynamic Secure Access Control and Data Sharing through Blockchain-Enabled Cloud-IoT Environment

Mr. Thangadurai K[1], Sathish kumar T[2], Suresh D[3], Balamurugan U[4], Karuppuchamy M[5]
Assistant Professor, Computer Science and Engineering [1]
Students, Computer Science and Engineering[2,3,4,5]
Mahendra Institute of Engineering and Technology, Namakkal, India

Abstract: *Cloud storage is a Peer-to-peer network in IoT environment where each node provides the storage service to the customer's data. The storage system is based on the blockchain domain where it is completely decentralized. The convergence of Internet of Things (IoT), Cloud Computing, and Blockchain offers a secure, scalable, and decentralized data management approach. However, ensuring granular and dynamic access control remains a significant challenge due to the distributed nature of IoT networks. This paper proposes a Dual Access Control Mechanism (DACM) that combines Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to provide fine-grained, adaptive, and secure access management for IoT applications. Cloud Computing is utilized for storage and processing, while Blockchain ensures data integrity, decentralization, and tamper-proof access control policies through smart contracts. The proposed Dual Access Control Mechanism (DACM) integrates IoT, Cloud, and Blockchain to enhance security, scalability, and decentralized access management. By leveraging RBAC & ABAC.*

Keywords: Cloud Computing, Blockchain, Smart Contract, Dual Access Control Machanism(DACM), KNN Algorithm, Naïve Bayes Algorithm, Resource Management, Security and Privacy

I. INTRODUCTION

The rapid advancement of the Internet of Things (IoT) has led to the proliferation of smart devices that generate massive volumes of data. To effectively manage and process this data, cloud computing has emerged as a powerful solution, offering scalable storage and computational resources. However, the centralized nature of traditional cloud models presents significant security and privacy concerns.

To address these challenges, blockchain technology has gained prominence due to its decentralized, tamper-proof, and transparent architecture. By integrating blockchain with cloud-based IoT systems, it is possible to enhance data integrity, authentication, and trust among connected devices. This fusion not only ensures secure data transactions but also supports decentralized decision-making and improved system resilience.

This presentation explores the architectural design and benefits of combining cloud computing and blockchain technologies in IoT environments. It aims to highlight the strengths, challenges, and potential applications of this integration in creating more secure, efficient, and trustworthy IoT systems.

II. LITERATURE REVIEW

1. Computing-based Data Storage and Disaster Recovery Cloud

Author - Zhang Jian-hua and Zhang Nan(2020).

This survey paper focuses on issues related to storing and sharing huge amounts of data on the cloud over the internet by using Cloud Storage technique.

2. Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique

Author - Kajal Rani1, Raj Kumar Sagar 2.(2021)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, May 2025 Impact Factor: 7.67

The challenges and issues related to cloud storage security were covered in was essay. By putting this proposed work into practise, we may strengthen the security of cloud storage using techniques like encryption, decryption, compression, and sharing.

3. Blockchain-based Security Architecture for Distributed Cloud Storage

Author- Jiaxing Li, Zhusong Liu, Long Chen, Pinghua Chen,JigangWU (2021)

In this work, a distributed cloud storage security architecture based on blockchain technology is suggested. In terms of network performance and security, the suggested design has been compared to two existing conventional architectures with tolerable network transmission delay.

4. Redundancy Prevention and Secure Audit of Encrypted Big Data in HDFS Cloud using Cloud Guard+ System

Author – Vinit Atul Shevade, D.A. Kulkarni (2022)

From above paper we gathered information about preventing duplications of data and integrity of cloud data.

III. METHODOLOGY

Problem Definition

The integration of IoT and cloud computing brings numerous benefits such as scalability, flexibility, and efficient resource utilization. However, it also introduces significant security and privacy challenges, including:

- Inadequate access control mechanisms for distributed IoT devices.
- Risk of data manipulation and unauthorized access in centralized cloud storage.
- Lack of transparency and traceability in data access and sharing.
- Traditional security solutions are insufficient for dynamic, decentralized, and large-scale IoT-cloud ecosystems.

These challenges necessitate a more robust, transparent, and decentralized security framework.

Proposed Technique

To address the identified issues, a blockchain-enabled architecture is proposed that integrates IoT, cloud computing, smart contracts, and machine learning. The key components of the proposed technique are:

Blockchain for Identity Management and Access Control:

- Each IoT device is assigned a unique blockchain identity.
- Smart contracts handle access permissions and enforce policies automatically.

Cloud Layer for Data Processing and Storage:

- Cloud infrastructure handles large-scale data storage and analytics.
- All data is verified through blockchain hash values before being stored.

Machine Learning for Anomaly Detection:

- Trained models monitor device behavior and detect suspicious or abnormal patterns in access or data flow.
- Alerts are generated in case of anomalies to initiate preventive action.
- This hybrid architecture ensures data integrity, privacy, and trust, while also enabling scalability and real-time processing.

