

A Study on Blockchain's Role in Cloud Security Enhancement

Bhavya Gupta¹, Shubham Yadav², Aditya Mukhija³ and Rajeev Kumar⁴

¹⁻⁴Netaji Subhas University of Technology, Delhi, India

Email: bhavyagupta791@gmail.com, shubham.yadav.inbox@gmail.com, Adityamukhija6830@gmail.com, Rajeev.kumar@nsut.ac.in

Abstract—Cloud services have become a cornerstone of modern computing due to their widespread accessibility. However, this accessibility also exposes them to various security threats, with data manipulation being a significant risk to data integrity. In cloud computing, which has gained rapid popularity, malicious actors can exploit vulnerabilities for their benefit. As more organizations and individuals rely on cloud services for data storage, ensuring data security and privacy has become increasingly critical. Data stored in the cloud is often encrypted to protect sensitive information, requiring users to obtain an access key, typically spread by a third party. Unfortunately, the integrity of this system can be compromised if the third party proves unreliable or dishonest, posing a significant threat to security. Common challenges, such as data piracy and hacking attempts, highlight the urgency to safeguard sensitive data against intentional and unintentional threats. Addressing these concerns is paramount for maintaining trust in cloud services. Integrating blockchain technology using cloud computing offers a promising solution to improve data safety and privacy. Blockchain's decentralized architecture stores data across a network of nodes, significantly reducing the chances of unauthorized access or tampering. This approach not only strengthens data protection but also enhances transparency and mitigates the risks associated with data breaches.

Index Terms—Cloud storage, access control, cloud computing, blockchain, data privacy, data security.

I. INTRODUCTION

Lately, with the quick growth of cloud computing and big data technology, increasingly businesses and individuals have chosen to outsource their data to the cloud service. Most of the data kept in the cloud is extremely delicate, for example, particular medical accounts and inside data of a firm. To safeguard the safety of data and the confidentiality of workers, data is typically kept on the cloud server in the form of ciphertext. To attain access control of the data, encryption technology can be viewed as a safety guarantee. However, how to attain access control for encrypted data is a huge task [1]. Data safety is often characterized by data security fears. The part of cloud computing is no dissimilar as it is disposed to numerous fears. The main purpose for this is that cloud computing combines numerous dissimilar technologies in its operation [2]. With the help of blockchain technology in cloud computing offers advantages such as improved transparency, traceability, and accountability.

It allows users to track the history of transactions and certify that all parties tangled in the process are held responsible for their actions. Instead of depending on a central authority to accomplish safe data, a scattered network of nodes can work collectively to authenticate and confirm transactions, making it tougher for bad actors to change the system [3].

This proposed System aims to provide a more comfortable and safer way to access the data on the cloud than the traditional System. Provide high end of security to the stored data. This allows the user to save data on the cloud without any worries. This will increase the trust of users to put highly confidential data on the cloud, thus making the cloud technology safer and cheaper for all types of users. The system will remove the dependency of access of third-party companies to maintain the data on the cloud [4]. Cloud security covers a wide area variety of security limitations from end-user and cloud service provider perspectives, where they will specifically be worried about the safety strategy, how data is stored, how the data is accessed, and who is accessing that data [5]. Cloud security is important because it is probably the biggest reason why cloud service providers fear the cloud [6], [7]. An organization named Cloud Security Alliance (CSA) has formulated the strategies and framework for employing safety within a cloud-executing location [8].

This paper is divided into 8 sections. Starting with the Introduction, followed by Methodology, the third section is Blockchain, the fourth section is Bitcoin, and the fifth section is Blockchain security and challenges faced by blockchain. The sixth section is an application, seventh section is tools. The eighth section is Discussions and Conclusion and the last section is Future Enhancement.

II. METHODOLOGY

When discussing the security domains of applications, it is essential to understand the service models, deployment types, and objectives within the security domain. Security measures vary depending on the level of interaction and responsibilities within the cloud. At the client level, security involves the use of Open APIs, SSH protocols, and input validation mechanisms to ensure safe communication and data handling. In monitoring domains, logging activities, alert systems, and reporting are crucial for detecting and responding to potential threats. For transmission medium security, protocols like VPN, SSL, and IPSEC are implemented to safeguard data during transfer.

