

## SERVER SECURITY USING CLOUD COMPUTING IN BLOCKCHAIN

Putta Srivani<sup>1</sup>, Y. Akshitha<sup>2</sup>, M. Ahalya<sup>3</sup>, Y. Sri vaishnavi<sup>4</sup>

<sup>1</sup>Associate professor, Department of IT, Malla Reddy Engineering College For Women (Autonomous Institution), Maisammaguda, Dhulapally, Secunderabad, Telangana-500100

<sup>2,3,4</sup>UG Scholar, Department of CS, Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda, Dhulapally, Secunderabad, Telangana-500100

Email : Pulla.srivani@gmail.com

### ABSTRACT

Cloud Computing is one of the most convenient, scalable, low-cost, accessible, and highly available technologies for delivering a variety of services in the era of digitalization. However, security concerns such as data breaches, privacy issues, and integrity risks remain significant challenges in cloud environments. This paper explores the integration of blockchain technology into Cloud Computing as a potential solution to these security concerns. Blockchain is a decentralized and cryptographically secure system of linked records, known as blocks, which provides an immutable ledger that enhances data integrity and transparency. The paper will discuss the disruptive potential of blockchain in addressing the vulnerabilities of cloud services and how blockchain-based electronic wallets can ensure protection of user data in cloud environments. In addition, the paper will provide a detailed overview of applications and recent technological advancements in combining blockchain with cloud computing. This approach promises to revolutionize cloud security by leveraging blockchain, providing enhanced protection and trust for cloud users.

**Keywords:** Cloud Computing; Blockchain Technology; Data Security; Data Integrity; Decentralization; Cryptography

### 1 INTRODUCTION

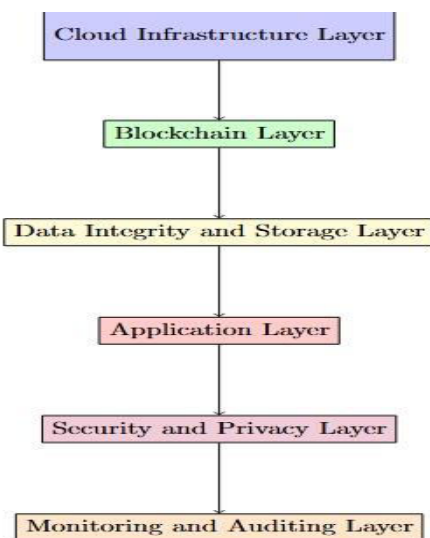
It is due to such fast-paced digitalization in different sectors that Cloud Computing has emerged as a very vital technology. Scalable resources, ease of access, and changes in the management, storage, and processing of data in business and individuals' ways have transformed all of these. Since cloud computing works on-demand without the physical need for infrastructure, the benefits have been significant in cost savings, operational flexibility, and reach into global

markets. Despite these advantages, several security issues have emerged as pressing concerns for users and service providers. Key issues range from compromising data privacy to security breaches with regards to sensitive information integrity.

Taking into consideration such issues, blockchain has emerged as a developing solution in response to these issues. It presents a decentralized, cryptographically secure form of data storage, with the records, or "blocks," being linked and therefore immutable,

ensuring integrity and transparency. Integrating blockchain with cloud computing can significantly enhance security in cloud services. Its distributed ledger system gives greater transparency while reducing the risks associated with centralized control and even in cases where data may be tampered with during a breach.

This paper explores the potential of blockchain technology in improving security in cloud computing. It examines how blockchain can enable decentralization to safeguard user data in environments requiring high degrees of trust and integrity in data. It also considers how blockchain-based electronic wallets further improve transactions and the details of a user in the cloud environment. Based on the analysis of recent developments, this paper introduces a conceptual framework of how blockchain can revolutionize security perspectives in cloud computing, and it further provides an elaborate discussion of applications and challenges involved with the use of these technologies.



