Cloud Security using Blockchain

Annika Yadav
annika270402@gmail.com

July 2022

Abstract

The growth of cloud computing technology is growing more advanced, yet it is always accompanied by security issues. Blockchain, as an emerging technology, possesses decentralization, distributed fault tolerance, and trustworthiness. Using blockchain technology to tackle cloud security issues is a very promising trend, and it is presently employed to safeguard cloud data security. Blockchain has emerged as a key technology to provide security especially in aspects of integrity, authenticity and confidentiality. Blockchain overcomes the security issues in cloud computing. This survey aims at analyzing and comparing various issues in the cloud environment and security issues using blockchain.

Keywords— Blockchain technology; Cloud computing; Cloud data security

1 Introduction

Cloud data security differs from traditional data security due to its unique storage architecture. Cloud computing often use distributed storage. Data ownership and control are distinct. Although users have ownership, cloud administrators have control. In addition to external harmful attackers, internal hostile cloud administrator threats and malicious cloud tenant threats have been added to the attacker's source. Current cloud data protection focuses on data storage, transit, and access authentication, and is usually accomplished via cryptography. Blockchain is a data structure comprised of chronologically ordered data chunks in a linked list format. It is cryptographically guaranteed to be unforgeable and untamperable. It is basically a distributed decentralised ledger capable of storing simple, hierarchical, and verifiable data securely. Furthermore, because the Blockchain has an openness quality, it can give data transparency when used to an area needing data disclosure. Because of these advantages, it may be used in a variety of settings, including the financial industry and the Internet of Things (IoT) environment, and its applications are projected to grow. Because of its efficiency and availability, cloud computing has been used in numerous IT applications. In addition, cloud security and privacy problems have been addressed in terms of critical security factors.

2 Related works

The researchers Xu et al.[35] examined the security risks associated with the cloud, then briefly introduced blockchain technology and summarised the categorization of the present blockchain technology to address existing issues with cloud data security. To preserve the cloud data, a novel cloud forensic storage architectural model based on blockchain technology is presented.The researchers Gai et al.[16] addressed a few technical dimensions for reengineering of cloud computing by using blockchain technology. Three technical dimensions are involved in the work, namely, service, security, and performance and further discussed about BaaS service model.The researchers Gupta et al.[18] firstly reviewed the various existing blockchain implementations for Cloud security and then discussed the general structure of Blockchain. Further, they analyzed the characteristics of Blockchain and Cloud Computing security requirements.The researchers Yadav et al.[36] developed an UI for the hospital which provided the patients with the flexibility of not carrying reports every time, they visit the hospital. Using the cloud for storage purposes increased the efficiency and capacity of storage and uploading reports as a softcopy lowered the paperwork of maintaining hard copies of each report.

The researchers Esposito et al.[15] described how the electronic health records are favorite target for cyber criminals and hence proposed a framework using blockchain technology and further discussed the benefits and disadvantages of using blockchain to address security and privacy concerns in an increasingly cloud-based environment.The researchers Rehman et al.[26] proposed a secured service providing mechanism for IoTs devices. In that proposed system, they also considered computing technologies such as cloud computing and edge transparent computing. To protect the IoTs devices from the malicious edge servers, they introduced blockchain technology and the validity of edge servers is maintained by the use of smart contract.The researchers Benil et al.[10] proposed an EC-ACS public verification and auditing scheme in the MCS using authorized blockchain technology where, the secure certificateless public verification scheme is designed using ECC for the key generation to encrypt and the signature on the data to verify the aggregate signature.The researchers Sharma et al.[31] proposed a novel constant restorative record sharing and security plan engaged by disseminated figuring, information grouping and Blockchain. The accentuation is on arranging a trustworthy access control framework subject to a single shrewd contract to administer customer access for ensuring powerful and secure medicinal information sharing.

The researchers Pavithra et al.[25] used Blockchain to overcome the security issues in cloud computing. They analyzed and compared various issues in the cloud environment and security issues using blockchain. The MD5 or SHA algorithm is used to check for the modifications in the data being stored in the cloud storage.The researchers Kollu et al.[20] explored the use of cloud computing protected by blockchain technology and provided a framework using ethereum blockchain to generate hash on data and smart contracts.The researchers Mayuranathan et al.[22] wanted to provide a security solution against

DoS and DDoS attacks in distributed and parallel (cloud) applications and to provide blockchain based security as a promising solution to Online (OTB) applications.The researchers Li et al.[21] developed a blockchain-based behavior audit framework that used blockchain to store files' metadata information and users' behavior information. The framework implemented operations such as auditing the integrity of files and auditing users' behaviors.

