Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 11, 2025

APPLYING BLOCKCHAIN TECHNOLOGY FOR ENHANCED CLOUD COMPUTING SECURITY: A REVIEW

Muhammad Haris[*1], Syed Khaldoon Khurshid[2], Talha Waheed[3], Idrees Mustafa[4], Abdul Qudoos[5]

[*1,2,3,4,5]*Computer Science Department University of Engineering and Technology* Lahore, Pakistan

[*1]harisbhaya786@gmail.com,[2]khaldoon@uet.edu.pk,[3]twaheed@uet.edu.pk,[4]idreesrind234@gmail.com, [5]qudoosrafique666@gmail.com

DOI:https://doi.org/10.5281/zenodo.17512552

Keywords
Blockchain, cloud computing security, smart contracts, decentralized ledger

Article History
Received: 12 September 2025
Accepted: 22 October 2025
Published: 03 November 2025

Corresponding Author: *
Muhammad Haris

Abstract

The evolution of cloud computing has extremely changed the storage and management of data by offering vital accessibility and flexibility mechanisms. Nevertheless, this change has also brought a variety of security challenges including data breaches, unauthorized access, information leaks, and service disruptions. These threats are only a few of the risks companies face in the digital landscape. Therefore, the aim of this article is to explore how blockchain can provide a solution to strengthen cloud security. This paper, particularly, examines the decentralized nature of blockchain to evaluate its effectiveness in ensuring data integrity and credibility. Furthermore, this study objects to fill gaps in existing literature on the connection of blockchain and cloud computing by utilizing a variety of research methods. The main goal is to prove that how blockchain is able to support cloud security improvements and address key queries in this area.

INTRODUCTION

cloud computing's emergence has revolutionized how are businesses and individuals managing their data. It has been shifting from traditional data management methods to more flexible and scalable models. However, the ability to access and manage data from virtually anywhere with the help of remote servers and fast internet connections is truly amazing. Under no circumstances, a advancement comes without significant challenges. The concerns surrounding the security of sensitive data in centralized environments has also triggered with the growth of adopting cloud services. High-profile data breaches and instances of unauthorized access have become common, that has led the businesses that rely on cloud services to high risks [1][2]These breaches not only endanger confidential information but also erode trust in cloud providers, that results in severe financial and reputational consequences. While traditional security measures like firewalls and encryption have been effective to some extent, they often struggle to keep up with the complexities and dynamic nature of modern cloud environments [3]. The limitations of these conventional methods have driven the findings of innovative plus efficient way out to secure data also ensure user privacy. This is where blockchain technology comes in. Originally developed to support cryptocurrencies [4], blockchain operates on a decentralized structure, offering significant advantages in terms of security, transparency, and immutability over traditional centralized systems.

Blockchain is an innovative technology proposed by Satoshi Nakamoto for Bitcoin in 2008, the technology of a distributed ledger (DLT) that securely stores transactions in an untrusted decentralized network. Blockchain transactions are taken as a series (or chain) of cryptographically linked blocks, which cannot be interrupted. Decentralization, on the blockchain is how it reduces the risks of fraud and how it eliminates sole points of collapse. One other feature of great importance: data is immutable, meaning that once logged, data can not be changed. Furthermore, all participate in a ledger that is synchronized and verifiable, which creates a trust and ac- countability. In the proof of Work and the proof of staking consensus structures, blockchain validates transactions as well as, to ensure data integrity, goes. This makes blockchain a great solution to solving cloud computing problems including data breaches due to unauthorized retrieve. According to the figures of various surveys, the global spending on blockchain will grow up to 19 billion in 2024 [1]. In light of that, its growing adoption in various industries indicates the potentials to create secure and transparent systems.

This paper aims to explore how and where blockchain technology might be able to secure the cloud computing. The purpose of this paper is to evaluate the possiblities of what would blockchain bring to the cloud security frameworks by reviewing the existing work as well as considering the related case studies. It also addresses the challenges and limitations of such integration, and offers insights into future research and development directions in this fast moving area. This review in the end tries to make it clear how blockchain could prove to be a vital weapon in defending cloud environments from novel threats of security.