Data and storage security form one of the most critical areas in the security domain. This includes data encryption, effective key management, disaster recovery strategies, garbage management, digital signatures, and data masking to ensure the confidentiality and integrity of information. Identity and access management (IAM) focuses on features like single sign-on (SSO), access control lists (ACL), authorization processes, and directory services for secure user authentication and access control. Virtual image security addresses issues like image encryption and registry security to prevent unauthorized access to virtual machine images. Additionally, network security plays a vital role in safeguarding the infrastructure, often relying on firewalls to inspect and control traffic under various conditions.

A. Cloud Security Framework Architectures

IaaS Cloud Security Framework

The Infrastructure as a Service (IaaS) model provides the foundational components of storage and networking for cloud architecture. This model primarily depends on APIs for managing and interacting with cloud resources. Security responsibilities for the infrastructure lie with the Cloud Service Provider, which focuses on enhancing the flexibility and scalability of cloud computing. A Network Packet Broker is utilized to provide visibility and transparency into security issues within cloud computing networks, allowing for better threat detection and mitigation.

SaaS Cloud Security Framework

Software as a Service (SaaS) is a prototype where software and data are centrally presented and accessed through web browsers. Cloud Access Security Brokers (CASBs) hold an essential role in identifying and addressing safety challenges in SaaS environments. CASBs provide robust access control mechanisms and often integrate encryption capabilities to protect sensitive data and ensure secure interactions within the SaaS model.

PaaS Cloud Security Framework

The Platform as a Service (PaaS) prototype allows users to deploy web applications without the need to manage the underlying hardware, software, or hosting infrastructure. Cloud Service Providers primarily secure the PaaS environment by managing resources and deploying advanced security measures. This reduces the complexity for users while ensuring the safety and availability of applications and data.

III. BLOCKCHAIN

When a new transaction occurs, all participants update their respective ledgers to ensure data integrity. With advancements in internet technology and cryptography, it has become possible for participants to verify the authenticity of transactions without relying on a vital authority. This effectively eliminates the risk of a single point of failure associated with dependence on third parties. An important advantage of blockchain is its capability to be implemented, connected, and scaled easily using open-source tools. The transaction records stored in a blockchain are publicly accessible, promoting transparency and reducing regulatory expenses. Blockchain can be considered a structured list that stores information in a distributed database format, making unauthorized manipulation of data extremely challenging. This is achieved as network participants collectively store and verify the blockchain, ensuring its integrity and resilience.

Every block within the blockchain consists of two key components: one is the header and the other is the body. The header comprises essential metadata, including the hash values of the current and earlier blocks, as well as a nonce used in the consensus process. The block data is contained in the body and can be competently retrieved using index-based methods. While blocks do not inherently store the hash of the subsequent block, they are linked in sequence, forming an immutable chain of records. This structure and decentralized validation process make blockchain a secure, transparent, and efficient method for managing transactions and data across a network.

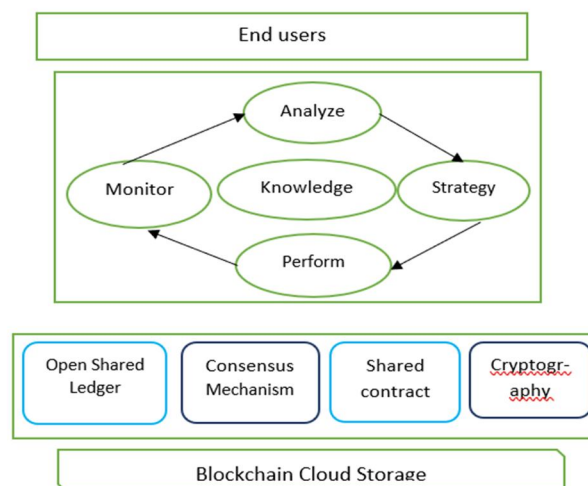


Figure 1. Secure Blockchain-based Cloud Framework

IV. BITCOIN

Bitcoin transactions are shared across the network, allowing all participants to verify them, ensuring both transparency and a cap on the total supply of the cryptocurrency. All network participants, or peers, maintain identical copies of the blockchain, and transaction data is stored within blocks, similar to a distributed storage system. While electronic transactions, including those involving Bitcoin, face several security threats, Bitcoin's underlying technology is designed to address and mitigate many of these risks. For instance, if someone attempts to falsify a transaction by redirecting funds from one account to another, this can be prevented through cryptographic verification using the sender's private key. Additionally, if two parties try to spend the same Bitcoin simultaneously, the network resolves the conflict by rejecting the chain that fails to reach a consensus, ensuring the integrity of the transaction history.

