Library Progress International
Vol.44 No. 3, July-December 2024:
P. 25576-25593

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Blockchain-Based Distributed Data Security and trust management System for Cloud Computing

Poonam Kumari[1] , Meeta Singh2

Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India.

How to cite this article: Poonam Kumari, Meeta Singh (2024) Blockchain-Based Distributed Data Security and trust management System for Cloud Computing. *Library Progress International,* 44(3), 25576-25593

Abstract

Cloud computing is rapidly being used in many facets of the IT business since it has emerged as a crucial technology for meeting infrastructure and data service demands at lower costs, with less effort, and with more scalability. Despite the rapid growth of cloud computing, data security remains a significant challenge that has yet to be fully resolved. This ongoing concern hampers the development of cloud services. In a landscape utilizing distributed ledger technology and service-oriented architecture, blockchain emerges as a promising decentralized solution. The main security problem, however, is key leakage, which makes it simple for outsiders to access guarded data.

This research presents the Blockchain-based Proof of Staking with Elliptic Curve Encryption (BPECE) technique, designed to enhance the security of data transfers in the cloud. To address potential vulnerabilities, it employs the Policy-based Key Authentication (PBKA) algorithm, which efficiently verifies the authenticity of each node in the network. This approach aims to provide a robust solution for securing cloud data transactions. The suggested method creates a public key for every document. In comparison to earlier ways, the suggested solution provides improved security performance.

Keywords: *Blockchain, Cloud Computing, Privacy, Data Security, Authentication, Algorithms.*

1. Introduction

A blockchain-based distributed data security system for cloud computing is a framework designed to enhance the security and privacy of data stored and processed in cloud environments. By leveraging blockchain technology, this system provides a more secure way to manage data, ensuring better protection against unauthorized access and breaches. Its innovative approach aims to create a safer cloud computing experience for users and organizations alike.

Traditional cloud computing architectures frequently depend on central data storage, which can be open to hacker assaults and data breaches. Incorporating blockchain can address various security and privacy challenges [1].

Blockchain, which is inherently decentralized and unchangeable, into cloud computing platforms.

1. Decentralized Data Storage: Using numerous nodes (computers) in the blockchain network, the system may disseminate encrypted data instead of keeping it on a single cloud server. Since each node maintains a copy of the encrypted data, it becomes significantly harder for unauthorized parties to access or modify the information [2].

2. Encryption of Information and Access Control: The data is encrypted to safeguard its secrecy before being placed on the blockchain. Smart contracts on the blockchain can be utilized to manage access control, ensuring that only authorized parties have the rights to access specific data [3].
3. Immutable Data Integrity: The blockchain's immutability guarantees that once data is recorded, it cannot be altered or deleted without the consensus of the majority of network participants. The possibility of unauthorized adjustments is decreased thanks to this feature, which helps protect the data's integrity and dependability [4].
4. The blockchain network employs a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate and agree on the current state of the blockchain. This technique guarantees that access requests and data alterations are only granted if they comply with the network's set criteria.
5. Identity management: A decentralized identity management system, made possible by blockchain, gives users authority over their digital identities. This lowers the possibility of identity-related attacks [6] and increases system security as a whole.
6. Transparency & Audit Trail: Every blockchain transaction generates an auditable and transparent trail that records every access to and alteration of data. Enhancing accountability and assisting with GDPR compliance are two benefits of this functionality[7].
7. Data resilience and fault tolerance: The blockchain's distributed data storage makes the system more resistant to malfunctions and

online assaults. The data is still available through other nodes in the network even if some of them fall offline.

8. Secure Data Exchange: Without the need for middlemen, blockchain-based smart contracts can enable secure data exchange between different parties. [8] This functionality can speed up data communication while ensuring the confidentiality and integrity of the data.

1.1 Cloud Computing

Cloud computing, in its simplest form, refers to the delivery of computing services over the Internet ("the cloud"), which includes servers, storage, databases, networking, software, analytics, and intelligence. This model fosters quicker innovation, flexible resources, and economies of scale. Typically, you only pay for the cloud services you use, which helps reduce operational expenses [6] [7] [8], enhances infrastructure management, and allows for growth in line with your company's evolving needs.

1. *Best features of cloud computing:* Cloud computing represents a significant shift in how organizations traditionally viewed IT resources. Businesses commonly cite the following seven reasons for adopting cloud computing services [9].

2. *Cost:* Transitioning to the cloud enables companies to lower their IT expenses. This is because cloud usage [10] mitigates the capital costs linked to purchasing hardware and software, as well as establishing and maintaining on-site data centers, which require server racks, continuous power for cooling, and IT personnel for infrastructure management—all of which can be quite costly.

3. *Speed:* Most cloud computing services are self-service and on-demand, allowing organizations to quickly provision even large quantities of computing resources, typically with just a few clicks [11][51]. This provides businesses with significant flexibility and alleviates the challenges of capacity planning.

4. *Global scope*: One major advantage of cloud computing services is the ability to elastically scale resources. This means providing the right level of IT resources at the right time and from the right location, whether that involves adjusting processing power, storage, or bandwidth.

5. *Productivity*: Managing in-house data centers often involves extensive hardware setup, software updates, and other time-consuming IT tasks [12]. Cloud computing reduces the need for many of these activities, allowing IT staff to concentrate on more strategic business goals.

6. *Performance:* Leading cloud computing services are supported by a global network of secure data centers that are continuously updated with the latest high-performance computing technology [13][52]. This setup offers several advantages over a single corporate data center, including reduced network traffic.

