International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024
https://doi.org/10.55524/CSISTW.2024.12.1.30
Computing for Sustainable Innovation: Shaping Tomorrow's World (CSISTW-2024) on 16th-17th February, 2024
Organized by B.N. College of Engineering and Technology, Lucknow, India

Using Blockchain as a Tool for Cloud Data Security

Harshita Gupta[1] and Prabhat Verma[2]

[1] Research Scholar, Computer Science and Engineering, HBTU, Kanpur, India
[2]Professor, HBTU, Kanpur, India

Correspondence should be addressed to Harshita Gupta: harshitagupta1311@gmail.com

ABSTRACT- Blockchain technology has emerged as a potentially effective remedy for cloud computing security issues. Blockchain presents a revolutionary method for boosting data protection, access control, and transparency in cloud environments by introducing decentralized and immutable methods. The integration of blockchain into cloud security is explored in this study, emphasizing major benefits such the maintenance of data integrity through cryptographically linked transactions, effective identity management, and secure automation utilizing smart contracts. Examined is the possibility of authorized parties working together and sharing data under specified circumstances. However, difficulties with scaling, difficult integration, and energy usage are highlighted. Blockchain technology holds the potential to greatly enhance data security, attack resistance, and transparency in multi-cloud scenarios with careful planning and thought.

KEYWORDS-Blockchain, Cloud Computing, Data, Integrity, Data Security.

I. INTRODUCTION

Cloud computing provides a convenient way to store and utilize data online, but it also introduces security worries. People want their information shielded from hackers and unauthorized access. This necessitates strong passwords, regulating access permissions, and maintaining data backups. Adhering to rules and regulations ensures data privacy in cloud services. When selecting a cloud provider, scrutinizing their security practices is essential. Preparing for potential issues like breaches or data loss is crucial.

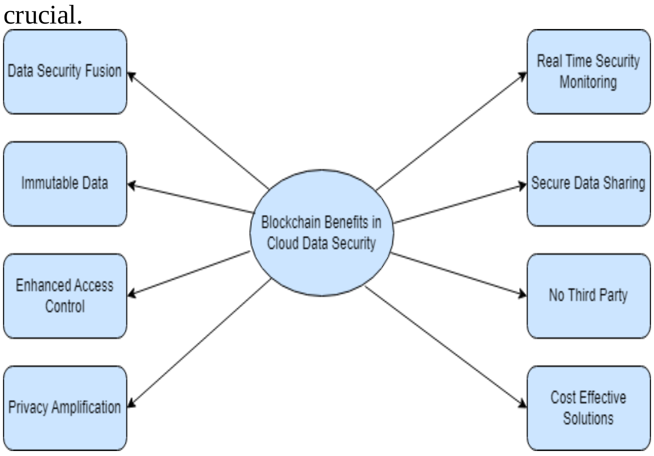

Figure 1: Benefits of Blockchain in Cloud Data Security

Blockchain technology has garnered considerable attention in recent years, primarily owing to its distinctive features like decentralization, immutability, and transparency. These characteristics position it as a viable alternative for establishing a trustworthy platform. Initially introduced through Bitcoin in Nakamoto's 2008 whitepaper for peer-to peer financial transactions, blockchain has now emerged as a focal point of interest within both the research and industrial communities. Notably, smart contracts play a pivotal role in driving the widespread adoption of blockchain technology, as they bring forth automated control, as articulated by Dorri et al. [1] in 2017. Smart contracts, described in an executable language, enable the execution of secure transactions without the need for intermediary third parties. The disruptive potential of blockchain and smart contracts extends across numerous domains within engineering and computer science. In this context, blockchain technology plays a pivotal role in boosting cloud data security. It ensures data remains unaltered once recorded, preventing unauthorized changes. Smart contracts control access to sensitive data, allowing only authorized users and minimizing breach risks. Privacy concerns are addressed by blockchain's private networks, confining access to approved users. The technology's transparency aids in tracking data for compliance purposes. Ownership of data is empowered through blockchain, even in shared cloud environments. Decentralization enhances data availability and reliability. Blockchain also enables real-time security monitoring for swift issue identification and response. Secure data sharing is facilitated through encryption, particularly for sensitive information exchange. However, integrating blockchain in cloud setups demands careful consideration of specific scenarios and potential obstacles. The fusion of blockchain and cloud computing offers a potent approach to enhancing data security, transparency, and overall cloud protection. In fig 1 we can see several benefits of using blockchain in cloud data security.