**Fig 1: System Architecture**

## II. RELATED WORK

### 1. Blockchain-based Cloud Manufacturing: The Decentralization

**Authors:** A. Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, G. Q. Huang (2019)

The authors in the paper suggest the use of blockchain for the decentralization of cloud manufacturing systems. Traditional centralized servers in cloud manufacturing pose risks such as data manipulation and loss of data integrity as well as lack of transparency. In summary, by decentralizing such processes via blockchain, a safer, transparent, and trustworthy system is promised by facilitating numerous stakeholders' interactions on one immutable shared ledger. Such a contribution extends the body of knowledge for blockchain use in cloud manufacturing as trust, integrity, and transparency form some of its most basic critical values.

### 2. Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities

**Authors:** A. Harshavardhan, T. Vijayakumar, S. R. Mugunthan (2018)

This paper deals with the integration of blockchain in cloud computing to overcome vulnerabilities inherent in cloud infrastructures. Some of the issues, like data breaches, unauthorized access, and loss of data, that are still common in the cloud systems of olden times have not been eliminated. They intend to integrate blockchain



into a decentralized, non-modifiable data structure so that transactions and data storage can improve privacy and security. The work stresses that blockchain can defend against internal and external threats and enhance overall trustworthiness in cloud services.

### 3. Blockchain and Supply Chain Management

**Authors:** A. Jabbari, P. Kaminsky (2018)

Jabbari and Kaminsky (2018) discuss the application of blockchain technology in supply chain management, which is an integral part of many cloud-based systems, especially in logistics and data management. Blockchain provides transparency and tamper-proof records that guarantee the authenticity of the transactions and the integrity of the supply chain. Their study is not directly on cloud computing, but it is very relevant because it shows how blockchain can be integrated into a system with a cloud in order to increase transparency, avoid fraud, and improve traceability across cloud-dependent industries.

### 4. Blockchain Technology in Cloud Computing: A Systematic Review

**Authors:** M. K. R. Ingole, M. S. Yamde (2018)

Ingole and Yamde provide a comprehensive review of the literature on blockchain applications in cloud computing. The paper systematically reviews various works that have integrated blockchain with cloud infrastructures and explores its application in securing the cloud storage of data, data privacy improvement, and automatic

process by smart contracts. This work is a contribution to the field, as it will organize the knowledge on how blockchain is applicable to cloud computing, hence providing a clearer understanding of challenges and benefits through the use of blockchain to resolve common issues in cloud security.

## III IMPLEMENTATION

Integration of blockchain technology within cloud computing environments is approached by adapting existing cloud infrastructures to utilize the distributed and secure nature of blockchain. Hybrid cloud architectures could be a common approach that utilizes blockchain for critical data, while less sensitive workloads remain on traditional cloud services. Blockchain-based smart contracts can execute tasks such as billing and resource allocation, reducing errors caused by human intervention. Access control also becomes better because there are no more intermediaries.

It provides an immutable ledger to validate cloud-stored data and hence ensures data integrity. Rather than storing raw data, blockchain can store its hash value, which is easily detected in case of any unauthorized alteration. The distributed ledger further allows for real-time auditing of all data transactions to enhance transparency and accountability. Risks associated with centralized control include data breaches and unauthorized access.

Moreover, blockchain electronic wallets can safeguard user information within cloud platforms. In these wallets, data encryption and decryption is achieved by public and private keys such that only an authorized person has access to it. When combined with the wallet



provided by the blockchain, multi-factor authentication is required for gaining access to the cloud-based resources.

To overcome the performance challenges associated with blockchain's resource-intensive consensus mechanisms, lightweight algorithms such as Proof of Authority or Practical Byzantine Fault Tolerance can be used. The consensus models provide faster, more scalable blockchain solutions. For larger datasets, off-chain storage can be used, storing only the blockchain references or hashes, thus balancing security with scalability.

The continuous monitoring of blockchain helps ensure its effectiveness in cloud computing. Continuous auditing and vulnerability assessments ensure the integrity of the system, which is very helpful in solving security threats. Blockchain's transparency features help in regular reviews that make sure cloud environments remain secure and efficient.