The researchers Xie et al.[34] firstly provided an overview on cloud exchange. Then they briefly discussed blockchain technology and the issues on using block chain for cloud exchange in aspects of security, privacy, reputation systems and transaction management.The researchers Deep et al.[14] explained the security flaw's existing in the cloud environment and has proved how insiders, as well as outsiders, can bypass the authentication system in cloud databases and proposed Blockchain authentication mechanism for counterfeiting insiders as well as outsider attacks.The researchers Yang et al.[37] designed an access control framework AuthPrivacyChain with privacy protection in cloud environment to overcome illegal access to resources by attackers in cloud and further implement the framework model based on the EOS blockchain.The researchers Siddiqui et al.[32] proposed the idea that since Blockchain technology ensured the anonymity. The blockchain was combined with the cloud computing to provide excellent stronger security to data and provided step by step solution to the threat to the information system by using blockchain technology.

The researchers Shah et al.[30] proposed system that enhanced the security of data by encrypting and distributing the data across multiple peers in the system. The system Implemented by them used the AES 256 bit encryption algorithm to encrypt the data ensuring the confidentiality of the user's data. Encrypted data is then distributed and stored across peers in the network using the IPFS protocol.The researchers Darwish et al.[13] proposed the framework which was built as a virtual cloud similar to the real cloud service infrastructure. It aimed to integrate the proposed framework on the virtualization machine located in the IaaS service model and to deploy the layer with the same environment and attributes container of the actual platform.The researchers Ashik et al.[8] analyzed a blockchain based fog-cloud architecture which could be used in a smart home. For the test case, they assumed an IoT device which sensed temperature and provided its output to the fog node for further processing.The proposed architecture gave rise to a different fog architecture which ensured better security, user authentication, and protection against known threats.The researchers Siva Kumar et al.[33] proposed a real-time service-centric feature sensitivity analysis-based blockchain algorithm which had been implemented and evaluated for its performance. Further, it performed RSFSA analysis to generate the sensitivity class of features which was performed by computing the sensitivity weight for various features, and based on the measure, the features were classified under different classes.

Table 1: **Literature Survey**

Author, year	**Key contribution**	**Portability**	**New architecture**	**Security of privacy**	**Lack of standards**	**Reliability**	**Governance**	**Metering**	**Denial of service**
Xu et al., 2019	Traceability of cloud data is realized and the integrity of cloud data is verified	No	Yes	Yes	No	No	No	No	No
Pavithra et al.,2019	Analyzed and compared various issues in the cloud environment and security issues using blockchain	No	No	No	Yes	No	No	No	No
Xie et al., 2020	Blockchain offers a potential decentralization solution to the challenges of current CloudEX platforms	Yes	No	Yes	No	No	No	No	No
Esposito et al.,2018	A conceptual blockchain-based EHR ecosystem is developed for ensuring privacy of the healthcare data	No	Yes*	Yes	No	Yes	Yes	Yes	No
Gai et al., 2020	Facilitates secure data sharing over cloud using blockchain techniques	Yes	No	Yes*	No	No	No	No	No
Deep et el., 2019	Provides a novel secure authentication mechanism by using Blockchain technology for cloud databases	No	Yes	Yes	No	No	No	No	Yes

Yang et al., 2020	Implement AuthPrivacyChain based on enterprise operation system (EOS)	No	Yes*	Yes*	No	No	No	Yes	No
Kollu et al., 2021	Examines the use of blockchain technologies to secure cloud computing	Yes	No	Yes*	No	No	No	Yes	No
Rehman et al.,2019	Proposed a secure service providing mechanism for IoTs using blockchain	Yes	Yes	Yes	No	Yes	No	No	No
Benil et al., 2020	Guarantees the integrity, traceability and secure storage of medical records in the cloud environment	Yes	Yes	Yes	No	No	Yes	No	Yes
Gupta et al., 2019	Information security concerns are resolved using distributed ledger of blockchain	No	No	Yes*	Yes	No	No	No	No
Shah et al., 2020	Blockchain technology used provides decentralized cloud storage system that ensures data security	No	Yes*	Yes	No	No	No	Yes	No
Darwish et al., 2020	Data integrity and reliability are preserved and user's privacy is increased	Yes	Yes	Yes	No	Yes	No	No	No
Ashik et al., 2020	Proposed architecture is way more flexible and robust than previous ones based on experiments	Yes	Yes	Yes	No	No	No	No	No