The following parts of the paper are arranged in the following manner: Section 2 offers a summary of research conducted in the field in recent years. Section 3 delves into an analysis of research gaps identified within the various research papers examined during the literature review. Recommendations for potential avenues of further investigation are deliberated upon in Section 4, and the paper concludes by presenting findings in Section 5.

II. LITERATURE REVIEW

The paper under consideration aims to evaluate the significance of integrating blockchain technology with cloud computing, focusing on insights from existing review papers. The main objective of this paper is to identify and address the limitations that previous articles may have had in their discussions on this topic.

In reference to the first source, denoted as [2], the author introduces the concept of creating a secure cloud ecosystem. This involves ensuring data security and privacy from the point of user authentication all the way to storing data in the cloud. To achieve this, the author employs encryption and decryption techniques such as RSA and AES. Additionally, the author uses hashing functions like SHA512 and the HMAC algorithm for key management. The highlight of this work is the development of an encryption system, termed a hybrid encryption system (HCS),that amalgamates the advantages of both symmetric and asymmetric encryption techniques.

The second source, referenced as [3], discusses the application of blockchain-based intrusion detection systems in cloud computing environments. This approach involves using containerization and virtualization techniques to collaboratively detect abnormal activities and threats, both from external sources (outsiders) and within the cloud environment itself (insiders). The main objective is to swiftly identify potential malware attacks, which is crucial for rapidly addressing these threats to mitigate disruptions and ensure smooth cloud operations. The article provides an overview of cloud infrastructure and categorizes modern security events based on their frequency across different types of cloud deployments.

Moving on to [4], the author presents a comprehensive overview of security measures in the context of cloud computing. This includes aspects like processing data access, encoding searches, and computing data encodings. One notable point discussed is the utilization of a mix of public and private clouds for managing sensitive and nonsensitive data. To guarantee user privacy, the author suggests the development of a more secure public key encryption system. The use of homomorphic encryption, a technique that allows computations on encrypted data without decryption, is emphasized in this work.

The research by Patel and Patel, indicated as [5], delves into the potential of blockchain technology in addressing challenges related to data integrity in cloud computing. They highlight blockchain's attributes such as persistence, distribution, transparency, and cost-effectiveness as qualities that can enhance security in cloud data storage.

In the context of [6], the author proposes a method for ensuring data integrity using a MAC-based (Message Authentication Code) technique. This approach is notable for not relying on third-party entities. The introduced method is designed to withstand common attacks like Man-in-the- Middle and replay attacks. However, it's important to note that unnecessary data removal is not addressed in this approach.

The research conducted by Gai et al., identified as [7], centers on the incorporation of blockchain technology into established cloud infrastructure. The authors investigate the Blockchain-as-a-Service (BaaS) model, a cloud-centric approach to providing blockchain services. Emphasizing security, the study assesses schemes related to searchable encryption and access control. The study evaluates the effectiveness of cloud datacenters with integrated blockchain support, considering both software and hardware considerations.

The study detailed in [8] introduces ChainFS, a middleware solution that employs blockchain technology to enhance the security of cloud storage. This system is constructed with Fuse-based clients, Ethereum, and Amazon S3 cloud storage. The performance of ChainFS is analyzed, showcasing its efficiency with minimal overhead. The system architecture involves a client-server model with interactions facilitated through an intermediary web server process. The SHA256 algorithm is used for hashing purposes in this context.

Murthy and Shri, referenced as [9], propose a mechanism to address issues related to cloud computing using blockchain. The primary focus is on achieving security through efficient blockchain utilization and removal. The authors emphasize that effectiveness studies are often required in addition to security considerations due to the decentralized nature of blockchain systems.

The work of Xuet al. [10] discusses challenges and vulnerabilities in cloud data security. The authors propose a novel architecture that employs blockchain technology to enhance cloud data security. The approach involves addressing risks in cloud environments and then concentrating on how blockchain solutions can bolster the security of cloud data.

The study by Prianga et al. [11] delves into a Proof of Work (PoW)-based blockchain approach. The goal is to resolve privacy concerns within cloud computing environments. The study provides insights into privacy issues in cloud computing and introduces a blockchain architecture that leverages PoW to tackle challenges related to Function-as-a- Service (FaaS) scenarios.