As Bitcoin gains attention, developers have begun leveraging blockchain technology to build new platforms using it as an infrastructure. Few platforms integrate the Bitcoin network for purposes such as notarization, crowdfunding, dispute resolution, and spam prevention. Cryptocurrencies depend on digital wallets to enable transactions and manage cryptographic key pairs, enabling users to send and receive funds. A Bitcoin wallet primarily stores the private key, which is essential for accessing and redeeming Bitcoins, as well as generating public addresses. Technologically, Bitcoins are not physically kept in the wallet but occur on the blockchain. Access is granted only to those possessing the correct private key, which is also used to digitally sign transactions, ensuring authenticity and security [13].

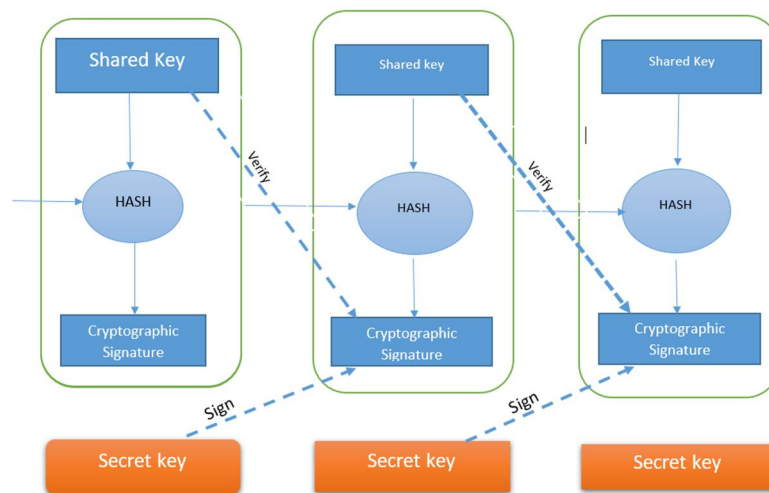


Figure 2. The structure of transactions in a Bitcoin blockchain

V. BLOCKCHAIN SECURITY AND CHALLENGES FACED BY BLOCKCHAIN

Blockchain technology, initially introduced alongside Bitcoin, is best known for supporting the security and integrity of transaction data. Bitcoin remains the most prominent application of blockchain, attracting an ever-growing user base. One of the important strengths of blockchain technology is its capability to function without the necessity for oversight by any centralized organization or government, making it decentralized and transparent. Data integrity is a critical feature of blockchain, which is why the technology is being explored for various applications beyond Bitcoin. However, despite its promise, blockchain faces several challenges that must be addressed for broader adoption. One of the significant hurdles is integrating blockchain technology with existing frameworks. Transitioning from a centralized system to a decentralized model can be costly and complex. Additionally, blockchain systems, including Bitcoin, are not immune to security risks, with issues related to market volatility and potential vulnerabilities impacting Bitcoin's security framework. These security concerns have, at times, influenced the market value of Bitcoin.

A Bitcoin contract is a mechanism for utilizing Bitcoin within existing financial and authentication services. One common approach involves the use of multi-sig (multiple signatures) scripts to enhance security. While these scripts can address a variety of challenges, their complexity also increases the risk of improper configuration, which can lead to failed transactions. For instance, if a Bitcoin transaction uses a locking script that cannot be unlocked due to incorrect configuration, it becomes unusable, and the transaction is discarded. Some studies have proposed models for verifying the accuracy of these Bitcoin contract scripts to mitigate such issues. The Bitcoin wallet, which stores critical information like private keys for unlocking scripts, is a crucial component in Bitcoin transactions. If this wallet information is lost, the associated Bitcoins cannot be accessed, leading to a permanent loss of funds. As a result, Bitcoin wallets have become a frequent target for hackers. To enhance security, some Bitcoin wallet services are incorporating biometric data or two-factor authentication methods, providing an additional layer of protection. While these measures improve security compared to traditional cold storage, challenges remain, such as the loss of cold storage or the difficulty in using hardware wallets due to user interface limitations. [20].