7. *Reliability:* Cloud computing simplifies data backup, disaster recovery, and business continuity by enabling data replication across multiple redundant sites within the cloud provider's network.

8. *Security:* Many cloud service providers offer a comprehensive array of policies, tools, and controls, which enhance overall security and protect your infrastructure, applications, and data from potential threats [14].

1.2 Distributed Data Security

A potent answer to the problems of protecting data privacy, integrity, and accessibility in cloud-based systems is distributed data security in blockchain technology. The decentralized and immutable nature of blockchain technology can safeguard sensitive data from unauthorized access and manipulation [15]. To ensure confidentiality and reduce the risk of a single point of failure, data is encrypted before being shared across multiple nodes in the blockchain network. Additionally, smart contracts facilitate access control, enabling fine-grained permissions and ensuring that only authorized users can interact with specific data sets. The transparency and audibility of the blockchain create an indelible audit trail that improves accountability [16] and makes it easier to comply with data standards.

The consensus technique also validates data transfers, prohibiting unauthorized changes and unauthorized access attempts. While encouraging data sharing and cooperation while preserving the confidentiality and integrity of their sensitive information, the integration of blockchain with cloud computing gives organizations more trust in data security. [17] However, as each organization's demands and expectations may differ, thorough planning and analysis of the unique use case are essential to developing an efficient distributed data security solution for cloud computing.

1.3 Blockchain as trust Management system

Blockchain offers a decentralized, transparent, and tamper-resistant architecture that has the potential to revolutionize trust management systems. Traditional [18] trust management techniques sometimes rely on centrally located authority or intermediates, which can be subject to manipulation, corruption, or single points of failure. On the other side, blockchain offers a distributed and consensus-driven solution to managing trust, providing greater standards of security, accountability, and openness.

Blockchain is an open, decentralized, and distributed database system, where each data block is produced by a cryptographic algorithm and often arranged in line with build linkages from. A new distributed computing [18] [19] paradigm is called blockchain. its main design principles benefits are decentralized, transferable, and don't require nodes to be trusted algorithms for encryption, methods for time stamping, methods for achieving consensus, and incentives mechanisms. Peer-to-peer-based point-to-point is implemented with the help of network technologies, coordination, sharing, and cooperation of information. A blockchain is made up of a series of blocks that are ordered chronologically and provide a comprehensive record of all active transactions in Figure 1.

Blockchain is an open, decentralized, and distributed database, where each data block is produced by a cryptographic [20] algorithm and often arranged in line with build linkages. A new distributed computing paradigm is called blockchain. Its main design principles benefits are decentralized, transferable, and don't require nodes to be trusted algorithms for encryption, methods for time stamping, methods for achieving consensus, and incentives mechanisms. Peer-to-peer-based point-to-point is implemented with the help of network technologies, coordination, sharing, and cooperation of information. [21] A blockchain consists of a sequence of interconnected blocks that are ordered chronologically and provide a comprehensive record of all active transactions.

Decentralization is a key feature of blockchain technology. In traditional trading systems, every transaction must be validated by a trusted central authority, leading to increased costs and security risks associated with a central server. In contrast, users within the blockchain network uphold data integrity through a consensus mechanism, removing the need for a central authority [22].

Furthermore, transaction data can be verified quickly, and once recorded on the blockchain, it is extremely difficult to delete, modify, or reverse a transaction. During the verification process, any block containing fraudulent transaction data is promptly identified and discarded.

To conceal their genuine identities, each user interacts with the blockchain using a randomly [23] created user address.

Finally, there's the aspect of audit ability. In Bitcoin, user balance information is managed through the Unspent Transaction Output (UTXO) mechanism, requiring each transaction to reference previous, unspent transactions. Once a transaction is recorded on the blockchain, its status is updated accordingly [24]. This structure allows transaction records to be easily traced and verified. Given the critical features of blockchain technology, such as security, irreversibility, and immutability, numerous fintech companies, government agencies, and tech firms have recently begun exploring and implementing this technology. Existing blockchain solutions can be broadly categorized into three types, similar to the way cloud computing has been classified by application, as shown in Figure 1. The first type is the Public Blockchain, exemplified by virtual currency systems like Bitcoin and Ethereum [25]. The second type is the Private Blockchain, with notable examples including the Hyperledger project from the Linux Foundation, the R3 Corda platform, and the Gem Health network. Lastly, the Consortium Blockchain category features initiatives such as IBM's Fabric, MicroBank's BCOS project, and the Golden Chain Alliance.

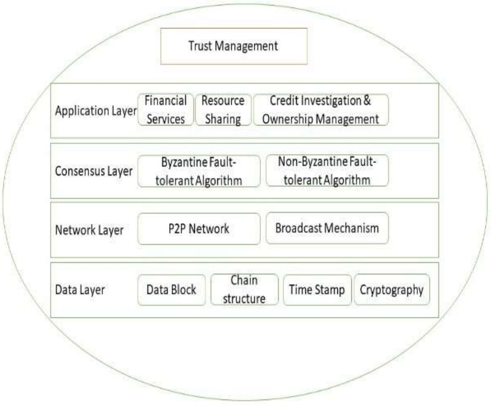

Figure 1: Layer used in Computing for Trust Management

1.3.1 Blockchain Infrastructure

1.3.1.1 Cloud Data Storage Security-Related Technology

After examining the security needs of modern cloud storage, it becomes clear that the three aspects of anti-eavesdropping, tamper resistance, anti-discarding, and anti-abuse correspond to the core elements of data security: confidentiality, integrity, and availability (CIA). Key methods for ensuring data security in cloud storage include data encryption, access control, [26] data integrity verification, and data recovery technologies. In this discussion, we will provide a brief overview of the technologies related to integrity verification and ciphertext access control.