I. RELATED WORKS

A. Security Challenges in Cloud Computing

Data Breaches: In cloud computing, data breaches are a major challenge, which means that they present a big risk to organizations as well as individual people [5]. In the past year, according to the 2022 Cybersecurity Breaches Survey, 39 percent of organizations experienced a cyberattack or data breach that hit your cloud services. As an example, the Capital One breach of 2019 uncovered more than 100 million clients' personal data[3] as well as exposing the vulnerabilities that may exist among cloud storages. In this case, a misconfigured firewall allowed an attacker access to pay and reputational cost with access to key information. These incidents therefore underline the importance of placing in place stronger security measures to prevent cloud environments from illegal access and data breaches [6].

Unauthorized Access: The access to the cloud continues to be one of the main issues of cloud computing. The reasons are difficulties in identity management and access control. Many traditional security measures such as passwords do not prove to be enough in protecting sensitive data in cloud environments. This problem becomes even more difficult due to the growing complexity of managing user identities on multiple platforms. For example, it could include allowing someone else have access to your confidential information by giving them your shared account and weak authentication methods. Similarly, many organizations struggle to put RBAC into practice, because such controls are essential to limit user permissions to those corresponding to their particular roles. In the absence of appropriate identity management systems, there is great risk of unlawful access to cloud resources.

Data Integrity and Availability: The challenge portends safely maintaining data integrity and availability in cloud computing. Data integrity deals with the reliability should the data be accurate during the entire life cycle, data availability is the ability of data to be accessed when needed. There are various sources which risk can be of data loss, corruption and data loss as hardware fails, software crash, and malware attack. For example, criminals can encrypt some critical data that renders it inoperative to organizations; causing massive operational disruptions. And remember it is cloud service outages that can sabotage the access to important data and applications in the case of technical issues or other attacks on the cloud service. It complicates business continuity to a very severe extent. As organizations increasingly use cloud services,

[1] it is more necessary than ever to protect data integrity and to make data availability available.

Compliance and Legal Issues: Organizations that use cloud services have extra challenges to fulfill regulatory require-ments, since the cloud internal data center or service provider facilities may be located in other countries. There are many industries bound by very strict data safety and privacy laws such as General Data Protection Regulation (GDPR) in European Union and Health Insurance Portability and Accountability Act (HIPAA) in the United States. The main part of these guidelines is about certain security measures that are necessary to ensure the secrecy of some data and correct input handling. However, in cloud computing, the common responsibility model may instill uncertainty on compliance obligations. But it can also create some questions to be answered if the responsibility lies with the customer, or the cloud service provider. This doubt can lead to compliance gap that increases the risk of legal issues and the financial penalties. The need for navigation of these complex regulatory requirements while practicing cloud security in accordance to legal standards is crucial. This means one of the keys to successful cloud security.

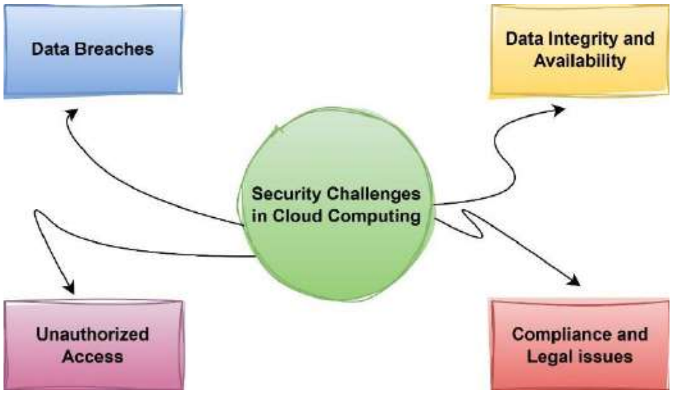
Data Breaches
Data Integrity and Availability
Security Challenges in Cloud Computing
Unauthorized Access
Compliance and Legal issues

Fig. 1.