VI. APPLICATION

A. Authentication & Login

The application needs users to authenticate by registering with their email and password. Upon successful registration, users can log in using their credentials. If a user disremembers their password, a safe password reset process is provided, which confirms the user's email. The reset link is sent exclusively to the registered email.

B. Home Page & Uploading Document

After a successful login, the user is directed to the homepage where they can upload files to the cloud by clicking on an "Upload File" button. There is also a search bar and a view button, enabling users to access documents from others by providing the relevant file code. Before uploading, an alert prompts the user to confirm the

operation, followed by a Metamask transaction to confirm the upload. Metamask is essential for interacting with the blockchain. After the completion of the transaction, the file is uploaded, and the file creation log is kept on the blockchain.

C. Sharing Document

To view or download a file, users click on the "View" icon, which also requires confirmation via a Metamask transaction. If the transaction is approved, the log is recorded on the blockchain. If the user rejects the transaction, a notification prompts that the operation cannot be completed, and the log will not be added to the blockchain.

D. Granting/Rejecting Permission

When a second user requests access to a file using a valid code, the request is sent to the file owner. The owner can approve or reject the request. If permission is granted, the file becomes accessible to the requester; in case of rejection, access is denied. In both cases, a Metamask transaction confirms the action, and the log is recorded on the blockchain.

E. Log Details

The user can access all file-related logs by clicking the "Logs" tab. These logs are fetched from the blockchain and include details such as the file name, performed actions, requester, access status, and timestamp. Filters are available to help users easily access relevant logs.

VII. TOOLS

- Microsoft Visual Studio: For building applications, an integrated development environment (IDE) is used for various platforms, including websites, mobile apps, and web services. It supports a range of coding languages and offers tools for debugging, code refactoring, and GUI design.
- Android Studio: The authorized IDE for Android Progress, supports native app development for Android devices. It provides various tools for efficient coding and application building.

VIII. DISCUSSIONS AND CONCLUSION

Blockchain has eliminated the necessity for an essential authority by enabling peer-to-peer transactions, where participants store and verify transaction data. With the help of security procedures like Proof of Work and Proof of Stake, blockchain ensures secure operations. This paper proposes the combination of blockchain by cloud computing to improve safety. Experimental results show the effectiveness of using Java in Eclipse to integrate cloud and blockchain technologies. The application uses RSA encryption to secure data kept in the cloud, ensuring secrecy and integrity. While blockchain technology is widely studied for its utility, this paper emphasizes the importance of security in blockchain applications.

The proposed system has practical applications across industries like big data, institutes, and web applications. It offers secure document sharing and transaction management via blockchain. The system ensures that sensitive data, such as company ERP data, is safely stored and accessed through a private cloud. Additionally, smartphone and laptop security features, such as biometrics and password validation, further strengthen the system's security. By integrating blockchain into cloud-based storage, the proposed system provides a robust and cost-effective solution for secure document management.

FUTURE ENHANCEMENT

The current system is designed to operate on a specific combination of operating systems; however, it can be expanded to support multiple OS configurations. At present, the system handles a single data type, but it can be enhanced to accommodate various types of data. Additionally, there is potential to make the system more cost-effective, and tailored to the exact needs of the user. Upcoming research should emphasize key areas such as risk management, minimizing efforts in handling security threats, and the development of effective risk assessment strategies.