Siva Kumar et al., 2021	Proposed RSFSA-ABE algorithm has achieved less time complexity compared to other techniques	Yes	Yes	Yes	No	Yes	No	No	Yes
Mayuranathan et al., 2021	Provides high performance in terms of time, cost and improved security than the existing approaches	No	Yes	Yes	Yes	Yes	No	Yes	No
Yadav et al., 2020	Lowered the task of maintaining hard copy records and provides security mechanism using blockchain	No	No	Yes	No	No	No	No	No
Siddiqui et al., 2020	Provides solution to the threat to the information system by blockchain technology	Yes	No	Yes	No	No	No	No	No
Li et al., 2018	Prevents Repudiation and Replay attacks on data stored on cloud	No	Yes	Yes	No	Yes	No	No	Yes
Sharma et al., 2020	Proposes a novel system of Blockchain models appropriate for healthcare continuous information	No	Yes	Yes	No	No	Yes	Yes	No

The Table 1 contains 8 parameters:

P1: Portability; P2: New architecture; P3: Security of privacy; P4: Lack of standards; P5: Reliability; P6: Governance; P7: Metering; P8: Denial of service.

3 Methodology

3.1 Background

The finest modern development is certainly the Blockchain revolution. Block chain is a legitimate, computerized ledger of financial transactions that can be used to record exchanges involving money as well as almost anything of value.

3.1.1 Definition

A blockchain is a type of linked list that contains data blocks in chronological order. It is immutable and tamper-resistant according to cryptographic guarantees. In essence, it is a distributed decentralised ledger that can securely store certain basic hierarchical data. A blockchain is essentially a decentralised database or ledger. Each node in the network has an identical copy of the whole database, and data are stored in data structures called blocks. Since the majority of the copies of the ledger do not reflect this modification, attempts to modify or remove an entry in one copy of the ledger will be refused, ensuring security.

3.1.2 Working mechanism

Blockchain can carry out user transactions without the assistance of any middlemen. A block reflecting that transaction will first be produced whenever a user initiates a transaction on a Blockchain network. The desired transaction is broadcast throughout the peer-to-peer network of computers, known as nodes, after a block has been formed. The nodes then validate the transaction. Cryptocurrency, contracts, documents, or any other important information can be part of a confirmed transaction. A new block of information for the ledger is created once a transaction has been confirmed and integrated with existing blocks.

3.1.3 Types of Blockchain

There are three different kinds of blockchain which are: Public blockchain, Private blockchain and Consortium blockchain. A blockchain network that is public or permission-less allows for unrestricted participation by anybody. On a public blockchain that is managed by laws or consensus algorithms, the majority of cryptocurrencies operate. Organizations can restrict who has access to blockchain data using a private, or permissioned, blockchain. Specific sets of data can only be accessed by those who have been given authorization. A permissioned blockchain is the Oracle Blockchain Platform. Federated or Consortium blockchain is a blockchain network where a predetermined group of nodes or a certain number of stakeholders tightly regulate the consensus process (mining process).

3.1.4 Typical Blockchain Workflow diagram

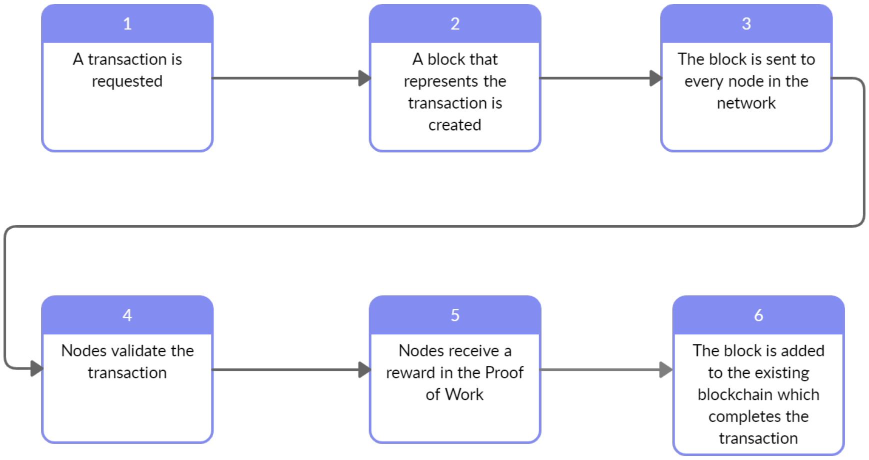
1
A transaction is requested
2
A block that represents the transaction is created
3
The block is sent to every node in the network
4
Nodes validate the transaction
5
Nodes receive a reward in the Proof of Work
6
The block is added to the existing blockchain which completes the transaction

Figure 1: How do Blockchains Work?