#### IV ALGORITHM

In conclusion, integration of blockchain technology with cloud computing holds great promise in the solution of several critical challenges related to security, integrity of data, and transparency. The studies reviewed in this survey highlight the potential of blockchain to revolutionize services based on clouds by offering decentralized solutions that ensure trust and transparency, which are often lacking in traditional cloud infrastructures.

Blockchain can improve the security of cloud computing systems through the use of immutable records and decentralized control over data that does not allow unauthorized access or tampering. This is especially crucial

for those industries that use sensitive data storage and transaction management. In this regard, the work of Vatankhah Barenji et al. (2019) demonstrates how decentralization with blockchain can secure cloud manufacturing systems, and Harshavardhan et al. (2018) have demonstrated the use of blockchain to safeguard cloud systems from security vulnerabilities.

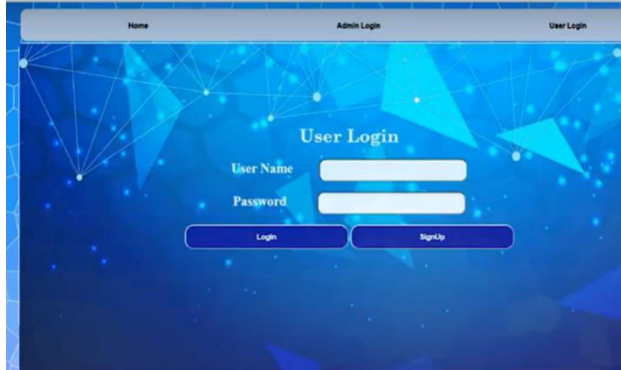
Moreover, blockchain's inbuilt feature of keeping the data transparent, auditable, and traceable is beneficial for supply chain management industries, as shown by Jabbari and Kaminsky (2018). This transparency will increase the authenticity of cloud-based transactions and allow for real-time monitoring, ensuring the integrity of the supply chain and other interconnected services.

Despite its promising applications, the adoption of blockchain in cloud computing faces certain challenges, such as scalability, privacy concerns, and computational overhead. While blockchain can offer solutions to security concerns, the need for research to overcome these challenges remains critical for its widespread adoption in cloud environments. Moreover, advancements in consensus mechanisms, smart contract automation, and privacy-preserving techniques will be essential for the seamless integration of blockchain into cloud systems.

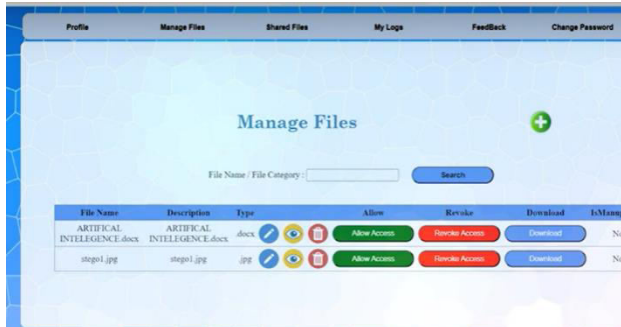
The next phase of work, with respect to scalability and performance optimizations as well as enhanced features for privacy, shall hold the key to bringing about blockchain's true promise for cloud computing. When blockchain successfully addresses these concerns, the reliability and trustworthiness of

services provided by clouds may become much more improved than earlier days.