Data storage serves as both the basis and the main focus of cloud computing in Figure 2. [27] The primary priority for cloud computing security protection is also data security. Consequently, data information is a crucial component of an enterprise's assets.

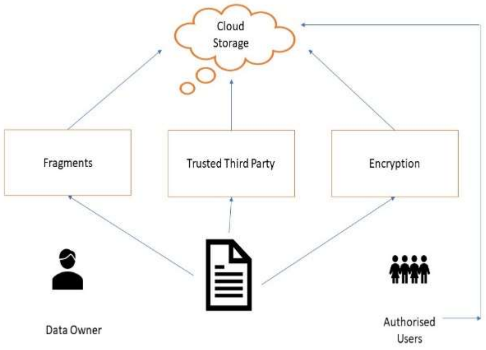

Figure 2: Data Security in Cloud Storage

Ciphertext access control technology ensures data confidentiality, meaning that unauthorized users cannot access or obtain data intentionally, and only data owners and authenticated users have the right to do so [28]. One of the most common methods for maintaining data secrecy is encryption, which users typically employ to encrypt their data before transmitting it. Their information to a cloud one of the essential methods for guaranteeing the legitimacy of usage of information, protection of network resources, and use of system resources, various access control models, the topic implements resource access depending on several rules due to the data. The user's access to data that is kept in the cloud and is in the cipher text state is referred to as a ciphertext access, control issue. The user's access is restricted via the ciphertext access control technique through encryption of the key data and access rights management [29].

The attribute-based ciphertext access control (ABAC) algorithm integrates access control with encryption techniques and restricts data access to those who meet certain requirements and choice criteria for attributes. ABAC offers greater flexibility and more precise access control granularity, so It is better suited to scenarios where cloud storage has several tenants and frequent permission changes. In the KP-ABE and CP-ABE algorithms, users can only decrypt data when the attribute set defined in the access tree is met. Given the high level of system openness, robust resource sharing, and the significant data dynamics in cloud storage environments, CP-ABE is the more suitable option [30] than KP-ABE, access control systems.

2. Literature Review

The study uses Bloom filters to give cloud-based trust and is based on a concept of data ownership that has been independently confirmed. The studies' findings [31] demonstrate that, even when the Bloom filter creates false positives, the suggested methodology is effective and yields validation rates comparable to those of the currently used methods. The recommended service may therefore analyze cloud trust management.

Table 1: Provides several explorations of the literature review, as can be seen.

Year/ Journal	Methodology	Research Gap	Outcomes

IEEE Access 2019	Cloud-based data security for the Internet of Things utilizing a Policy Decision Point (PDP) method with a Bloom filter.	However, the suggested approach has not been used to successfully upload data from a particular IoT device into cloud storage and then validate that data.	the suggested service can analyze a huge volume of data created in an IoT context efficiently.
Cybernetics and Information Technologies, 2019	The (DBFH-CDS) method is based on the Java programming language and the bank marketing dataset sourced from the UCI machine learning repository.	When the fragments are encrypted using various cryptographic methods, the security of the DBFH-CDS Technique is significantly increased.	When compared to state-of-the-art studies, it is clear that cloud data storage capacity gives more precise findings.
Chinese Journal of Electronics, 2020	a safe method of transmitting information using CBF,	Transfer of information from a source cloud to two or more destination clouds.	Accomplish safe data sharing and be able to delete information for good.
IEEE 2019	Cryptographic	Public key-recognizable encryption in cloud storage.	Using direct secure encryption scheme to secure data through tokens
IEEE 2020	Content-Based Image Retrieval	CBIR and K-cluster issues with privacy protection.	Parallelism research for an encrypted image in secure cloud computing.
IEEE 2022	Validate the versatility and effectiveness of Chain FL by incorporating a complex offloading decision model into the platform and implementing it in an Industrial IoT environment that faces security risks.	However, the suggested approach has not provided more scalability and reliability	Chain FL can be implemented as a federated learning platform with improved security to tackle the challenges presented by big data and potential attacks in Industrial Internet of Things (IIoT) environments.
Journal of Cloud Computing, 2021	A thorough survey of blockchain-based trust approaches in cloud computing systems.	There exists a significant gap between the theoretical aspects of the method and its practical implementation.	Examines the application of blockchain through the lens of trust.
JOURNAL OF LATEX CLASS FILES, 2019	Proposes a distributed and trusted authentication system that leverages blockchain and edge	To enhance performance and availability, implement this system in a blockchain-based data	Simulation results demonstrate that the proposed caching strategy achieves a higher hit ratio and lower

	computing to enhance authentication efficiency.	sharing platform for pilot verification.	delivery latency compared to other caching methods, such as popular caching and random caching.
IEEE, 2021	A novel vehicular fog cloud network (VFCN) comprising various components and heterogeneous computing nodes.	The budget and fault-tolerance considerations for IoT applications within the VFCN.	The proposed scheme surpasses existing contemporary scheduling methods in terms of cost, security, and deadline adherence.
JOURNAL OF LATEX CLASS FILES, 2021	A many-objective optimization algorithm utilizing a dynamic reward and penalty mechanism (MaOEA-DRP) to enhance the validity model for shard validation.	The issue of dynamic nodes needs to be addressed.	The proposed algorithm markedly enhances the throughput and validity of sharding, resulting in improved security for blockchain-enabled Industrial Internet of Things (IIoT) systems.