In reference [12], the author presented a privacy preservation strategy centered on Identity-Based Encryption (IDE). Their research is notable for presenting a comprehensive approach to preserving privacy, encompassing various privacy concepts and proposing a mechanism for safeguarding it. While the scheme proposed in their work offers numerous advantages, it also exhibits certain limitations. One of the key requirements of the IDE scheme is the necessity for a secure communication channel for data transmission.

In reference [13], the author conducted a survey encompassing a range of research endeavors concerning the verification of data integrity within cloud systems. Various methods were investigated, encompassing Provable Data Possession (PDP), Proof of Retrievability (POR), hashing techniques, signature methodologies, and encryption protocols. The common objective across these strategies is to guarantee the maintenance of data integrity, upholding attributes such as precision, faithfulness, uniformity, and validity.

Table 1: Summary of Literature survey

Ref. Num ber	Identified Problem	Proposed Techniques
[2]	Cloud Ecosystem with data security and privacy.	SHA-512,bcrypt function and HMAC algorithm
[3]	Detect Malicious attacks, data privacy and data management	Cloud based intrusion detection system
[4]	Levels of security for sensitive and insensitive data.	Homomorphic encryption algorithm.
[5]	Data integrity problems	Blockchain
[6]	Replay attack and Man-in- the-Middle attack.	MAC based integrity checking.
[7]	Data Integrity and Data security	Blockchain enabled data provenance, blockchain based access controls.
[8]	Preventing against forking attacks	Ethereum S3FS
[9]	Data security	Blockchain
[10]	Data privacy and data integrity	VMI, IPFS
[11]	Data security	Consensus algo-rithm(PoW)
[12]	Privacy preservation	Identity Based Encryption
[13]	Comparison of various Data integrity schemes.	PDP,POR, Hashing, Signature methods, Encryption.

III. CLOUD SECURITY ISSUES

After a thorough examination of multiple research papers, we can deduce several security challenges that arise when utilizing cloud computing. We can see all of them in fig 2.

a) Data Breach:

When unauthorised people access sensitive data, a data breach occurs. Attackers may gain access to sensitive data through weak authentication methods, stolen passwords, or flaws in cloud platforms. This risk can be reduced by using robust authentication procedures, frequent security audits, and intrusion detection systems.

b) Data loss

Data loss is a risk that cloud storage providers face. Data loss or corruption due to human error, software defects, or hardware malfunctions is possible. Organizations should develop data backup and recovery plans, storing copies of crucial data in many locations, to combat this.

c) Insufficient Encryption:

Encryption is essential for safeguarding data during both transmission and storage. Useless key management or weak encryption methods might make encryption useless. Insufficient encryption of data exposes it to unauthorized access when stored or intercepted during transmission. To avoid unauthorized access to sensitive data, organizations should implement robust encryption algorithms and follow best practices for key management.

d) Insider threats:

These are malicious operations carried either by members of the cloud provider organization or the user organization. Access to sensitive data may be misused by privileged persons for their own gain or harmful purposes. Effective access controls, consistent monitoring of user activities, and adherence to the principle of least privilege can mitigate the risk of insider threats. Additionally, organizations should have clear security policies in place and inform staff members of the repercussions of misuse.

e) Insecure APIs:

APIs are the interfaces that enable communication and interaction between various software systems. Attackers may use poorly secured or inadequately built APIs to obtain unauthorised access to data or cloud resources. Data breaches or even control over the cloud environment may result from this. To stop such attacks, APIs must be properly secured using authentication, authorisation, and input validation.

f) Shared Responsibility:

Security is a shared responsibility between cloud service providers and customers. Users are in charge of protecting their apps, data, and access restrictions while providers are in charge of securing the underlying infrastructure. Users' errors or poor security procedures might create vulnerabilities that attackers can take advantage of. To reduce risks, organisations should apply security best practises and fully grasp the shared responsibility paradigm.

g) Lack of Control:

Cloud companies frequently provide only a limited amount of visibility into their security procedures and controls. Organizations may find it challenging to evaluate the security of their data and applications due to this lack of openness. Organizations may combat this by using third-party security solutions, conducting routine audits of their cloud environment, and requesting openness from their cloud providers.

h) Data residence and Compliance:

Depending on where the data center is located, data stored in the cloud may need to adhere to various data residence and privacy standards. When working with crossborder data transfers, this can be difficult. The right controls should be in place as organizations carefully choose cloud regions that comply with their compliance needs.