3.1.5 Softwares or Tools available to implement Blockchain

There are different Blockchain tools which are required for Blockchain development. Some of the most popular tools are: MetaMask [19], Web3j [7], Prysm [4], Remix Project[5],Truffle Suite[6]. A Chrome browser plugin called MetaMask [19] can communicate with decentralised apps (dApps). Users may send and receive digital assets using this open-source, decentralised wallet. The makers of Java WebSocket API developed Web3j [7] as a tool for blockchain. This useful library enables interaction and connection between developers and blockchain-based Ethereum-based decentralised apps (dApps). Prysm[4] is a tool created for developers to aid in the creation of decentralised applications. Along with a fully-featured client for the Ethereum 2.0 protocol built in Go, it also offers a thorough tutorial on how to create your first decentralised application so that you can get started right away. A platform for development tools using plugin architecture is called Remix Project[5]. It includes projects like Remix Libraries, Remix Plugin Engine, and of course Remix IDE.The Ethereum Blockchain framework known as Truffle[6] was created to offer a development environment for creating Ethereum-based applications.

3.1.6 Role of Blockchain in Cloud Security

Blockchain technology provides advanced solutions to address the challenges of the Cloud Computing. One of the most significant difficulties facing cloud computing is security and privacy. The greatest security risk for cloud computing is thought to be data leaks. Blockchain technology allows better database security and data account encryption. Yet another pervasive cloud threat is visibility. Blockchain helps create a shared, decentralized paradigm of trust that promotes more transparency. Public blockchain lowers data tampering and improves visibility of every activity. Information that has been saved in a series of blocks cannot be changed by anybody. Data integrity and authenticity are guaranteed since utilising data from anyone's computer on a blockchain network has no effect on the data stored on the other network devices. In addition, data stored on a blockchain is kept there indefinitely. As a result, it makes it simple to track out who is using the data and where, when, and how. Cloud computing depends on outside suppliers, which might result in significant data loss if these sources fail. Blockchains, on the other hand, are controlled by codes and don't involve third parties, making them an excellent reason for cloud computing. using blockchain technology

3.2 Problem Statement

According to Statista [28], in 2021, 64 % of the respondents feel that the biggest cloud security concern is data loss. 16.68 % of executives believe data security and privacy are the areas in greatest need of modification to help boost blockchain adoption as per findstack [11] which implies that Block chain technology is an effective solution to overcome the challenges faced by the Cloud Security. Many researchers observed transparency as another major threat to cloud security. Blockchain helps construct a decentralized and distributed trust model that allows more transparency.

There are several limitations in the methodologies proposed by the researchers in the related works section. Refining of the framework and implementation and validation of the results are required [35]. The efficiency of the proposed method was less than the previous proposed models [25]. The heavy size of blockchain highly limits the wide application of blockchain-based CloudEXs [34]. Blockchain technology could be somewhat disruptive and a radical rethink and significant investment in the EHR ecosystem is required[15]. This system had the potential to improve security protection, but there were still numerous unresolved problems, including difficult network node configuration, a multichain environment, hardware assaults, and privacy leaks [16]. More focus on authorization policies to club with authentication rules to grant user privileges is required [14]. Although it provided with great results but the proposed solution was complex to implement [37]. Reduction in access from the single point and location across the entire storage pool was dependent on the pay model [20]. MAC spoofing attacks were not considered for edge service providers and there was also need of security mechanism at LWC layer [26]. Because the proposed scheme used ECC algorithm the implementation became complex [10]. Software used in Bitcoin was of major concern, as the bug in the software which was used in Bitcoin could be critical [18]. An adaptive scheduling algorithm could be incorporated in future [30]. Blockchain-based hybrid algorithm inside the cloud infrastructure used more computational power and time and consumed more energy [13]. The user authentication scheme need to be developed further to ensure better access control [8]. The proposed method was complex to implement [33]. The mathematical model involved in blockchain security was trivial and needed more efficiency [22]. The proposed algorithm need to be more efficient and simple to be able to be adopted by Health sector [36]. Blockchain technology was realized as cyber money, and it was being used but some security problems with the wallet, transactions, and software were observed [32]. Due to the problem of packing delay in the blockchain system, the file records may be packed into the block for a long time, resulting in a long waiting time for the user [21]. In an open Blockchain, all records were unmistakable to the general population and anybody could partake in the understanding procedure [31].