B. Overview of Blockchain Technology

Decentralization:

Blockchain technology boasts a decentralized structure. Blockchain uses a distributed network of nodes and operates differently with every single system being controlled by a centralized structure. By being decentralized, this reduces the risk of a single node of failure, and increases security. No one party can dominate or manipulate the entire system, because of that. Once had a copy of complete ledger in each participant in the network. This means that malicious actors are extremely difficult to change or harm the data without the majority of the network[7].

Immutability: Immutability refers to term that implies data once stored on the blockchain cannot be altered or deleted. The secure and unchangeable chain is any transaction which is linked cryptographically to the previous one. This feature guarantees to confirm the fidelity of any entry and to provide a verifiable audit trail. Immutability implies designed incor- ruptibility of the data, stores integrity of the distributed data and builds trust in the network participants [8].

Transparency: Blockchain technology offers increased trans- parency because each nodes on the network can have access to the same information. The benefit is that it's accountable, for it records every transaction and can be scrutinised by anyone deemed within the authorised group. Especially, it is precious in the context when trust is necessary, because it enables the verification of transactions without the need to rely on the central authority. Improving security is a key feature for this. However, it does prevent fraudulent actions easily, which makes these actions detectable.

Data Security: It is due to its distributed structure and how the data is stored that blockchain technology's data security is reinforced. Each block has a piece of data. Once added to the blockchain, the data is protected with strong cryptography, like hashing algorithms like SHA-256. This is so altering data becomes next to impossible, because if you change a block, you would need to change every other block and thus need an enormous computing power[9]. Public key encryption is also used for secure identification and transaction protection by blockchain. But digital signatures give participants the right to confirm the legitimacy of transactions without giving their privacy away. Also, the blockchain has ways like Proof of Work (PoW) and Proof of Stake (PoS) to stop malfeasants from getting control of the network. They're smart contracts (also called automated programs), and they operate based on rules without third party involvement. Additionally, it provides better security as action will be executed as agreed. The features make blockchain a strong solution against data breaches, fraud and unauthorized alterations [10].

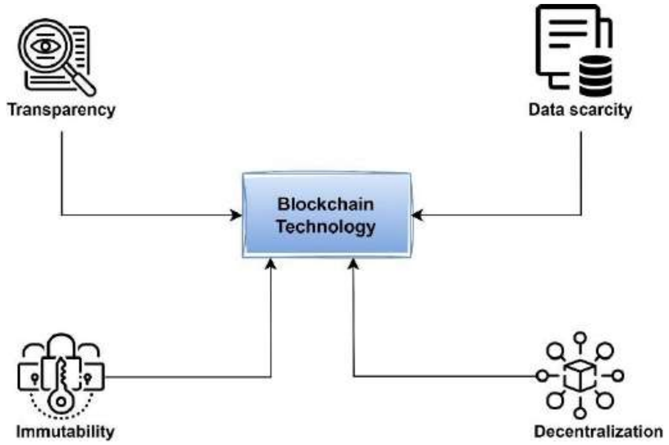

Fig. 2.

subsectionTypes of Blockchain Public Blockchains: There are public blockchains such as Bitcoin or Ethereum. This creates an open network where everyone can join as network nodes, participants in verifying transactions, and have access to full ledger. For this openness, there is decentralization and transparency but also scalability and privacy as the tas. But all the information is visible to the public in the meantime. This means that your network may not be able to process massive volumes of transactions and there are reservations about exposing sensitive data.

Private Blockchains: Basic Private blockchains can be ac-cessed by a selected group of authorized users. To participate in it you need permission.

Most of the time these networks are used by organizations that wish to control their data and transactions more. They provide better privacy and scalability than the private blockchains. Public blockchains offer some decentralization benefits that they might sacrifice to do that.