i) Risks Associated with Multi-Tenancy:

A cloud architecture known as multi-tenancy allows several users to share the same physical infrastructure. This could result in data leakage or unauthorized access amongst tenants if it is not securely segregated. To prevent cross-tenant security breaches, cloud providers should adopt robust isolation measures, such as virtualization.

j) Denial of Service (DoS) attacks:

Attackers may target cloud storage services in DoS assaults by saturating them with traffic. This can have an effect on availability and possibly cause data loss or corruption. Cloud service providers ought to put in place defences against DoS assaults, like rate limitation and traffic analysis.

k) Vendor lock-in:

When relying significantly on one cloud provider, it can be difficult to switch to a different provider or go back on- premises. To lessen the effects of vendor lock-in, organisations can think about developing multi-cloud strategies and employing standardised formats.

l) **Unsafe File Sharing**:

Cloud storage services offer collaboration capabilities that make it simple for users to share data. However, if these technologies are not set up properly, confidential information may unintentionally be made available to strangers. To guarantee that shared files are adequately protected, organisations should train users on secure sharing procedures and put controls in place.

m) Third-Party Risks:

To add more functionality, cloud storage services frequently rely on third-party plugins, APIs, or components. These components could pose threats to the cloud environment if they have security flaws. Organizations should thoroughly examine thirdparty components, make sure they are secure and up to date, and evaluate any potential effects they may have on the overall security posture.

n) Lack of Accountability:

The shared responsibility model used in cloud security can occasionally cause misunderstandings over who is in charge of safeguarding certain components of the environment. Roles and duties should be clearly defined within organizations as well as with cloud service providers in order to ensure that security measures are properly applied and monitored.

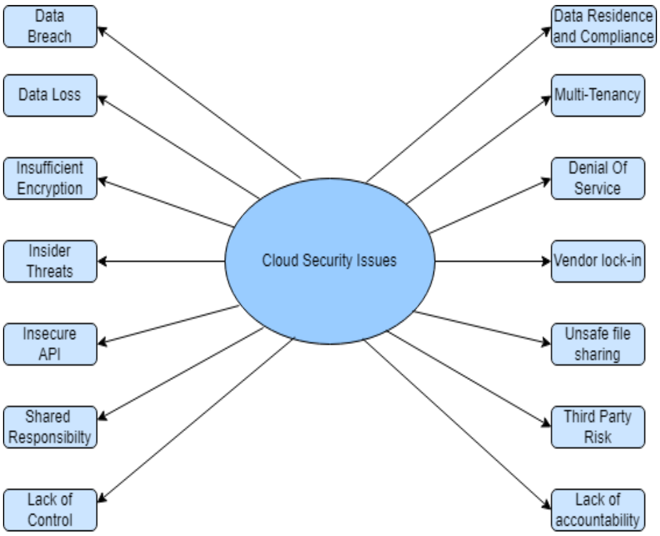

Figure 2: Cloud Security Issues

IV. INTEGRATION OF BLOCKCHAIN AND CLOUD TECHNOLOGY

Blockchain and cloud computing integration provides a strategic synergy that improves security, openness, and effectiveness across multiple applications. There are various ways to accomplish this connection. First, by storing user IDs on the blockchain and decreasing dependency on centralized systems, the decentralized identity management system of blockchain improves authentication. Furthermore, the integrity of data saved in the cloud is guaranteed by the immutability built into blockchain technology. This is especially helpful for important data or digital assets that must be securely recorded and checked over time. Real-time data collected by IoT devices is beneficial for supply chain management because it can be safely stored on the blockchain and then analyzed by cloud-based applications to reveal supply chain efficiency and integrity.

Blockchain-powered smart contracts streamline company procedures and user interactions with cloud services. These self-executing contracts can do away with middlemen and activate cloud resources in accordance with predetermined criteria. As data is spread across a network of nodes rather than centralized servers, integrating decentralized blockchain-based solutions with cloud storage improves security and privacy for data storage. The possibility of data breaches is decreased by this decentralized strategy.

Using smart contracts to automate permission management and give users control over data access, blockchain technology also enables safe data sharing and cooperation. Blockchain-based security event logs help security auditing by ensuring accountability and transparency. By administering and enforcing copyrights in cloud environments, blockchain furthers digital rights management by ensuring equitable pay for content providers.