A detailed study on the different Blockchain technology for Cloud Security was conducted and presented in Table 1. Upon analysing, it is understood that more researchers ([35],[15],[14],[37], [26],[10],[30],[13], [8],[33],[22],[21], [31]) have worked and developed solutions on parameter 2,3,5 and still, a lot of work needs to be done w.r.t parameter 1,4,6,7,8 as per Table 1. Though individual mechanisms have been proposed by multiple authors but the implementations of some architectures were not explored. Implementation of blockchain technology for securing health records in cloud for health sector is still in progress and needs more work which could be explored in the near future.

3.3 Discussion of existing solutions

Due to increase in amount of data day by day has caused a huge issue for its storage. To resolve this issue cloud based storage services are used. But it requires high end security of the stored data on the cloud which is accomplished by using blockchain technology. The suggested solution utilises a private cloud that is accessible from anywhere in the world and houses the ERP data of a corporation. It verifies and protects the company's personnel data. This concept is strengthened and made simpler for end users to utilise by adding security capabilities to smartphones and laptops like biometrics and password validation. Between the user and the background, laptops and smartphones' local validation processes serve as a user interface. Additionally, it serves as the next degree of security for user information validation. Consequently, a safer method of accessing cloud services is provided.

The local system verifies and handles the user request. This request is sent to the cloud server, which handles it based on whether data is being retrieved from the cloud or uploaded there. According to the request, the blockchain algorithm in this step either encrypts or decrypts the data. Furthermore, the cloud server verifies the accuracy of the data. The local server receives the output of the retrieval request and displays it to the user. When data is uploaded, the cloud

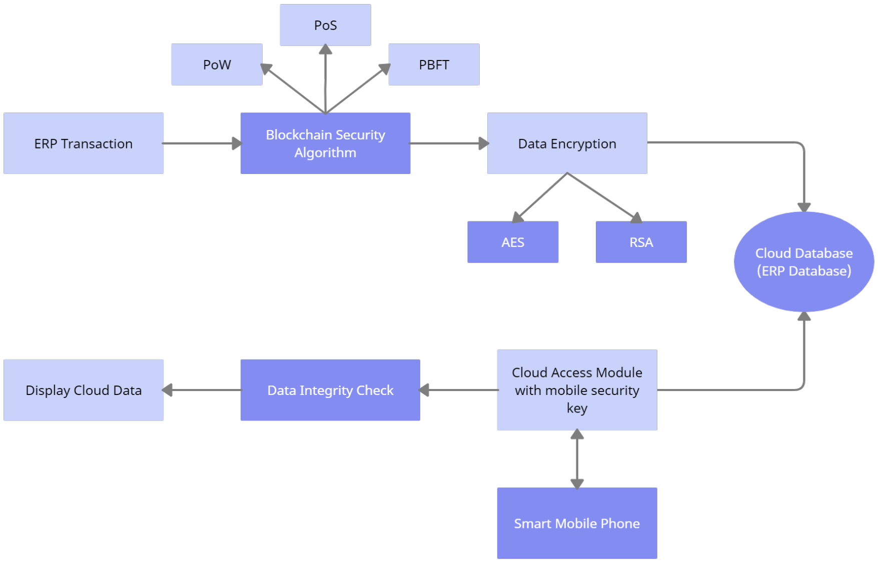
PoS
PoW
PBFT
ERP Transaction
Blockchain Security Algorithm
Data Encryption
AES
RSA
Cloud Database (ERP Database)
Display Cloud Data
Data Integrity Check
Cloud Access Module with mobile security key
Smart Mobile Phone

Figure 2: Overall architecture

receives it after the algorithm has been run.

According to the above diagram, to proceed with an ERP transaction requested by the user it goes through the Blockchain security algorithm. After which the data is encrypted and sent to the cloud database (ERP database). The data stored on cloud is accessed from smart mobile phones with security keys. Before displaying the cloud data, data integrity check is applied on the data stored on the cloud.

An ER diagram is used to describe the relationship between the various components of the architecture diagram. Through the ER diagram the overall scenario of the system becomes clearer. According to the ER diagram, the proposed system is divided into 4 parts: (i) Server-side definition which is the link between a user's system and a cloud system. (ii) Block chain development, validation, and verification. (iii) Android app with a two-step authentication process. (iv) Data storage in the cloud.

The ERP System is accessed by the users and admins. Employees and the customers of the company are considered as the potential users. Also, there can be a possibility of multiple admins. Admin authenticate the user request through Biometric authentication by the fingerprint matching for the security of the system. Users go through a data integrity check from the block database to ensure the reliability of the data. Meanwhile, the admin create the block and sets the access permissions to upload, delete or update the data stored on the cloud. Admin monitors all data transaction done by all users. Before user can access the cloud data, admin once again authenticate the user for the two-step authentication process.