2.1 Phases of Blockchain trust approaches

A thorough analysis of block chain trust methods for authentic interactions with cloud computing settings is provided in this section.

The fundamental trust research taxonomy and blockchain techniques in the many trust-based cloud computing applications serve as our foundation for document categorization. As a result, three categories are used to group the associated solutions: a [32] blockchain-based fundamental trust framework, a framework and methods for trust interaction, blockchain enhanced cloud data management in Figure 3.

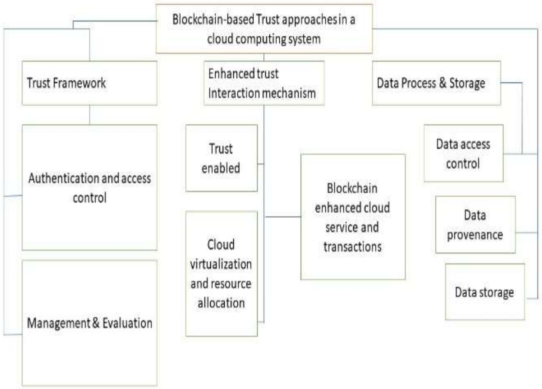
Blockchain-based Trust approaches in a cloud computing system
Trust Framework
Enhanced trust Interaction mechanism
Data Process & Storage
Authentication and access control
Management & Evaluation
Trust enabled
Cloud virtualization and resource allocation
Blockchain enhanced cloud service and transactions
Data access control
Data provenance
Data storage

Figure 3: Blockchain trust approaches in cloud computing

There are two sub-research modules in the fundamental trust framework: Identity identification and access control, followed by behavior monitoring and management. The framework and methods for blockchain-enhanced trust interactions encompass the following four sub-research modules[33] : 1) Blockchain cloud transactions, 2) Blockchain resource allocation and job offloading, 3) Blockchain resource management, and 4) Trust-enabled Cloud Virtualization. The three main sub-research topics for blockchain-enhanced data management include: 1) data access model, 2) data provenance, and 3) data storage. We shall outline the research developments in the aforementioned areas in the section that follows.

2.2 Framework for fundamental Trust based on Blockchain

[34] Traditional trust frameworks rely on a centralized model, placing a significant processing and computing burden on the central node. This setup is prone to potential issues, such as single points of failure and susceptibility to malicious fraud, making it less effective for real-time application scenarios. Additionally, trust ratings are not completely acknowledged because the center can only see the trusted proof.

The trust authentication process may be decentralized because to blockchain's inherent decentralization feature, which solves the aforementioned centralization-related issues[35] .

2.3 Identity verification and access management

The core element of trust-based cloud computing is identity management. Identity authentication ensures that service providers, consumers, and other stakeholders in the cloud are verified as [36] legitimate nodes. Traditional identity management methods often rely on a third-party management center, which introduces potential security risks, including excessive authority of the certification center and single points of failure. An alternative approach, identity federation, can help tackle security and trust challenges across diverse domains in large distributed systems, but it also complicates system design and operation [37].

They studied how blockchain may assist players in mitigating attacks against them and presented an abstract authentication draw on blockchain architecture and graph theory, as outlined in Tables 2 and 3, trust-related data can be integrated into an encrypted blockchain framework. they demonstrated that five widely used attacks could be successfully alleviated.

Table 2: Access Management for Authentication Mechanism

Reference	Effectiveness	Rely on accuracy	Safety/ Privacy
[17]	√		
[18]			√
[19]	√	√	
[20]		√	√
[21]			√

Table 3: Contribution of target & improvement in Blockchain

Reference	Target & contribution	Improvement in Blockchain	Solution to attack
[22]	To create a trust network for authentication, a graph theory model is used, and open distributed ledgers are used to protect TM systems.	a consensus graph-theoretic model.	Attacks with covert targets, duplicate registration, outdated information, denial-of-service attacks, and censorship.
[23]	A blockchain-based trust model to assist CSPs in managing trust on their own	proof-of-stake and proof-of-eligibility combined	/
[24]	Decentralised WSN trust management and authentication	/	/

[25]	mechanism for managing identities based on blockchain	Mechanisms for voting and reputation-based incentives (RpCoin rewards and penalties)	/
[26]	Utilise blockchain to control accounts in cloud data centres	Contracts for the Saranyu Manager, the Tenant, and the Delegation	/
[27]	In-vehicle networks using a blockchain-based reputation system for data trustworthiness	/	Fake messaging

3. Methodology

3.1 Framework and procedures for trust interaction augmented by blockchain

3.1.1 Framework for blockchain cloud services

In real-world situations, Service Level Agreements (SLAs) don't always hold up and aren't carried out as needed. For the purpose, modified the conventional SLA service model by including a new function called "witness" to identify service breaches and so assure credibility. [38] In order to negotiate and cut petrol usage, cloud providers and customers applied the game theory concept of Nash equilibrium.

In the proposed model, witnesses are regular nodes within the blockchain network that oversee cloud transactions, as illustrated in Figure 4. They ensure that transactions proceed as intended and that all parties fulfill their obligations. The witness pool is established after customers and providers agree on the implementation details of the Service Level Agreement (SLA) during the transaction, which includes aspects such as service duration, cost, compensation, and the number of [39] co-employed witnesses. Following this, a smart contract for the witness pool is executed to randomly select a specified number of witnesses.