In order to facilitate interoperability and safe data transmission across various cloud providers and on-premises systems, the combination of blockchain with cloud is particularly beneficial. As a result, hybrid cloud solutions are made possible that maximize flexibility and effectiveness. Additionally, the immutability of blockchain can act as a pillar for forensic investigations and incident response,

producing an irrefutable record of security occurrences and unauthorized access.

Assessing particular use cases, choosing suitable blockchain platforms, and building architectures that prioritize data privacy, security, and scalability are all necessary for effective integration. To fully realize the benefits of this integration and accomplish organizational goals in an increasingly connected digital landscape, collaboration between experts in blockchain and cloud technologies is essential.

Blockchain as a service

Blockchain as a Service (BaaS) in cloud computing is a solution offered by cloud service providers that streamlines the adoption of blockchain technology for organizations. BaaS facilitates the deployment and management of blockchain-based applications and smart contracts without the need to construct and maintain an entire blockchain network independently. Cloud providers offer pre-configured blockchain infrastructures, often utilizing popular frameworks like Ethereum or Hyperledger Fabric. They also furnish simplified development tools, APIs, and scalable resources, making it easier for developers to create blockchain applications. Security is paramount, with cloud providers offering encryption, identity management, and compliance features. Managed services ensure the reliability of blockchain networks, and integration with other cloud services simplifies connections with existing systems. BaaS is cost efficient as users pay based on resource usage. It suits a wide range of industries and use cases, such as supply chain management, finance, and healthcare. However, organizations should consider factors like vendor lock-in and regulatory compliance when choosing a BaaS provider. Overall, BaaS in cloud computing offers a straightforward path to leverage blockchain's benefits while minimizing operational complexities.

V. CONCLUSION

In conclusion, the combination of blockchain technology and cloud data security offers a crucial remedy to the weaknesses of centralized systems. Because of this integration, processes are expedited through the use of smart contracts, strong authentication, and secure communication. This combination creates a fortified digital landscape with increased security against breaches, enhanced transparency, and compliance across jurisdictions. Adopting this combination enables organizations to proactively combat changing cyber threats, protect sensitive data, and promote stakeholder trust, ultimately paving the way for a more secure and robust digital future.

CONFLICT OF INTERREST

The authors declare that they have no conflict of interest

REFERENCES

[1] Dorri, A., Steger, M., Kanhere, S.S., Jurdak, R., 2017. Blockchain: A distributed solution to automotive security and privacy. IEEE Commun. Mag. 55 (12), 119–125. http: //dx.doi.org/10.1109/MCOM.2017.1700879.

[2] Akshay Arora,Abhirup Khanna, Anmol Rastogi, Amit Agarwal (2017), "Cloud Security Ecosystem for Data Security and Privacy", IEEE.

[3] Weiwei Kong, Yang Lei, Jing Ma (2017),"Data Security and Privacy Information Challenges in Cloud Computing", International Conference on Intelligent Networking and Collaborative Systems, IEEE.

[4] YindongChen, LipingLi, ZiranChen (2017),“ An Approach to Verifying Data Integrity for Cloud Storage”, IEEE

[5] Stephen S Kirkman,(2018) A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains, IEEE International Conference on Cloud Engineering.

[6] QiwuZou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, (2018),IEEE 11th International Conference on Cloud Computing ,ChainFS: Blockchain-Secured Cloud Storage.

[7] Prianga, S., Sagana, R., Sharon, E.: Evolutionary survey on data security in cloud computing using blockchain. In: 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA). IEEE (2018)

[8] Xu, H., et al.: A survey: Cloud data security based on blockchain technology. In: 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC). IEEE (2019).

[9] Gai, K., et al.: Blockchain meets cloud computing: a survey. IEEE Commun. Surv. Tutor. 22(3), 2009–2030 (2020)

[10] Murthy, C.V.B., Shri, M.L.: A survey on integrating cloud computing with blockchain. In: 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). IEEE (2020).

[11] Patel, P., Patel, H.: Review of blockchain technology to address various security issues in cloud computing. In: Data science and intelligent applications, pp. 345–354. Springer, Berlin (2021)

[12] Hongbing Cheng, ChunmingRong, ManyunQian, and Weihong Wang (2018), “Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption”, IEEE.

[13] KamileNurSeviş, Ensar Şeker, “Survey on Data Integrity in Cloud”, (2016), IEEE 3rd International Conference on Cyber Security and Cloud Computing.