Journal of Information Systems Engineering and Management
2025, 10 (29s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

A Framework for Secured Access Control of Cloud Data Using Blockchain Technology

Versha Verma[1], Vipin Saxena[2], Vishal Verma[3] and Karm Veer Singh[4]
[1,2,4]*Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India*
[3]*Department of Computer Applications and Science, School of Management and Science, Lucknow, India*
[1]*versha19822005@gmail.com*
[2]*profvipinsaxena@gmail.com*
[3]*drvishalv72@gmail.com*
[4]*kvsingh.bhu@gmail.com*

ARTICLEINFO

Received: 26 Dec 2024

Revised: 14 Feb 2025
Accepted: 22 Feb 2025

ABSTRACT

Cloud computing provides a scalable storage, but ensuring data security and access control are still challenging areas of research. The present work proposes an efficient framework for secure access control of cloud data using blockchain technology. The framework leverages blockchain's decentralized nature to enhance trust and transparency. Smart contracts automate access control, policy for ensuring access of authorized users. Cryptographic technique is used to secure data transmission and storage. The system eliminates reliance on third-party entities, reducing vulnerabilities. Experimental results show improved performance in terms of security and access efficiency. The computed results are presented in the form of table and graph.

Keywords: Cloud Computing, Data Security, Blockchain, Cryptography, Vulnerabilities and Efficiency

INTRODUCTION

By the use of physical machines, users are well connected over the cloud servers which are interconnected through topological structures and only accessible through high-speed internet connectivity. In many public organizations, Government of India (GoI) provides high speed internet connectivity via National Knowledge Network (NKN) and speed of connectivity is more than 1 Gbps which is used for accessing the video contents in a seamless manner. On the other hand, privacy is a key factor for an individual or group of users and must have ability to control the information, share and access it thoughtfully. It depends on the various key aspects of privacy and one of the promising ones is that how much information is shared or accessed. Users tend to be more concerned about recent data disclosure policies which are changed from time to time and even the accessing of the historical data depends upon the access policy. Users are generally comfortable when friends may request own information directly but is passes through the cloud servers and hackers are also connected through the servers and any confidential information may be stolen by the hackers for which users may not automatically alert. In the various commercial organizations, it is very essential to keep large data in a proper and manageable manner so that it may be protected from the unauthorized access by the intruders. For this purpose, organizations must establish rules, guidelines, and procedures to safeguard personally identifiable information, effectively. This institutional security is crucial for maintaining trust and ensuring compliance with privacy standards.

From the literature, it is found that major privacy challenges include trust, uncertainty, and compliance. Trust pertains to the proper management of Personally Identifiable Information (PII), while uncertainty involves verifying information that may have been mishandled by those tasked with its protection. The said challenges underscore the complexities of maintaining privacy in dynamic and global data flows across the world-wide network.

Current access control models are increasingly favored over traditional methods within cloud frameworks. Some of them are

(a) Role Based Access Control (RBAC)

It is a fundamental requirement for any data system. In the RBAC model, users are categorized according to specific role which will determine to access to various functions and the said approach allows only to users to operate effectively in designated critical areas by granting permissions based on assigned roles.

(b) Attribute Based Access Control (ABAC)

It is an access control model that grants permission based on attributes assigned to the users, resources, and the environment. This model considers a wide range of characteristics to make decision on accessing the information. The key components this type of control are attributes, policies and dynamic decision.

(c) Blockchain Based Access Control (BBAC)

This method leverages distributed ledger technology (blockchain) as an access controller to safeguard pointer privacy, alongside an off-chain distributed hash table (DHT) that is authorized by blockchain to protect encoded data. When a user logs in, a new compound identity is created and aggregated. This identity is linked to a unique key that encrypts and decrypts the information. The compound identity consists of key pairings for both the user and the service. Blockchain ensures the verification of both the user’s identity and the service’s access right to the information. It prepares the hash needed to retrieve data from off-chain storage.