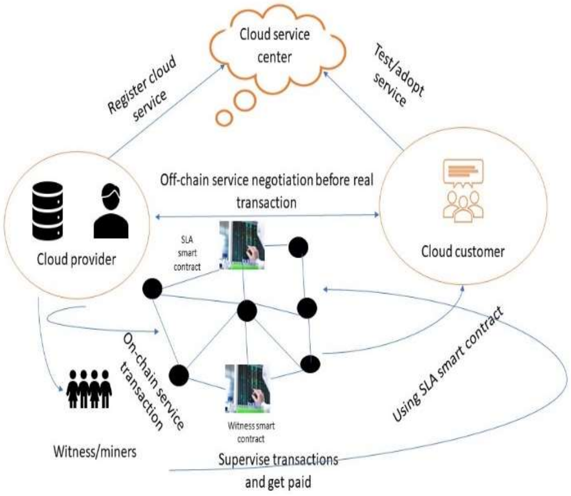

Figure 4: Cloud Service Center for transaction

3.1.2 Cloud transactions based on the blockchain

The core activities of cloud computing are service transactions since it is a type of business model that offers IT services. [40] Untrusted computer environments cannot, of course, guarantee a secure transaction. It proposed a bilateral agreement utilizing a consortium blockchain architecture referred to as the Clean room Security Service Protocol (CSSP), which is effectively a CSSP. The SaaS computing environment was the primary focus of CSSP's design.

3.1.3 Enhanced by trust, cloud virtualization

The most widely used virtualization solution nowadays is Docker, which significantly increases operating system resource utilization with minimal added expense. Authentication is crucial for cloud users to determine whether an image is malicious. However, the current authentication solution provided by Notary Docker is inadequate to defend against attacks.

Decentralized Docker Trust (DDT), a blockchain-based trust architecture, was introduced by Q. Xu et al. [41] in order to address the possible vulnerabilities in Docker Content Trust (DCT). DDT has the benefits of lowering the possibility of DoS attacks and offering digital signature verification services Table 4.

Table 4: Verification services for Authentication vulnerabilities

Reference	Efficiency	Overhead	Effectiveness	Trust accuracy	Throughput	Se Pri
[38]		√				
[39]			√			
[40]		√	√			√
[41]	√	√	√		√	
[42]	√			√	√	
[43]	√					√
[44]	√				√	
[45]	√	√	√			
[46]	√					
[47]	√			√		

Reference	Efficiency	Overhead	Effectiveness	Trust accuracy	Throughput	Se Pri
[48]	√					
[49]						√
[50]	√	√		√		√

3.2 The correctness of the verification process

During the evidence validation phase, the user, after receiving the evidence submitted by the storage service, uses their public key and predetermined parameters to compute the verification equation. This allows them to determine whether data integrity has been compromised. If the data remains intact—meaning the parameters have not changed—the user calculates both sides of the verification equation.

3.3 Algorithm

3.3.1 Rivest-Shamir-Adleman

The RSA algorithm is an old algorithm and it is an asymmetric cryptography. The RSA algorithm is a block cipher that can [42] transform plaintext into encrypted message and encrypted message back into plaintext. When User A's public key is utilized for encryption, it can only be used for decoding purposes.

The RSA technique is not very effective for authenticating huge amounts of data when using the same virtual network. Authentication tokens' trustworthiness must be proven by a non-domestic organization. Because of the involvement of intermediaries, the cryptosystem is vulnerable to corruption [45] .

3.3.2 Data Encryption Standard *(DES) Algorithm in Cryptography*

To encrypt and decrypt data, the Data Encryption Standard (DES) uses a block cipher, classifying it as a symmetric cipher technique. DES serves as the industry standard for security, and its operation is based on the structure of the Fiesta cipher. DES processes a 64-bit plaintext block and produces a 64-bit ciphertext.

1. Sub-key Generation
2. Encryption

4. Implementation

In the method that has been presented, the content of the file is recorded on the blockchain, and Bitcoin is transferred from one patient's wallet to another via smart contracts. This is done by passing the cryptocurrency from one peer to another.

AES is an encryption method that can be used to increase the safety of user data that is kept in cloud storage. The solution that is being proposed associates a user's wallet address to their file in such a manner that only[46] the user who is the rightful owner of the file may access the file's contents. The Ethereum blockchain stores all of the user data. In order to use smart contracts, the Ethereum blockchain network must exist, which are the means by which the blockchain can hold the information of a file that was submitted by a user. The data that is uploaded and downloaded using the proposed method is encrypted and decrypted at each and every step of the process. The IPFS Protocol is utilized by the[system to facilitate the effective distribution of files across the various peers that make up the network.

Metamask: Metamask is a crypto currency wallet that enables users to securely store, send, and receive cryptocurrencies. It acts as a bridge between the Ethereum network and standard [46] browsers, facilitating interaction with decentralized applications (dapps) on the Ethereum platform. To use Metamask effectively, it is essential to understand some key terms associated with it.

Peers: Users that have committed to renting out part of the free storage space to meet the file storage demands of other users are known as "storage providers." The Advanced Encryption Standard (AES) is a symmetric-key algorithm featuring a block length of 128 bits, with support for key lengths of 128, 192, or 256 bits, depending on the user's preferences [47].

4.1 Cloud service transaction model based on a double- Blockchain structure

Identity verification and behavior evaluation are integral components of a comprehensive trust authentication system. In a P2P network topology, a node's identity information is typically static and easy to authenticate and assess. In contrast, trading behavior is dynamic, requiring significant processing power to record and analyze. To enhance the reliability and efficiency of trust certification in real-time transactions, a cloud service transaction architecture based on a dual blockchain structure is proposed, as illustrated in Figure 5.