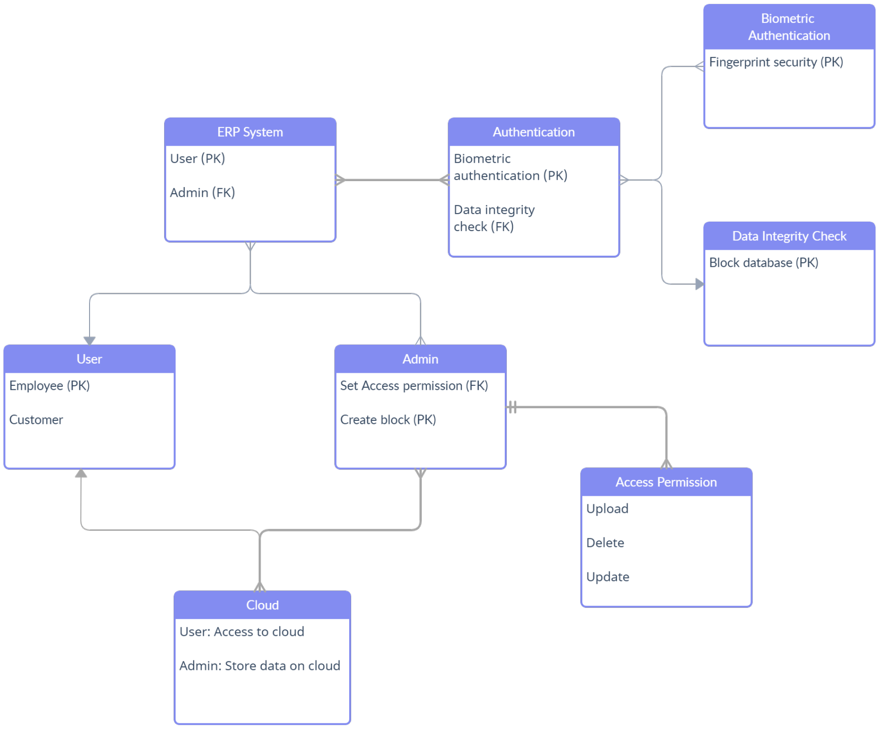

Figure 3: ER Diagram

Our proposed system uses the following algorithms for data encryption:
(1) AES Algorithm [24]
(2) RSA Algorithm [27]

To validate the transactions, Blockchain Security algorithms (also known as Consensus Algorithms) are used:
(1) Proof of Work (PoW) [23]
(2) Proof of Stake (PoS) [29]
(3) Practical Byzantine Fault Tolerance (PBFT) [9]

This proposed system aims to end the reliance on outside businesses to access and maintain cloud data so that the users can trust to put their confidential data on the cloud.

4 Evaluation

The process of measuring a system's performance while it is being tested is called performance evaluation. This assessment can include system-wide metrics like response time or latency as well as measure-specific tasks like the time it takes to write a block to persistent storage. Understanding and documenting the performance of the system or subsystem being tested is the aim of any performance evaluation. This frequently entails monitoring what transpires when dependent variables are changed; for instance, monitoring the system's throughput while the number of concurrent requests is changed.

The following tools are used for the evaluation of the proposed system:

(1) MS Visual Studio [12]

(2) Android Studio [17]

The following are the popular datasets used by the researchers for testing the performance of their proposed blockchain methodology:

(1) Blockchain explorer [1]

(2) Blockseer [2]

(3) Etherchain [3]

When creating a blockchain performance evaluation, there are a number of important factors to take into account. When evaluating the environment for performance testing, we need to keep the following in mind as well:

(i) Consensus protocol

(ii) Geographic distribution of nodes

(iii) Hardware environment of all peers

(iv) Network model

(v) Number of nodes involved in the test transaction

(vi) Software component dependencies

(vii) Test tools and framework

(viii) Type of data store used

(ix) Workload

The Table 2 describes the evaluation metrics used for measuring the performance of Blockchain used for the security of data on cloud:

Table 2: **Blockchain Performance Metrics**

Blockchain Metrics	**Network Metrics**	**Node Metrics**
Transaction Throughput Number of transactions committed per second	RPC response time The time required to complete a remote procedure call or REST-API	Cache hit ratio The ratio of number of serving and requesting contents from a node's cache
Transaction delay The time between submitting a transaction and committing it	Propagation delay The time taken to propagate a transaction throughout the Blockchain peer to peer network	Transaction per memory Utilization of memory for processing every transaction