LITERATURE SURVEY

There are many algorithms called as encryption and decryption algorithms which support the data privacy when one is accessing from the cloud servers. Chen and Zhao [1] addressed the data security and privacy protection issues in cloud computing, providing foundational insights that inform subsequent research in the field and it highlights the necessity for robust security measures in cloud environments. Further, there are Internet of Things (IoT) devices supporting the accessing of cloud data and the intersection of IoT security and blockchain technology is defined in [2] which provides a comprehensive systematic review of existing security challenges in IoT and propose blockchain-based solutions to enhance data integrity and security. The research work illustrated in this paper identified the open challenges which must be addressed for effective implementation, emphasizing the potential of blockchain to secure IoT environments. The role of blockchain in sustainable supply chain management is explained in [3] which highlights the improvement in blockchain technology in terms of transparency, traceability, and accountability within supply chains. It is a critical activity for fostering sustainable practices and the importance of integrating blockchain into supply chains is also explained for enhancing operational efficiency and environmental sustainability. A systematic review on blockchain technology in the field of Artificial Intelligence (AI) applications is explained in [4] which provide address issues of trust and data integrity in AI systems, also presented open research challenges that could further enhance the synergy between the technologies. The work presented in this paper lays down the foundation for future studies investigating the collaborative potential of blockchain and AI.

Further in the year 2019, Salman et al. [5] presented state-of-the-art overview of security services utilizing the concept of blockchain technology. The comprehensive analysis serves as a valuable resource for understanding the breadth of blockchain's applicability in security frameworks. Blockchain-based database model is explained to ensure data integrity in cloud environments byShukla et al. [6] and the model may be effective related to data tampering and unauthorized access, providing a promising avenue for enhancing the cloud security. Wang et al. [7] provides an idea of cloud storage framework that incorporates blockchain for access control. Deep et al. [8] proposed an authentication protocol for cloud databases using blockchain mechanism which may facilitate secure authentication processes, thereby enhancing overall cloud security. Kumar and Saxena [9] proposed a concept of hybrid approach for encrypting and decrypting the data to be uploaded and downloaded from the cloud servers thus enhanced the security levels for the cloud data. Further, Yang et al. [10] discussed secure data access control in smart grids using blockchain technology which has been introduced as per need for fair accountability and privacy protection in smart grid data sharing, demonstrating blockchain's effectiveness in addressing the related concerns. Privacy-preserving mechanism is investigated in smart homes using blockchain technology that may effectively protect user privacy while enabling secure interactions among smart devices [11]. Agyekum et al. [12] discussed a proxy re-encryption approach which may be used for securing data sharing in IoT using blockchain.

In the recent years, there is tremendous growth in the uploading and downloading data from the cloud servers or one may say that there is exponential growth of storage of data over the cloud servers. In this regard, Kumar and Saxena

[13] proposed BB84 protocol and concept of the genetic approach for security of the cloud data. The data security in cloud computing using the Rivest, Shamir and Adleman (RSA) algorithm has been discussed in [14], Still in the software industries, cracking of the RSA is not recorded in the literature. Gautam and Saxena [15] explained the concept of binary serach algorithm for optimizations of the files and folders to be uploaded and downloaded from the cloud servers, obviously it will optimize the storage of the cloud servers. Choudhary et al. [16-18] also explained the concept of the blockchain technology for faster accessing of the large database stored over the cloud servers and further, clustering approach is used by the authors for accessing of the desired records in the optimize time period from the cloud servers. Akinolaet al.[19] focused on blockchain-enabled security solutions for medical devices which are functioning under cloud environment. Yadav et al. [20] proposed an enhanced cloud data security model using the AES algorithm, demonstrating its effectiveness in protecting sensitive data in cloud storage. Shrivastava et al. [21] also emphasized the significance of encryption technique in safeguarding data against unauthorized access, contributing to the ongoing dialogue about cloud security. Gautam et al. [22] proposed an approach for removal of the duplicate contents of stored data over the cloud servers. The method is applicable on the files and folders which are securely accessed by the users. Saxena et al. [23] enhanced the concept of data cube technology for providing the secure data storage and faster accessing of the database and it is further enhanced through the concept of the blockchain technology [24-25].