Consortium Blockchains: Consortium blockchains are man- aged by a group of organisations rather than a centralized one. This is a hybrid between both a public or a private blockchain. It enables authorized parties to collaboratively control and cooperate. The use of consortium blockchains is especially helpful in the industries where there are multiple stakeholders and these participants need to collaborate to manage privacy and security. [11]

Smart Contracts: Smart Contracts are self executing agree- ments, where for some or all of the terms, conditions or where all of it is directly coded in written code. They do move through blockchain networks and they execute and enforce contractual agreements automatically when those conditions are met. The importance of smart contracts in improving security and automating processes is significant:

Automation: By automating complex processes with smart contracts, middle men are removed. There are no errors from human because of enhanced efficiency.

Security: Blockchain technology provides transparent and immutable security, and because of this smart contracts can expand. It cannot be modified, and all participants can verify itself execution.

Trust: On this decentralized platform, smart contracts build trust among participants. All outcomes in smart contract are defined and transparent. It reduces dependencies on any one entity, and increases confidence in contract execution.

II. Integrating Blockchain with Cloud Security

A. Access Control

Cloud security is about efficient access control. It grants permissions to those users to only authorized data and re- sources. Decentralized Identity Systems (DID) use to increase identity management by linking the user's identity securely to a blockchain. With cryptographic techniques such as public private key pairs and digital signatures used, users get to main- tain full control over those identity data which reduces the risk of access by illegal tampering. Access Rights Management is mechanized by smart contracts that dynamically and transpar- ently enforce permissions without the need for intermediaries. Due to this Decentracized aproach, identity theft is prevented and data is immutable, additionally decreasing user onboarding time. It also cuts down on an administrative burden to manage credentials.

B. Data Integrity

Data integrity is confirmed in this cloud computing. It's all spread across multiple systems. Blockchain technology has strong solutions that use cryptographic hashing to protect data from tampering when data is being stored, or when it is trans- mitted. A hash function (e.g., SHA256) is used to process each data element, this resulting in a unique digital fingerprint that we record in blockchain. Tampering and keeping immutability requirements are met by each modification in data resulting in an overall different hash immediately. This is done to offer a verifiable, secure audit trail for the data, and build trust in the data's authenticity. This allows organizations to meet verifiable, accurate and unchanged data regulations (for example, GDPR, HIPAA). But it takes blockchain to improve cloud security and reliability.

C. Auditing and Compliance

Such organizations must ensure compliance and whether the Cloud services they choose enhance and enhance security or compromise it. Since the blockchain ledger is transparent and is immutable, it gives answers for the recording and monitoring all activities. A tamper proof, verifiable audit trail is created for each transaction or access event, secured via a timestamp and cryptographic signature. This trans- parency, allowing auditors to directly inspect the records in the blockchain by the nodes, removes the risk overhead of mid- dleman and compromised logs. Additionally, smart contract can be used to automatically perform real time compliance checks and maintain ongoing loyalty to regulatory standards (e.g. GDPR, SOC 2). It also increases the governance and accountability of cloud environments.[12]

D. Decentralized Storage Solutions

Blockchain technology is forced to distribute data across multiple nodes while removing reliance on central servers in decentralized storage systems. With this method security and resilience is increased because data is encrypted into fragmented shards and distributed out across the network. By doing this, malicious attackers have much more trouble compromising the whole dataset. Data redundancy, availability and decentralized control are settled through protocols like InterPlanetary File System (IPFS) and Filecoin. It offers safe storage while avoiding single node failure. In Blockchain based identity systems, data owners can encrypt files and control access perimeters.[7] Integration of blockchain with cloud environments can bring organizations with access con- trol, data integrity, compliance automation and decentralized storage solutions. This comprehensive approach makes cloud more secure, reduces the reliance on traditional providers, and enhances flexibility and control in an ever expanding digital world.[13]

III. Case Studies and Applications

A. Examples of Existing Solutions

In recent years, several organizations and campaigns have seen it fit to merge blockchain technology to fortify cloud computing security. Here are a few notable examples:

IBM Cloud and Hyperledger Fabric: It uses Hyperledger Fabric, its own private blockchain framework, to combine blockchain technology with its cloud services. This system allows organizations to create secure and transparent appli- cations while keeping control of their data. IBM Cloud's Block chain offerings are secure identity management with data integrity guarantees. This helps businesses to comply with regulatory requirements easier than before.