Implementation

The implementation is divided across three interconnected layers:

IoT Layer:

- Devices collect real-time data and request access to services.
- Devices are authenticated through blockchain-based identity verification.

Cloud Layer:

- Acts as the storage and computation hub.
- Data is processed and analyzed in real-time.
- Only blockchain-verified data is stored to ensure tamper resistance.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Blockchain Layer:

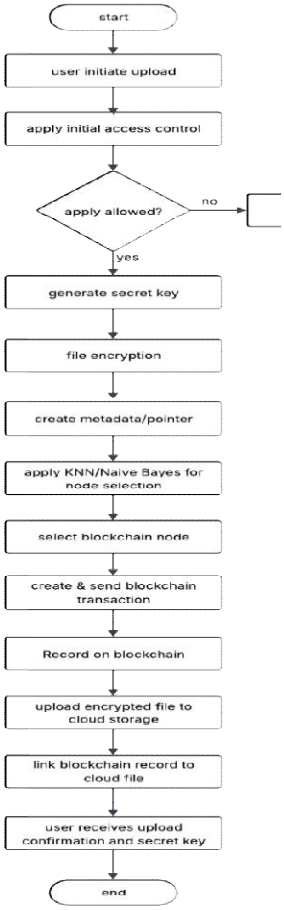
- Smart contracts define and enforce fine-grained access control policies.
- Immutable logs and authentication records are maintained to ensure traceability and accountability.
- Blockchain acts as a decentralized authority to eliminate single points of failure.
- The integration of machine learning occurs at the cloud layer, where real-time data and access logs are analyzed for any signs of threats or anomalies, thus improving system resilience.

IV. PROPOSED SYSTEM

There are various security concerns nowadays, including challenges with access control, scalability, virtualization, privacy, and enormous amounts of data processing for data and applications in the IOT Environment and the cloud, traditional security techniques are no longer appropriate. Applications and data stored in the cloud have no fixed restrictions because cloud computing is scalable and location independent. When exchanging and storing data on centralised servers, difficulties with data manipulation and authentication frequently arise. By avoiding malicious users and improving security & privacy, this paper propose a blockchain platform for data and cloud storage which is built by using access control mechanism and machine learning.

Flow chart for uploading and retravel the file in cloud is given below:

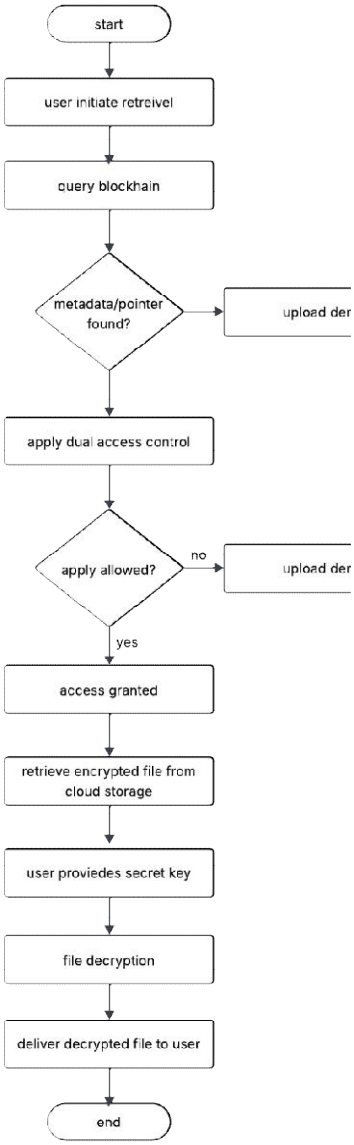
1. Uploading:



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

The upload process begins when a user initiates the upload of a file. The system first applies an initial access control check to verify if the user is authorized to upload. If the upload is allowed, a unique secret key for this specific file. The file is then encrypted on the user's device using this key. The encrypted file may undergo further preparation, such as splitting, if needed. Next, the system creates metadata about the encrypted file, including a pointer to its storage location, while ensuring the secret key itself is not stored. Features are extracted from the encrypted file and/or the user, and machine learning algorithms (KNN and Naive Bayes) are applied to select the most suitable blockchain node(s) for storing this metadata. A blockchain transaction containing the metadata, pointer, and node information is created and recorded on the selected node(s). The encrypted file is then uploaded to cloud storage, and the blockchain record is linked to the file's cloud location. Finally, the user receives confirmation of the successful upload, along with the secret key for future retrieval.