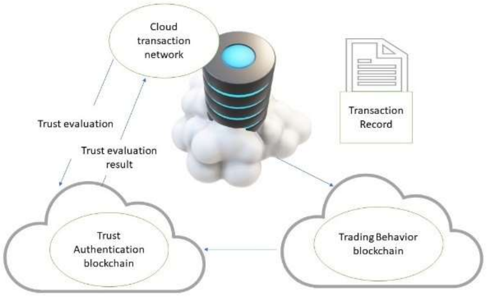
Cloud transaction network
Transaction Record
Trust evaluation
Trust evaluation result
Trust Authentication blockchain
Trading Behavior blockchain

Figure 5: Cloud transaction network based on double blockchain

4.2 Trust Authentication Blockchain (TAB)

In cloud service marketplaces, TAB is responsible for managing trust data and distributing the results of trust assessments to other nodes. The trust data is divided into two distinct categories for each block in TAB: identity trust data and behavior trust data. When a node initially joins, only identity trust is added to a block; however, as time progresses and [48] transactions occur, behavior trust is continuously incorporated into new blocks. Authentication is carried out by a select group of supervisors, which may include regular miners or specific nodes designated by the market authority.

Miners utilize specially designed consensus methods to store, validate, and ensure the consistency of trust data. Nodes are required to pay a fee to execute a smart contract for initial identity verification when they apply to join the trade network. Additionally, they must pay a fee to access the trust information of other nodes. This funding serves as the incentive fee for the miners. [49]

4.3 Trading behavior Blockchain (TBB)

The trading data block must be created and stored by the Transaction Blockchain (TTB). Miners in the Trust Behavior Blockchain (TBB) are responsible for receiving the latest transaction results, generating the transaction block, assessing behavior trust, creating the trust block, and sending it to the Trust Authentication Blockchain (TAB). The miners will then confirm and store the corresponding trust block in TAB.

4.3.1 Double-Blockchain Structure

The dual blockchain architecture, consisting of TAB and TBB, facilitates double-chain parallel computing, enhancing computational efficiency. Moreover, this structure allows for mutual monitoring between the chains, which improves security and data traceability [50]. By assigning the responsibility of providing the trust value to TAB and delegating large-scale calculations or evaluations of trust to TBB, latency can be significantly reduced. Consequently, blockchain technology enables the realization of more real-time and high-reliability scenarios.

5. Result & Discussions

Cloud computing experiences a greater impact on storage, security, and privacy as a result of blockchain integration. Our survey indicates thatprivacy, security, and storage are the key parameters of the cloud ecosystem that have been significantly enhanced by blockchain technology, as shown in Figures 6 and 7.

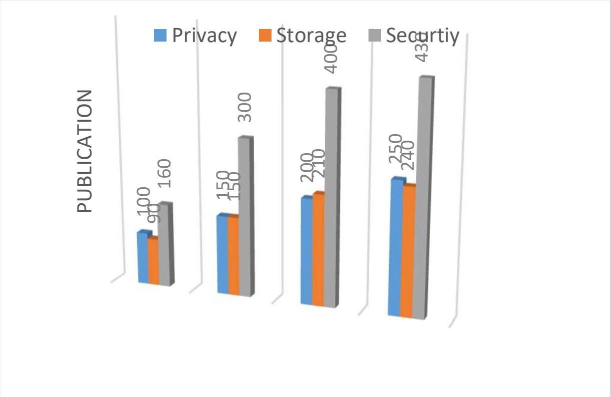

Figure 6: Publication of cloud security, storage and privacy during 2019 to 2022 period.

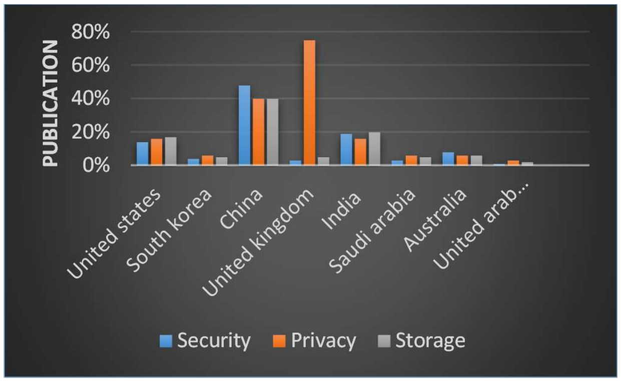

Figure 7: showing country-wise publication on applicability of Blockchain technology and cloud storage, security and privacy.

According to our survey, the five sub domains listed (Blockchain integrated with Cloud for Smart Healthcare; Block chain integrated with Cloud for Finance; Blockchain integrated with Cloud for Agriculture; Blockchain integrated with Cloud for Supply Chain; Blockchain integrated with Cloud for Smart City) are the most significant ones in terms of works relating to blockchain and integrating the cloud.

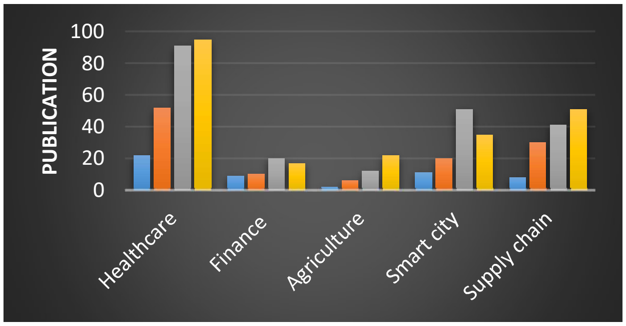

Figure 8: Publication in different application areas during the period of 2019 to 2022.