REFERENCES

- [1] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on Blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019. doi:10.1109/access.2019.2929205

- [2] V. Agarwal, A. K. Kaushal, and L. Chouhan, "A survey on cloud computing security issues and cryptographic techniques," in *Social Networking and Computational Intelligence*. Singapore: Springer, 2020, pp. 119_134, doi: 10.1007/978-981-15-2071-6_10.
- [3] "Blockchain in Cloud Computing for Securing Document." *International Research Journal of Modernization in Engineering Technology and Science*, 14 May 2023, doi:10.56726/irjmets38879.
- [4] S. Jadhav, A. Bhawsar, and D. Katoriya, "ENHANCED CLOUD SECURITY USING," vol. 8, no. 11, pp. 3314–3317, 2020.
- [5] Julija Golosova et.al. "The Advantages and Disadvantages of Blockchain Technology", IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.
- [6] Jin Ho Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges.", Seoul National University of Science and Technology, SoongSil University, Korea; Research Article, 2017.
- [7] S. Kumar, A. Singhal, and A. Dumka, "Analysis of Cloud Security Framework Using Blockchain Technology," *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3383151.
- [8] Kaskaloglu, K. Near zero Bitcoin transaction fees cannot last forever. In *Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014)*, The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic, 24–26 June 2014.
- [9] Ziegeldorf, J.H.; Matzutt, R.; Henze, M.; Grossmann, F.; Wehrle, K. Secure and anonymous decentralized Bitcoin mixing. *Future Gener. Comput. Syst.* 2016.
- [10] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry (Basel)*, vol. 9, no. 8, pp. 1–13, 2017, doi: 10.3390/sym9080164.
- [11] D. Yermack, "Is Bitcoin a real currency? An economic appraisal," in *Handbook of Digital Currency*. New York, NY, USA: Academic, 2015, pp. 31_43.
- [12] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1_34, 2019.
- [13] Bozic, N.; Guy, P.; Stefano, S. A tutorial on blockchain and applications to secure network control-planes. *SCNS IEEE* 2016.
- [14] Bradbury, D. The problem with Bitcoin. *Comput. Fraud Secur.* 2013, 11, 5–8.
- [15] Kaskaloglu, K. Near zero Bitcoin transaction fees cannot last forever. In *Proceedings of the International Conference on Digital Security and Forensics (DigitalSec2014)*, The Society of Digital Information and Wireless Communication, Ostrava, Czech Republic, 24–26 June 2014.
- [16] Paul, G.; Sarkar, P.; Mukherjee, S. Towards a more democratic mining in bitcoins. In *Proceedings of the International Conference on Information Systems Security*, Hyderabad, India, 16–20 December 2014; Springer International Publishing: Cham, Switzerland, 2014.
- [17] Bamert, T.; Decker, C.; Wattenhofer, R.; Welten, S. BlueWallet: The Secure BitcoinWallet. In *Security and Trust Management*; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 65–80.
- [18] Anceaume, E.; Lajoie-Mazenc, T.; Ludinard, R.; Sericola, B. Safety analysis of Bitcoin improvement proposals. In *Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, 31 October–2 November 2016.
- [19] Upadhyaya, R.; Jain, A. Cyber ethics and cybercrime: A deep dwelled study into legality, ransomware, underground web and bitcoin wallet. In *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 29–30 April 2016.
- [20] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", Elsevier, 2018
- [21] Ilya Sukhodolskiy, Sergey Zapechnikov, "A Blockchain-Based Access Control System for Cloud Storage," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
- [22] Google Cloud Platform Documentation: <https://cloud.google.com/docs>.
- [23] G. Zyskind, O. Nathan, and A. Pantland. Decentralizing privacy: Using blockchain to protect personal data. In *IEEE Security and Privacy Workshops (SPW)*, 2015.
- [24] GSA, Cloud Computing Initiative Vision and Strategy Document (DRAFT), <http://info.apps.gov/sites/default/files/Cloud-Computing-Strategy-0.ppt>.
- [25] J. Benet, "IPFS_content addressed, versioned, P2P _le system," 2014, arXiv:1407.3561. [Online]. Available: <https://arxiv.org/abs/1407.3561>.
- [26] C. Gray. (2014). Storj Vs. Dropbox: Why Decentralized Storage is the Future. [Online]. Available: <https://bitcoinmagazine.com/articles/storj-vs-dropbox-decentralized-storage-future-1408177107>.