METHODS

In the present work, implementation-based research design is produced in which theoretical comparison of RBAC with blockchain is elaborated. Later on, the setup for implementation of secured access control on cloud using blockchain shall be discussed the backbone software CloudSim 3.0. Blockchain for access control in cloud data offers several advantages, enhancing security, transparency, efficiency, dynamism and scalability. Comparison of RBAC control on cloud data using blockchain and without blockchain technology has been presented in the Table 1.

Table 1. Comparison of RBAC with and without Blockchain Technology

Factor	RBAC with Blockchain	RBAC without Blockchain
Control	Decentralized	Centralized
Data Integrity	Enhanced Security	Vulnerable
Auditing	Transparent	Trust-based
Scalability	Scalable, but may have transaction limits	May face bottlenecks
Flexibility	Dynamic and automated adjustments	Static permission changes

The market for blockchain technology is growing rapidly. Many industries are adopting it to improve transparency and security. Sectors like finance, supply chain, and healthcare are leading the sectors with applications include Decentralized Finance (DeFi) and Non-Fungible Tokens (NFTs). The various companies are also using private blockchain for enhancing the operations of the organization. From time to time, regulatory frameworks are being developed to protect consumers and encourage innovation. There is a strong emphasis on sustainability, with a move toward energy-efficient blockchain solutions. Additionally, blockchain is integrating with other technologies like IoT and AI, boosting its effectiveness. The trend position of blockchain is a vital part of future digital changes.

Incorporating blockchain technologies into cloud storage systems is a promising trend that enhances trust and reduces computing costs. This integration makes the system credible, decentralized, and publicly verifiable, allowing connected devices to establish trust through blockchain. The blockchain model enables data owners to maintain ownership and control over the information. The storage system offers improved privacy protection for individual's data, addressing issues related to data privacy. The access control mechanism supported by blockchain is designed to enhance security. Effective access control is essential for ensuring data privacy, making it a critical tool in this context.

A Framework for using Blockchain on Cloud Data

In the proposed model, data owner, data user, cloud server, and blockchain are recommended as major components. Access of data kept by any specific user is control through smart contracts of blockchain. Ethereum smart contracts are used by data owners and users to store and retrieve ciphertext data for the purpose of executing encryption and decryption algorithms. The blockchain records each contract call and due to this information exchanged between data owners and users is non-repudiation and non-tampering. A framework is shown below in the following Figure 1.

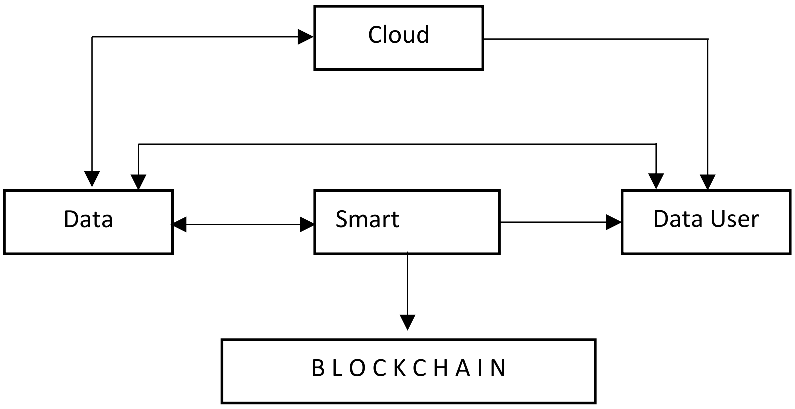

Figure 1. A Framework for Access Management of Cloud Data using Blockchain

Data owners are responsible for different tasks like, designing the access control policies, assigning attribute sets, uploading encrypted files on cloud server, installing smart contracts on blockchain and adding valid access durations for data users which access an encrypted file stored in the cloud when its attributes set matches the access structure given in the ciphertext. In order to retrieve the content key needed to decrypt the encrypted file, data users can decipher the received ciphertext. Decentralized blockchain technology is used through Ethereum 2.0 which facilitates the creation and use of smart contracts and decentralized applications. The steps for secured access control are given below:

Step1: Smart contract created by data owner are deployed in Ethereum;

Step2: Data Owner receives the contract address;

Step3: File ID is kept in the smart contract by the data owner;

Step4: Data Owner collects the contract address, File ID, encrypted file and then upload to the cloud server;

Step5:Data Owner saves the path of file given by cloud server;

Step6: Data Owner stores the ciphertext of the encrypted document in the Ethereum blockchain software;

Step7: Access request is sent by data user to data owner;

Step8:The secret key of data user is encrypted by data and saved into smart contract;

Step9: Contract details along with user information is shared by data owner;

Step10: Encrypted files are downloaded by data users from the cloud server;

Step11:The secret key for ciphertext is also obtained by data users from smart contract.

RESULTS

It is obvious that addition of an extra layer of blockchain will improve the security of data on cloud from access point of view. The extra layer will also increase the response time of access requests of users. RBAC access mechanism is selected and implemented with and without blockchain using Ethereum simulation tool. A parameter total response time is the time taken to process an access request from submission to granting or denying access can be calculated by using formula:

$$T_{(response)} = T_{(create)}+T_{(propagate)}+T_{(validate)}+T_{(confirm)}+T_{(decision)} \quad (1)$$

Average response time and peak response time are also computed for analysis of the data. The following Table 2 contains the data of response time computation using simulation tool Ethereum on CloudSim 3.0. In first case RBAC was implemented on cloud and response time is computed and further experiment shows the implementation of RBAC with and without blockchain concept.

Table 2. Comparison of Response-Time for RBAC with and without Blockchain

Access Request	RBAC with Blockchain (in ms)	RBAC without Blockchain (in ms)
50	7 ms	15 ms
100	11 ms	27 ms
200	17 ms	39 ms
500	28 ms	67 ms
1000	40 ms	104 ms

Data presented in the above is represented in the form of line chart as shown in the Figure 2. It has been analyzed that while increasing the number of access requests from 50 to 1000, response time of RBAC with blockchain increases from 7 ms to 40 ms while on other hand, the response time without blockchain increases from 15 ms to 104 ms which is higher and expected in the second case.

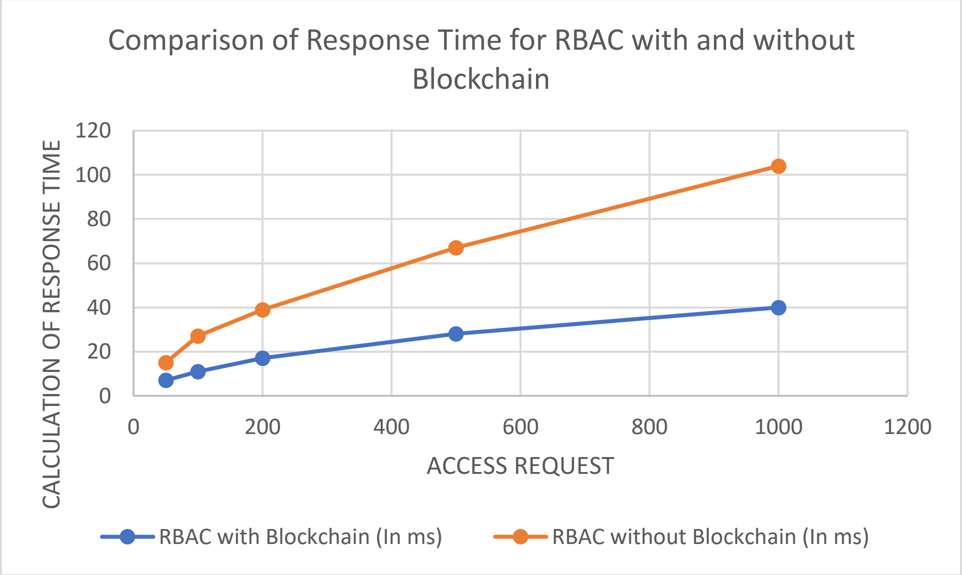

Figure 2. Comparison of Response Time for RBAC with and without Blockchain

From the given data in Table 2 and Figure 2, average response time and peak response time are also calculated. Average response time and peak response time for system with blockchain is 21.5 ms and 40 ms but it is 50.4 ms and 104 ms for system without blockchain which shows that the blockchain technology reduces the average response time. It is shown below in the table 3.