2. Retrieval:



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

The retrieval process starts when a user requests a file. The system queries the blockchain to find the metadata and pointer associated with the requested file. If found, the system applies dual access control to verify the user's permissions. If access is granted, the encrypted file is retrieved from cloud storage using the pointer. The user is then prompted to enter the secret key, and the frontend decrypts the file. The decrypted file is delivered to the user. Optionally, the system can verify the integrity of the decrypted file by comparing its hash with a hash stored on the blockchain.

V. RESULTS AND DISCUSSION

Functional Verification:

- Describe how you tested the core functionalities: file upload and retrieval.
- For upload, state that files were successfully uploaded to cloud storage, and their metadata (including the cloud storage pointer) was recorded on the blockchain.
- For retrieval, confirm that users could retrieve files by querying the blockchain for the metadata/pointer, accessing the cloud storage, and decrypting the file with the correct secret key.
- Quantify success rates: e.g., "100% of uploaded files were successfully retrieved."

Performance Metrics:

- Average uploading, retrieval and Blockchain transaction processing time is significantly higher than the existing system
- The KNN/Naive Bayes algorithm achieved an average node selection accuracy of significant percentage
- Compared to a random node selection strategy, the ML-based approach reduced average retrieval latency is high

Performance Analysis:

- "The improved node selection reduces retrieval latency, enhancing the user experience."
- "Distributing metadata across the blockchain network improves system resilience and availability."

Comparison to Existing Systems:

- Our system introduces additional overhead due to:
- Client-side encryption: Encrypting the file before upload adds processing time on the user's device.
- Blockchain interaction: Recording metadata on the blockchain involves transaction processing, which can take some time.
- ML-based node selection: The time taken by the KNN/Naive Bayes algorithms to select a node.

Limitations and Future Work:

- Acknowledge any limitations t (e.g., limited scalability testing, specific consensus mechanism used in the blockchain).
- Suggest areas for future research or improvement:
- "Further research is needed to evaluate the system's scalability for a large number of users and files."
- "Exploring different consensus mechanisms could improve the blockchain's performance."
- "Investigating automated key recovery mechanisms could address the user's responsibility for key management."

VI. CONCLUISON

In conclusion, the proposed blockchain-based file storage system prioritizes security and data integrity by employing client-side encryption, dual access control, and decentralized metadata management. While this approach may introduce some overhead compared to traditional cloud storage solutions, particularly in terms of upload and retrieval times, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

enhanced security and immutability offered by the blockchain make it suitable for applications where data protection and reliability are paramount. The use of machine learning for node selection further optimizes the system's performance within the decentralized network.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to the following individuals and organizations for their invaluable contributions to this project:

My mentor, Mr. Thangadurai K (AP-CSE), for his guidance, support, and expert insights throughout the development and execution of this research.

Sathish kumar T, Suresh D, Balamurugan U, karuppuchamy M, my team members, for their help in collecting data, analysing results, and providing valuable feedback during the course of the study.

Mahendra Institution, and the Department of Computer Science and Engineering, for providing access to the necessary resources and research facilities.

I also wish to acknowledge the participants of the study, whose cooperation and time were essential for the success of this project.

REFERENCES

[1]. Vijay Sharma Dept. of Computer Engineering, PCCOE Pune, India Prof. G. B. Sambare Dept. of Computer Engineering, PCCOE Pune, India.

[2]. Blockchain-based Secure Big Data Storage on Cloud International Journal of RecentTechnology and Engineering 9(4):37-45 DOI:10.35940/ijrte.D4744.119420

[3]. Ruiguo Yu et al Text Encryption Protocol is used to prevent from malicious user while mining seed. RSA algorithm was also used prevent the data from the unauthorized users.

[4]. Iqbal, Waseem; Khan, Suba's; Rauf, Bilal; Rashid, Imran (2018). [IEEE 2018 IEEE 27

[5]. International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) - Paris, France (2018.6.27-2018.6.29)] 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enter prises (WETICE) - Decentralized Authentication for Secure Cloud Data Sharin,(), 95–99. doi:10.1109/WETICE.2018.00025

[6]. Cloud Harmony, "Service Status," http://cloudharmony.com/ status-of-storage-group-by-regions, 2019 Cloud Security Alliance, "Top Threats," http://cloudsecurityalliance.org/ group/top-threats/, 2016

[7]. M. A. C. Dekar, "Critical Cloud Computing: A CIIP perspective on cloud computing service (v1.0)," European Network and Information security Agency (ENISA), Tech. Rep., 2012.

[8]. Guiyi Wie, Jun Shao, Yang Xaing, Pingping Zhu, Rongxing Lu, "Obtain Confidential or/and authenticity in Big Data by ID-based Generalized Signcryption," Elsevier Journal on information Sciences, 2014.

[9]. Zhiyuan Tan, Upasana T. Nagar, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, Song Wang, and Jiankun Hu, "Enhancing Big Data Security with Collaborative Intrusion Detection," IEEE Cloud Computing, 2014