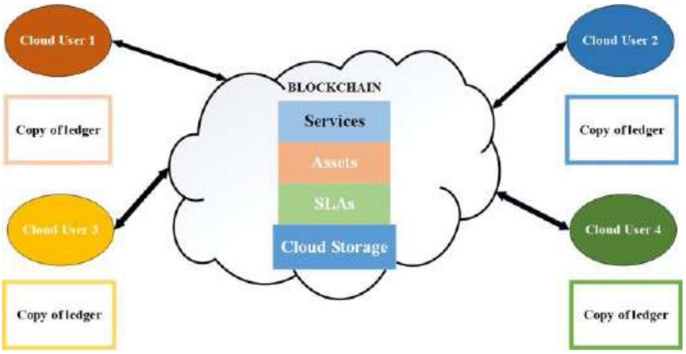

Fig. 3.

Storj: The distributed cloud storage service Storj has har- nessed blockchain technology in order to create a secure and distributed storage system. This is because it breaks files into smaller segments, then encrypts them, and finally distributes them on a global network of nodes which gives you better security and privacy capability. With this method clients still have control over their data and the movement of it and higher protection against possible threats and losses of data.

Civic: Created using blockchain technology, Civic is a de- centralized platform for identity verification. In civic, the users who own their identity and decide which one they want to share their access are able to reduce the risk of identity stealing as well as the illegal access. Especially for organizations who have to enforce a demanding identity verification procedure, this approach is intrinsic.

B. Success Stories

Numerous organizations have effectively incorporated blockchain technology for improved security, highlighting the possible advantages of this method:

Everledger: Diamonds and wine are two such industries, and Everledger is a blockchain based program that improves asset tracking security and transparency. With everledger you can stop fraud and prove the integrity of value assets with a tamper proof record of ownership and source. The supply chain is secured, but this approach also creates trust to stakeholders.

Guardtime: Guardtime is a cybersecurity firm that makes use blockchain technology to protect data integrity on be- half of government and corporate clients. Guardtime's KSI Blockchain technology enables real time verification of the integrity of data and enables organizations to detect unau- thorized changes and achieve regulatory compliance. Defence and financial service sectors have successfully adopted this solution by Guardtime. That is a testimony of the strength of blockchain in protecting sensitive information.

Microsoft Azure's Blockchain Workbench: The capability of Microsoft to do blockchain stuff now lives in the Azure cloud platform. This has made it easy to create and deploy blockchain applications. The Azure Blockchain Workbench provides tools to manage blockchain networks and to help perform secure identity verification, alongside data integrity. Organizations that use Azure can use these features to help them secure their clouds and simplify the development pro- cess.

C. Challenges and Limitations

Scalability Issues: Block chain technology implies scala- bility as a major challenge from a cloud environment. As transaction volumes in public blockchains increases, they can hit significant slowdowns. Specifically, this is largely caused by the fact that whatever consensus mechanism is involved in the verification of transactions leads to bottlenecks due to network activity. For example, this is approximately not enough for large scale applications — for example, we can process approximately 30 transactions per second on Ethereum (which may be enough for Ethereum applications, but not for large scale applications).However, this scalability bottleneck can prevent blockchain from being utilized in the cloud when clients demand is high.

The scalability challenges also limit blockchain working well in places where speed of transaction processing and high performance are of vital importance are cloud computing. To address modern issues being faced with these solutions like sharding, layer2 technologies (Lightning Network, Rollups) and more efficient consensus structures (Proof of Stake) etc. are being explored. Nevertheless, these approaches remain complicating due to implementation and widespread accep- tation. That makes it hard to take full advantage of what blockchain is capable of in cloud environments.