Table 3. Comparison of Average Response-Time and Peak Response-Time

System Type	**Average Response Time** **(In ms)**	**Peak Response Time** **(In ms)**
Without Blockchain	21.5 ms	40 ms
With Blockchain	50.4 ms	104 ms

CONCLUSION

Traditional cloud access control systems offer simplicity and manageability, and it may be vulnerable to centralized risks and trust issues. In contrast, blockchain enhances security, accountability, and flexibility, making it an appealing choice for organizations requiring robust access control in sensitive environments. However, implementing blockchain comes with its own challenges, such as scalability and transaction speed, which need to be considered based on specific use cases. In the present work, recommendation for using RBAC mechanism using blockchain has been recommended. It is concluded that blockchain based access control mechanism will always be excellent choice and secure but response time of such systems will always increase due to extra layer of security. The work may be extended for proposing control mechanism to reduce the response time and also will address the cost effectiveness of system.

REFRENCES

[1] Chen, D., and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing, *International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, pp. 647-651, https://doi.org/10.1109/iccsee.2012.193

[2] Khan, M. A., and Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[3] Saberi, S., Kouhizadeh, M., Sarkis, J., and Shen, L. (2018). Blockchain Technology and its Relationships to Sustainable Supply Chain Management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

[4] Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. IEEE Access, 7, 10127–10149. https://doi.org/10.1109/access.2018.2890507

[5] Salman, T., Zolanvari, M., Erbad, A., Jain, R., andSamaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. IEEE Communications Surveys & Tutorials, 21(1), 858–880. https://doi.org/10.1109/comst.2018.2863956

[6] Shukla, Rahul Deo, Pratap, Ajay and Suryavanshi, Raghuraj Singh. (2019). Packet Blocking Performance of Cloud Computing Based Optical Data Centers Networks under Contention Resolution Mechanisms, Journal of Optical Communications, vol. 44, no. s1, 2023, pp. s853-s862. https://doi.org/10.1515/joc-2019-0287

[7] Wang, S., Wang, X., and Zhang, Y. (2019). A Secure Cloud Storage Framework With Access Control Based on Blockchain. IEEE Access, 7, 112713–112725. https://doi.org/10.1109/access.2019.2929205

[8] Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., and Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. Sensors, 19(20), 4444. https://doi.org/10.3390/s19204444

[9] Kumar, J., Saxena, V. (2020), Hybridization of Cryptography for Security of Cloud Data, International Journal of Future Generation Communication and Networking Vol. 13(4) 4007–4014.

[10] Yang, W., Guan, Z., Wu, L., Du, X., andGuizani, M. (2021). Secure Data Access Control With Fair Accountability in Smart Grid Data Sharing: An Edge Blockchain Approach. IEEE Internet of Things Journal, 8(10), 8632–8643. https://doi.org/10.1109/jiot.2020.3047640

[11] Qashlan, A., Nanda, P., He, X., and Mohanty, M. (2021). Privacy-Preserving Mechanism in Smart Home Using Blockchain. IEEE Access, 9, 103651–103669. https://doi.org/10.1109/access.2021.3098795

[12] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., and Gao, J. (2022). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. IEEE Systems Journal, 16(1), 1685–1696. https://doi.org/10.1109/jsyst.2021.3076759

[13] Kumar, J.,Saxena, V. (2022), Cloud Data Security through BB84 Protocol and Genetic Algorithm, Baghdad Science Journal, Vol. 19(6), Special Issue,1445-1453, doi: https://dx.doi.org/10.21123/bsj.2022.