6. Future Scope

Despite numerous scholars proposing ideas for blockchain trust management, there remain substantial gaps between theory and real-world applications. The following outlines future research directions, categorized into four modules based on various trust research domains.

1. Trust foundation: Framework for decentralized trust based on blockchain: Naturally decentralized and peer-to-peer consensus architecture is blockchain. However, cloud computing systems may be built in a variety of ways, and as IoT, edge computing, and fog computing applications have grown in popularity, so too has the cloud's manner of realisation. Consequently, a blockchain trust framework must consider how to adapt to different cloud application scenarios and provide specialized and flexible trust authentication architecture.

2. Decentralized establishment and upkeep of trust relationships: The collaboration and rivalry between provider and user, broker and provider, broker and provider, and broker and provider are only a few examples of the many different types of trust relationships that exist in cloud computing systems.

3. Aspecialised blockchain trust operation method: The key problems in blockchain applications include smart contracts, consensus methods, and incentive mechanisms. The blockchain-based trust management still has to solve these concerns. For instance, how to solve blockchain security challenges like attacks against blocks or smart contracts, faked transactions, etc., and how to motivate miners to actively engage in trust evaluation, trust judgements, and data verification.

4. Trust Assessment Methodology: Blockchain, a distributed ledger, enables the creation of comprehensive and verifiable transaction records across cloud organizations. However, calculating trust from the original transaction data necessitates the use of specialized assessment techniques. Thus, it is crucial to explore suitable trust assessment methodologies.

5. Regard for authorization and delivery: Trust is transitively conditional. People are able to gauge their level of confidence in an unknown or newly traded company. Accurately assessing a node's trust level in a blockchain-based trust network is straightforward; however, challenges remain in determining a node's recommendation trust and in allocating trust rights to a composite application or other connected nodes.

7. References

1. Xu M, Buyya R (2019) Brownout approach for adaptive Management of Resources and Applications in cloud computing systems. ACM Comput Surve 52(1):1–27

2. Zhu Y, Zhang W, Chen Y, Gao H (2019) A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment. EURASIP J Wirel Commun Netw 247(2019). https://doi.org/10.1186/s13638-019-1605-z

3. Li X, Gui X (2010) Cognitive model of dynamic trust forecasting. J Software 21(1):163–176

4. Tahta U, Sen S, Can A (2015) GenTrust: a genetic trust management model for peer-to-peer systems. Appl Soft Comput 34(2015):693–704. https://doi.org/10.1016/j.asoc.2015.04.053

5. Sanadhya S, Singh S (2015) Trust calculation with ant Colony optimization in online social networks. Procedia Computer Sci 54(2015):186–195. https://doi.org/10.1016/j.procs.2015.06.021

6. Gao H, Huang W, Duan Y (2021) The cloud-edge-based dynamic reconfiguration to service workflow for Mobile ecommerce environments: a QoS prediction perspective. ACM Transact Int Technol 21(1):1–23. https://doi.org/10.1145/3391198

7. Zhang P, Kong Y, Zhou M (2017) A novel trust model for unreliable public clouds based on domain partition. In Proceedings of IEEE 14th International Conference on Networking, Sensing and Control (ICNSC). IEEE, pp 275–280

8. Li W, Ping L, Pan X (2009) Trust model to enhance security and interoperability of cloud environment. In: Proceedings of CloudCom'09 the 1st International Conference on Cloud Computing. Beijing. Springer, Berlin, pp 69–79

9. Li W, Wu J, Zhang Q, Hu K, Li J (2014) Trust-driven and QoS demand clustering analysis based cloud workflow scheduling strategies. Cluster Comput 17(1):1013–1030

10. Li X, He J, Du Y (2015) Trust based service optimization selection for cloud computing. Int J Multimedia Ubiquitous Engineering 105(2015):221–230

11. HuckleS. **et al.**Internet of things, blockchain and shared economy applications Procedia Comput. Sci. (2016)

12. YuanY. **et al.**

    1.1. Blockchain: The state of the art and future trends Acta Automat. Sinica (2016)

13. PilkingtonM.

    1.1. Blockchain technology: Principles and applications Soc. Sci. Electron. Publ. (2015)

14. PassR. **et al.** Analysis of the blockchain protocol in asynchronous networks

15. AzariaA. **et al.** MedRec: Using blockchain for medical data access and permission management

16. Yli-HuumoJ. **et al.** Where is current research on blockchain technology?-A systematic review Plos One (2016)

17. ZhangN. **et al.**Blockchain technique in the energy internet: Preliminary research framework and typical applications Proc. Csee

    (2016)

18. KiayiasA. **et al.** Ouroboros: A provably secure proof-of-stake blockchain protocol

19. WeberI. **et al.** Untrusted business process monitoring and execution using blockchain

20. YueX. **et al.**

    1.1. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control J. Med. Syst. (2016)

21. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. In IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE. DOI: 10.1109/BigDataCongress.2018.85

22. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2016). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computers in Biology and Medicine, 2, 30-42. DOI: 10.1016/j.compbiomed.2016.04.010

23. Wang, S., Wen, Q., Hao, Y., Zhang, Y., & Yang, J. (2019). A Blockchain-based Cloud Storage System with Enhanced Security and Privacy. Future Generation Computer Systems, 95, 674-686. DOI: 10.1016/j.future.2018.12.026