Interoperability: One of the biggest challenges in integrating blockchain technology with already existing cloud infrastruc- ture is interoperability. Different cloud services and platforms are used by many organizations, who each employ their own blockchain protocols and standards. There are obstacles to communication between systems and to the use of blockchain solutions in a multi cloud environment, due to this diversity. Seamless interoperability will be a requirement for organizations wanting to exchange data via multiple blockchain networks and will lead to the development of standardized pro- tocols that facilitate data exchange between various blockchain networks. Adding blockchain solutions into already existing cloud architectures is hindered by lack of widely accepted standards. It also makes systems more complex, and more prone to security risks as they try to talk to one another.

Energy Consumption: It is a well known fact that blockchain technology consumes a significant amount of energy, espe- cially when a network is run on Proof of Work (PoW) consensus methods. This energy consumption is high due to these systems need for large amounts of computing power to validate transactions. For instance, bitcoin mining uses a huge amount of electricity compared to some small countries during a year. The question that the previously mentioned concern asks is about the sustainability of such networks. However, energy efficiency is crucial in cloud environments, where the large energy needs of blockchain could negate organizations' objectives for reducing carbon footprints and operating sustainably. Blockchains like Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) offer more energy efficient solutions and transitioning systems over to these ones can be difficult in the worst case. [10]

Finally, the blockchain technology can contribute to sig- nificant improvement of cloud security and has solved chal- lenging issues such as scalability, interoperability, and energy consumption that are critical for its use and diffusion. To fully realize the benefits of integrating blockchain with cloud computing organizations must effectively manage these con- straints.

IV. FUTURE DIRECTIONS

A. Research Opportunities

The fields of blockchain and cloud computing with their progresses can create numerous promising avenues for future investigation, and can greatly improve their collaboration and efficiency:

Scalability Solutions: To address scalability this is being explored for the current blockchain systems by means of advanced scaling techniques such as sharding and layer 2 solutions. The tradeoff between scalability and security will give some important insights on the development of more efficient and robust systems.

Interoperability Frameworks: There are some very important research on developing standardized protocols for interoper- ability between blockchain networks and existing cloud infras- tructures. It also involves testing out crosschain transmission protocols that allow data and value to flow without any pillars between different platforms.

Energy-Efficient Consensus Mechanisms: It is necessary to investigate new consensus algorithms which lower the energy consumption while still ensuring security and level of decentralization. Furthermore, hybrid models consisting of various consensus mechanisms is perhaps a viable caching medium to block chain solutions for cloud environments.

Privacy-Enhancing Technologies: As privacy becomes an increasing concern, the use of privacy preserving techniques such as zero-knowledge proofs and secure multi-party com- putation can augment transaction secrecy while relying on blockchain's transparency.

Regulatory Compliance Solutions: There was an exploration of how blockchain applications may support regulatory com- pliance such that organizations may employ tools to automate and reduce compliance processes. This is helpful for compa- nies and helping them abide by standards.

B. Emerging Trends

Numerous emerging technologies and trends are expected to influence the incorporation of blockchain into cloud computing in the years ahead:

Artificial Intelligence (AI): Using of AI and blockchain in cloud platforms can enhance decision making, security and data analysis. Blockchain networks may benefit from the existence of AI for anomaly detection for the sake of security.

This means that blockchain can serve as secure and reliable data sources to the AI system.

Internet of Things (IoT): As more and more IoT devices grow, the need for secure data transfer and management also grows. A decentralized framework for secure, device authentication and data exchange through a Blockchain. The security in IoT environments in a cloud environment can be very much improved by IT.

Decentralized Finance (DeFi): As DeFi applications are coming to life – it implies that blockchain has the potential to revolutionize the financial services. On one hand, organi- zations will be spending a lot of time researching secure and efficient methods of managing financial transactions since they will be exploring the integration of DeFi solutions into cloud computing.

Quantum Computing: New challenges to blockchain secu- rity arise from the introduction of quantum computing. The protection of blockchain network against future computational threats will be a main focus of investigation of quantum resistant algorithms and regulations.