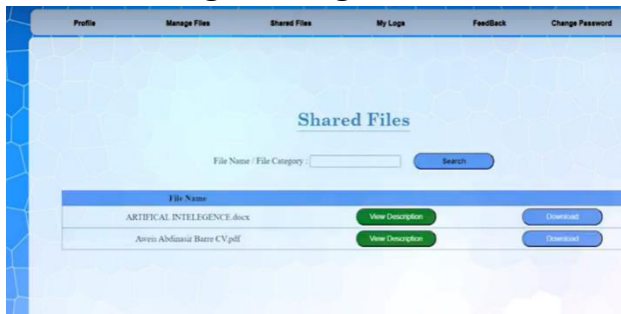
## RESULT



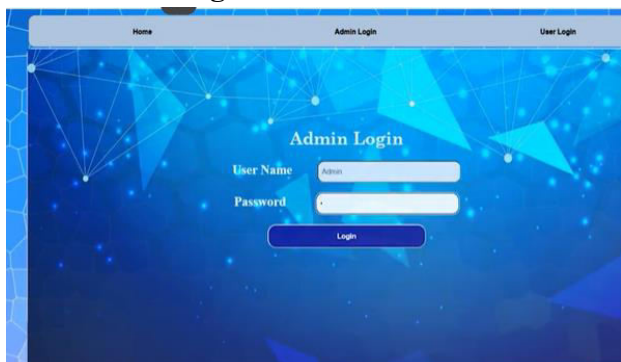
**Fig1: User Login**



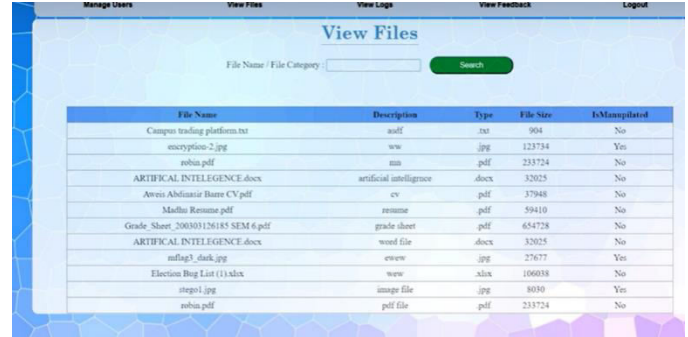
**Fig2: Manage Files**



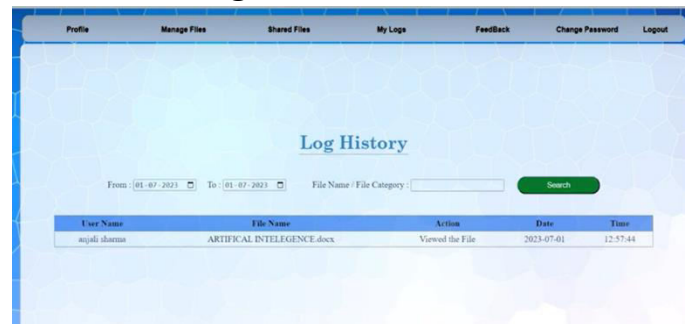
**Fig3: Shared Files**



**Fig4: Admin Login**



**Fig5: View Files**



**Fig6: Log History**

## CONCLUSION

The promise of using blockchain technology to supplement cloud computing will be immense in helping overcome many pressing issues of security, integrity, and transparency. Based on the various studies in this review, blockchain-based solutions will certainly transform services offered over clouds with greater decentralization for trusted transparency, something largely absent from traditional cloud infrastructure.

Blockchain can improve cloud security through immutable records and decentralized control over data, which prevents unauthorized access and tampering. This is highly relevant for industries that have sensitive data storage and transaction management. The research by Vatankhah Barenji et al. (2019) demonstrates how



decentralization through blockchain can make cloud manufacturing systems more secure, while Harshavardhan et al. (2018) highlight how blockchain can be applied to protect cloud systems from security vulnerabilities.

In addition, blockchain allows for self-sustaining transparent, auditable, and traceable data, an advantage for any industry or business, like supply chain management, that Jabbari and Kaminsky showed in 2018. This transparency makes cloud-based transactions more authentic and helps in real-time monitoring and integrity of supply chains as well as other inter-related services.