24. Zheng, Z., Xie, S., Ning, H., Wang, H., & Yang, Y. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE. DOI: 10.1109/BigDataCongress.2017.85

25. Xu, R., Zhang, L., David, K., Li, Y., & Li, S. (2020). A Survey of Blockchain Technology Applied to Smart Grids and Cloud Computing. In 2020 IEEE/ACM 1st International Workshop on Emerging Trends in Microservices and Serverless (TREND) (pp. 33-38). IEEE. DOI: 10.1109/TREND49487.2020.00009

26. Li, J., Gao, Z., Kim, J. S., Kim, S., Li, S., & Huh, E. N. (2017). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. Journal of Network and Computer Applications, 171-180. DOI: 10.1016/j.jnca.2017.06.016

27. Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL) (Vol. 310, p. 8).

28. Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations (pp. 225-253). Edward Elgar Publishing.

29. Tai, S., Xu, S., Li, Z., & Ni, Q. (2019). Towards Practical Blockchain-based Integrity Verification Schemes for Cloud Storage Systems. Future Generation Computer Systems, 97, 61-73. DOI: 10.1016/j.future.2019.02.056

30. Belotti M, Bozic N, Pujolle G et al (2019) A Vademecum on Blockchain Technologies: When, Which and How. IEEE Commun Surveys Tutorials 21(4):3796–3838.

31. Belotti M, Bozic N, Pujolle G et al (2019) A Vademecum on Blockchain Technologies: When, Which and How. IEEE Commun Surveys Tutorials 21(4):3796–3838. https://doi.org/10.1109/COMST.2019.2928178

32. Ali M, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehman M (2019) Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Commun Survey Tutorials 21(2):1676–1717

33. Liu Y, Yu F, Li X, Ji H, Leung VM (2020) Blockchain and machine learning for Communications and networking systems. IEEE Commun Survey Tutorials 22(2):1392–1431. https://doi.org/10.1109/COMST.2020.2975911

34. Gai K, Guo I, Zhu L, Yu S (2019) Blockchain Meets Cloud Computing: A Survey. IEEE Communications Survey Tutorials. https://doi.org/10.1109/COMST.2020.2989392

35. Saad M, et al. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 22(3):1977–2008

36. Yang R, Yu F, Si P, Yang Z, Zhang Y (2019) Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. IEEE Commun Survey Tutorials 21(2):1508–1532

37. Cole J, Milosevic Z, Raymond K (2011) Decentralized trust management. In: van Tilborg HCA, Jajodia S (eds) Encyclopedia of cryptography and security. Springer, Boston

38. Li H (2016) Study on trust model and controversy discovery under web 2.0 circumstance. Doctor thesis, XiDian University, China

39. Kuwabara K (2000) Reputation systems: facilitating Trust in Internet Interactions. Commun ACM 43(12):45–48

40. Kamvar S, Schlosser M, Garcia-Molina H (2003) The Eigentrust algorithm for reputation management in P2P networks. ACM 2003:640–651

41. Xiong L, Ling L (2004) PeerTrust: supporting reputation-based Trust for Peer-to-Peer Electronic Communities. IEEE transactions on knowledge \& data

42. Li W, Ping L, Pan X (2010) Use trust management module to achieve effective security mechanisms in cloud environment. In: Proceedings of 2010 international conference on Electronics & Information Engineering IEEE, p 2010

43. Li X, Ma H (2015) T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services. IEEE Transact Information Forensics Security 10(7):1402–1415

44. Mrabet M, Saied B, Saidane L (2016) A new trust evaluation approach for cloud computing environments. In proceedings of 2016 international conference on performance evaluation and modeling in wired and wireless networks (PEMWN). IEEE

45. E. Abdallah, M. Zulkernine, Y. Gu , et al. 2017. TRUST-CAP: A Trust Model for Cloud-Based Applications in Proceedings of IEEE Computer Software & Applications Conference. IEEE 2017

46. Singh S, Sidhu J (2015) A collaborative trust calculation scheme for cloud computing systems. 2015. In proceedings of international conference on recent advances in Engineering & Computational Sciences. IEEE 2015

47. Nagarajan R, Selvamuthukumaran S, Thirunavukarasu R (2017) A fuzzy logic based trust evaluation model for the selection of cloud services. In proceedings of international conference on Computer Communication & Informatics. IEEE 2017

48. Pooranian Z, Shojafar M, Garg S, Taheri R, Tafazolli R (2021) LEVER: secure Deduplicated cloud storage with EncryptedTwo-party interactions in cyber-physical systems. IEEE Transact Industrial Informatics. https://doi.org/10.1109/TII.2020.3021013

49. Zhang P, Kong Y, Zhou M (2017) A novel trust model for unreliable public clouds based on domain partition. In proceedings of IEEE international conference on networking. IEEE 2017

50. Yefeng R, Durresi A (2017) A trust management framework for cloud computing platforms. In proceedings of IEEE 31st international conference on advanced information networking and applications (AINA), IEEE 2017

51. Kumari Poonam, Singh Meeta, "A Review: Different Challenges in Energy – Efficient Cloud Security" IOP Conf. Series: Earth and Environmental Science **785** (2021) 012002 IOP Publishing doi:10.1088/1755-1315/785/1/012002.

52. Kumari Poonam, Singh Meeta, "Cloud Security and Challenges" Review Of International Geographical Education ISSN: 2146-0353 ● © RIGEO ● 11(8), SPRING, 2021.