Contract execution time The time for executing a smart contract and deploying in the Blockchain	Peer discovery time Time required for a Blockchain node to find out its peer	Transaction per CPU The utilization of the CPU when running the smart contracts
Consensus cost time The time taken for a transaction to be processed and validated	State updating time Time required for the world state to be changed while running smart contract	

5 Future directions

The proposed system currently works on only a prescribed combination system OS but it can be designed to work on any combination of OS. The System now only works with one kind of data, but it may be made to handle any kind of data. Depending on how the user uses the system, the cost can be reduced.

A cloud service transaction architecture based on double-blockchain structure is suggested in order to increase the reliability and effectiveness of trust certification in real-time transactions. This Cloud service transaction model based on a double-blockchain structure can be used for authentication of users in the architecture proposed in existing solutions section as a hybrid system.

The Trust Authentication Blockchain (TAB) is in charge of managing trust information in the cloud service marketplaces and disseminating the findings of trust assessments to other nodes. Identity trust data and behaviour trust data are the two pieces that make up each block in TAB. By using specially created consensus processes, miners are in charge of storing, validating, and verifying the consistency of the trust data. The trade data block is created and stored by the trading behaviour blockchain (TTB).

Double-chain parallel computing may be accomplished with the advantages of the double-blockchain construction TAB + TBB, which boosts computational effectiveness. Furthermore, double-chain mutual monitoring offers increased security and data traceability. Additionally, because the TAB provides the trust value and leaves the large-scale computation or evaluation of trust to the TBB, this may significantly minimise latency. As a result, more real-time and high-reliability scenarios can be achieved using blockchain technology.

6 Conclusion

The proposed system enhances the security of data by encrypting and distributing the data across multiple peers in the system. The general structure of

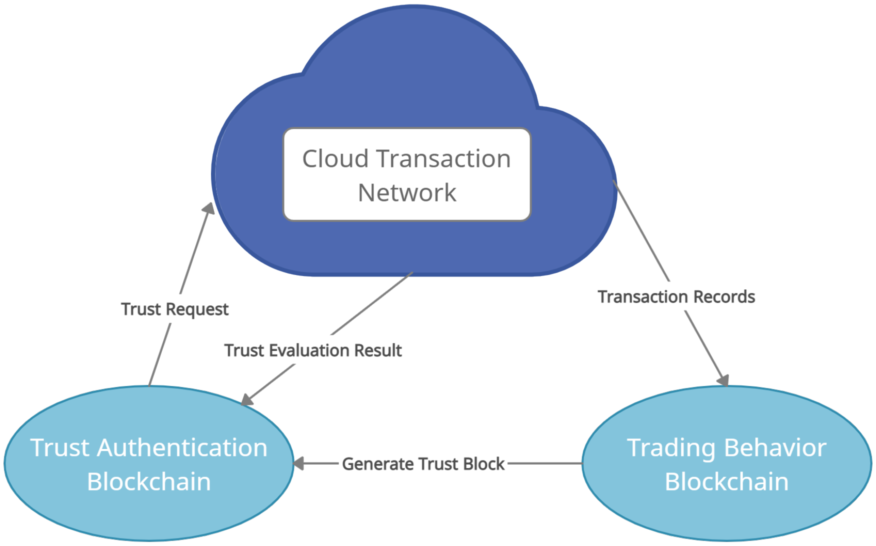
Cloud Transaction Network
Trust Request
Trust Evaluation Result
Transaction Records
Trust Authentication Blockchain
Generate Trust Block
Trading Behavior Blockchain

Figure 4: Cloud service transaction model based on a double-blockchain structure

Blockchain has been explored in this paper. Furthermore, the security needs of Blockchain and Cloud Computing have been examined. Based on this investigation, it has been shown that Blockchain can be an appropriate and powerful technology for providing security in the Cloud Computing environment. Cloud computing is considered to be the future of computing and storage technology. This research also examined the various available blockchain solutions for Cloud security.

References

[1] Blockchain explorer. https://www.blockchain.com/explorer.

[2] Blockseer. https://www.blockseer.com/.

[3] Etherchain. https://etherchain.org/.

[4] Prysm tool. https://github.com/prysmaticlabs/prysm.

[5] Remix project tool. https://github.com/ethereum/remix-project.

[6] Truffle suite tool. https://trufflesuite.com/.

[7] Web3j tool. https://github.com/web3j/web3j.