Edge Computing: As the computing grows, the computation and data storage near the source, and the block chain tech- nology can be improved. As organizations strive to minimize performance peaks and latency, a new wave of looking into how blockchain can improve security and data integrity at the edge will become energetic.

V. CONCLUSION

In the age of data breaches and cyber threats which are becoming more and more common, cloud security advanced solutions are more important than ever. This is because organizations are aligned to move operations to the cloud and need to have in place the robust security regulations that ensure crucial data is protected and clients remain assured of same. Integration of blockchain technology can help reduce many of these vulnerabilities by bringing in better identity management, data integrity and openness as a service to cloud computing. Decentralization and immutability of blockchain as inheritance characteristics can be strong foundation for secure cloud environments. Not only will these features help safeguard companies' data, but it will also enable them to increase operational efficiency in a way that increases compliance and auditing processes. What should be done further is to look ahead where further research and exploration on the use of blockchain technology on cloud security is needed. By overcoming such challenges as scalability and interoperability and taking advantage of current technologies, organizations will be able to fully leverage blockchain to build secure and resilient cloud infrastructures. A big initiative focused on driving moderate and ensuring the cloud security keeps up with the calls of a more confused digital world will be collaborations of various research individuals, business pioneers, and officials. Blockchain technology adoption promises a future of secure and efficient and resilient cloud computing.

References

Smith, J., Doe, R., & Brown, T. (2022). The Impact of Data Breaches on Cloud Security. Cybersecurity Review, 8(1), 33-50.

Johnson, A. (2023). Cloud Security: Challenges and Solutions. Journal of Cloud Computing, 10(2), 45-60.

Williams, H., & Chen, L. (2021). Evolving Security Protocols for Cloud Environments. Cloud Security Journal, 9(3), 87-98.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

Liu, Y., & Wu, Z. (2021). Integrating Blockchain Technology into Cloud Computing. International Journal of Computer Science, 15(4), 102-118.

Zhao, X., Li, Y., & Zhang, Q. (2020). Blockchain Technology for Cloud Security: A Review. Future Generation Computer Systems, 112, 268- 284.

Jawaher, A., Fadhil, S. R. M., & Zeebaree, S. (2024). Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges. Indonesian Journal of Computer Science, 13(2). https://doi.org/10.33022/ijcs.v13i2.3794

Meenakshi, K., Bharathi, B., John, S., Thangaraj, J., & Sivasubramanian, S. (2023). Cloud Security Analysis using Blockchain Technology. In Proceedings of the 2023 International Conference on Cloud Computing and Artificial Intelligence (pp. 56-67). IEEE. https://doi.org/10.1109/icecaa58104.2023.10212415

Choubey, A., Choubey, S., Jaiswal, D., & Jaiswal, M. (2024). Integrating Blockchain in Cloud Computing for Enhanced Data Management and Security. Proceedings of the 2024 International Conference on Information Technology and Operations Research (pp. 45-58). IEEE. https://doi.org/10.1109/icrito61523.2024.10522328

Tamboli, S., & Arage, C. S. (2023). Enhancement of Privacy Preservation and Security in Cloud Databases using Blockchain Technology. In Proceedings of the 2023 IEEE International Conference on Cloud Computing and Artificial Intelligence (pp. 123-134). IEEE. https://doi.org/10.1109/ieeeconf58110.2023.10520353

Divya, S., & Gini, R. (2023). Enhancing Data Security in Cloud Computing using Blockchain. In Proceedings of the 2023 International Conference on Cloud Engineering and Security (pp. 67-80). https://doi.org/10.59544/kjqt5979/ngcesi23p26

Cloud in Blockchain Technologies. (2024). Indian Scientific Journal of Research in Engineering and Management, 12(4). https://doi.org/10.55041/ijsrem34982

Manivannan, K., Bellam, K., Raja, J., & Shanthi, D. (2024). Blockchain Technology in Cloud Security. In Advances in Information Se- curity, Privacy, and Ethics Book Series (pp. 75-88). IGI Global. https://doi.org/10.4018/979-8-3693-2081-5.ch003