[14] Hanupriya, L., and Ramya, S. A. (2023). Data security in cloud computing using RSA Algorithm. 2, 3(2), 95–98. https://doi.org/10.46632/daai/3/2/18

[15] Gautam, D. and Saxena, V. (2023). Optimization of Storage of Cloud Servers Through Binary Search Algorithm, *IEEE 7th Conference on Information and Communication Technology (CICT)*, Jabalpur, India, 2023, pp. 1-6, doi: 10.1109/CICT59886.2023.10455361.

[16] Choudhary, B. and Saxena, V. (2023). Blockchain Implementation for Faster Accessing of Database of Banking Industry, International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 11(7), 504-512.

[17] Choudhary, B. and Saxena, V. (2023) K-Means Clustering of Cloud Data using Weka and R Language. International Journal of Computer Applications. Vol. 184(49), 33-39, doi=10.5120/ijca2023922613

[18] Saxena, V., Singh, K.V. and Choudhary, B. (2023) Fuzzy Elgamal Technique for Securing Data Over Cloud. International Journal of Computer Applications. Vol. 184(51), 38-44. doi=10.5120/ijca2023922642

[19] Akinola, O., Akinola, A., Oyekan, B., Oyerinde, O., Adebiyi, H. F., and Sulaimon, B. (2024). Blockchain-Enabled Security Solutions for Medical Device Integrity and Provenance in Cloud Environments. International Journal of Innovative Science and Research Technology (IJISRT), 123–135. https://doi.org/10.38124/ijisrt/ijisrt24apr225

[20] Yadav, V., Soni, M. K. and Pratap, A. (2024). Secured Identity and Access Management for Cloud Computing Using Zero Trust Architecture. In: Chaturvedi, A., Hasan, S.U., Roy, B.K., Tsaban, B. (eds) Cryptology and Network Security with Machine Learning. ICCNSML 2023. Lecture Notes in Networks and Systems, vol 918. Springer, Singapore. https://doi.org/10.1007/978-981-97-0641-9_47

[21] Shrivastava, S., Soni, M.K. and Pratap, A. (2024). Analysis of Security Aspect in Cloud Implementation: A Case Study of Google Cloud Provider. In: Chaturvedi, A., Hasan, S.U., Roy, B.K., Tsaban, B. (eds) Cryptology and Network Security with Machine Learning. ICCNSML 2023. Lecture Notes in Networks and Systems, vol 918. Springer, Singapore. https://doi.org/10.1007/978-981-97-0641-9_38

[22] Gautam, D., Rimer,S. and Saxena, V. (2024), Secure Access of Folders and Files after Removal of Duplicacy over the Cloud, International Journal of Computer Network and Information Security (IJCNIS), Vol.16, No.1, pp.48-60, doi:10.5815/ijcnis.2024.01.04

[23] Saxena, V., Verma, V., Verma, V. and Singh, K.V. (2024). Data Cube Technology for Accessing of Large Database. In: Devi, B.R., Kumar, K., Raju, M., Raju, K.S., Sellathurai, M. (eds) Proceedings of Fifth International Conference on Computer and Communication Technologies. IC3T 2023. Lecture Notes in Networks and Systems, vol 897. Springer, Singapore. https://doi.org/10.1007/978-981-99-9704-6_4

[24] Kumar, J., Kumar, H., Singh, K.V. and Saxena, V. (2024), Secure Data Storage and Retrieval over the Encrypted Cloud Computing, International Journal of Computer Network and Information Security, Vol.16, No.4, pp.52-64, 2024. doi:10.5815/ijcnis.2024.04.04

[25] Verma, V., Kumar, H., Saxena, V., Singh, K.V. and Verma, V. (2025) Blockchain Technology: A Comprehensive Review, Grenze International Journal of Engineering and Technology, January Issue, 2445-2458, Grenze Scientific Society, Grenze ID: 01. GIJET.11.1.et.