[8] M. H. Ashik, M. M. S. Maswood, and A. G. Alharbi. Designing a fog-cloud architecture using blockchain and analyzing security improvements. In *2020 international conference on electrical, communication, and computer engineering (ICECCE)*, pages 1–6. IEEE, 2020.

[9] M. C. Barbara Liskov. Practical byzantine fault tolerance (pbft). `https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/`, 1999.

[10] T. Benil and J. Jasper. Cloud based security on outsourcing using blockchain in e-health systems. *Computer Networks*, 178:107344, 2020.

[11] R. Carter. The ultimate list of blockchain statistics (2022). `https://findstack.com/blockchain-statistics/`, March 2022.

[12] M. Corporation. Ms visual studio. `https://visualstudio.microsoft.com/`, 1997.

[13] M. A. Darwish, E. Yafi, M. A. Al Ghamdi, and A. Almasri. Decentralizing privacy implementation at cloud storage using blockchain-based hybrid algorithm. *Arabian Journal for Science and Engineering*, 45(4):3369–3378, 2020.

[14] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain. Authentication protocol for cloud databases using blockchain mechanism. *Sensors*, 19(20):4444, 2019.

[15] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37, 2018.

[16] K. Gai, J. Guo, L. Zhu, and S. Yu. Blockchain meets cloud computing: a survey. *IEEE Communications Surveys & Tutorials*, 22(3):2009–2030, 2020.

[17] J. Google. Android studio. `https://developer.android.com/studio/`, May 2013.

[18] A. Gupta, S. T. Siddiqui, S. Alam, and M. Shuaib. Cloud computing security using blockchain. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 6(6):791–794, 2019.

[19] C. S. Inc. Metamask tool. `https://metamask.io/`, 2016.

[20] P. K. Kollu et al. Blockchain techniques for secure storage of data in cloud environment. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(11):1515–1522, 2021.

[21] C. Li, J. Hu, K. Zhou, Y. Wang, and H. Deng. Using blockchain for data auditing in cloud storage. In *International Conference on Cloud Computing and Security*, pages 335–345. Springer, 2018.

[22] M. Mayuranathan, M. Murugan, and V. Dhanakoti. Enhanced security in cloud applications using emerging blockchain security algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 12(7):6933–6945, 2021.

[23] C. D. Moni Naor. Proof of work (pow). https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/, 1993.

[24] U. N. I. of Standards and T. (NIST). Aes algorithm. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/, 2001.

[25] S. Pavithra, S. Ramya, and S. Prathibha. A survey on cloud security issues and blockchain. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, pages 136–140. IEEE, 2019.

[26] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Naseer. Cloud based secure service providing for iots using blockchain. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2019.

[27] L. A. Ron Rivest, Adi Shamir. Rsa algorithm. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/, 1977.

[28] J. A. Sava. Biggest cloud security concerns 2020-2021. https://www.statista.com/statistics/1172265/biggest-cloud-security-concerns-in-2020//, July 2022.

[29] S. K. Scott Nadal. Proof of stake (pos). https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/, 2012.

[30] M. Shah, M. Shaikh, V. Mishra, and G. Tuscano. Decentralized cloud storage using blockchain. In *2020 4th International conference on trends in electronics and informatics (ICOEI)(48184)*, pages 384–389. IEEE, 2020.

[31] S. Sharma, A. Mishra, D. Singhai, et al. Secure cloud storage architecture for digital medical record in cloud environment using blockchain. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[32] S. T. Siddiqui, M. Shuaib, A. K. Gupta, and S. Alam. Implementing blockchain technology: way to avoid evasive threats to information security on cloud. In *2020 international conference on computing and information technology (ICCIT-1441)*, pages 1–5. IEEE, 2020.

[33] A. Siva Kumar, S. Godfrey Winster, and R. Ramesh. Efficient sensitivity orient blockchain encryption for improved data security in cloud. *Concurrent Engineering*, 29(3):249–257, 2021.

[34] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran. Blockchain for cloud exchange: A survey. *Computers & Electrical Engineering*, 81:106526, 2020.

[35] H. Xu, J. Cao, J. Zhang, L. Gong, and Z. Gu. A survey: cloud data security based on blockchain technology. In *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, pages 618–624. IEEE, 2019.

[36] D. Yadav, A. Shinde, A. Nair, Y. Patil, and S. Kanchan. Enhancing data security in cloud using blockchain. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 753–757. IEEE, 2020.

[37] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu. Authprivacychain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access*, 8:70604–70615, 2020.