Despite the promising applications, blockchain in cloud computing faces challenges in terms of scalability, privacy, and computational overhead. Even though blockchain can offer solutions to the security concerns, the critical need for research in these areas remains a significant hurdle for the adoption of blockchain in the cloud environment. Additionally, the future advancement of consensus mechanisms, smart contract automation, and privacy-preserving techniques will be critical for the smooth integration of blockchain into cloud systems.

In future work, further exploration into blockchain's scalability, performance optimization, and privacy features would be key to realizing the full potential of blockchain in cloud computing. This is because addressing these concerns can significantly enhance the reliability and trustworthiness of cloud services, paving the way for more secure and efficient cloud computing environments.

## REFERENCES

- [1] A. Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang and G. Q. Huang, "Blockchain-based cloud manufacturing: Decentralization", arXiv:1901.10403, 2019, [online] Available: <http://arxiv.org/abs/1901.10403>.
- [2] A. Harshavardhan, T. Vijayakumar and S. R. Mugunthan, "Blockchain technology in cloud computing to overcome security vulnerabilities", Proc. 2nd Int. Conf. I-SMAC (IoT Social Mobile Anal. Cloud)(I-SMAC) I-SMAC (IoT Social Mobile Anal. Cloud)(I-SMAC) 2nd Int. Conf., pp. 408-414, Aug. 2018.
- [3] A. Jabbari and P. Kaminsky, "Blockchain and supply chain management", 2018.
- [4] M. K. R. Ingole and M. S. Yamde, "Blockchain technology in cloud computing: A systematic review", 2018.
- [5] C. Qiu, H. Yao, C. Jiang, S. Guo and F. Xu, "Cloud computing assisted blockchain-enabled Internet of Things", IEEE Trans. Cloud Comput., Jul. 2019.
- [6] D. Dujak and D. Sajter, "Blockchain applications in the supplychain" in SMART Supply Network, Cham, Switzerland: Springer, pp. 21-46, 2019.
- [7] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire and P. R. Inácio, "Security issues in cloud environments: A survey", Int. J. Inf. Secur., vol. 13, no. 2, pp. 113-170, 2014.



- [8] D. B. Rawat, V. Chaudhary and R. Doku, "Blockchain: Emerging applications and use cases", arXiv:1904.12247, 2019, [online] Available: <https://arxiv.org/abs/1904.12247>.
- [9] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities", Proc. IEEE 8th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON), pp. 469-474, Oct. 2017.
- [10] D. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach", IEEE Consum. Electron. Mag., vol. 8, no. 4, pp. 38-44, Jul. 2019
- [11] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain technology overview", arXiv:1906.11078, 2019, [online] Available: <http://arxiv.org/abs/1906.11078>.
- [12] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments", 2017.
- [13] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Renew. Sustain. Energy Rev., vol. 100, pp. 143-174, Feb. 2019.
- [14] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology", Procedia Comput. Sci., vol. 123, pp. 116-121, 2018.
- [15] F. Knirsch, A. Unterweger and D. Engel, "Implementing a blockchain from scratch: Why how and what we learned", EURASIP J. Inf. Secur., vol. 2019, no. 1, pp. 2, Dec. 2019
- [16] S. Sharma, G. Gupta and P. R. Laxmi, "A survey on cloud security issues and techniques", arXiv:1403.5627, 2014, [online] Available: <http://arxiv.org/abs/1403.5627>.
- [17] G. J. Katuwal, S. Pandey, M. Hennessey and B. Lamichhane, "Applications of blockchain in healthcare: Current landscape challenges", arXiv:1812.02776, 2018, [online] Available: <http://arxiv.org/abs/1812.02776>.
- [18] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment", J. Med. Syst., vol. 42, no. 8, pp. 156, Aug. 2018.
- [19] L. Zhang, "A blockchain-based decentralized cloud resource scheduling architecture", Proc. Int. Conf. Netw. Netw. Appl. (NaNA), pp. 324-329, Oct. 2018.
- [20] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey", Int. J. Web Grid Services, vol. 14, no. 4, pp. 352-375, 2018.