**Abstract**:

Cloud computing has broadened its service area, provides a better user experience than traditional platforms, and brings significant economic and societal benefits thanks to virtualization and resource integration. Building a trust-enabled transaction environment has emerged as a crucial aspect in the serious security and trust crisis that cloud computing is currently experiencing, according to a wealth of research. Traditional cloud trust models frequently use a centralized design, which results in significant administrative costs, network sluggishness, and even single points of failure. Furthermore, the outcomes of trust evaluations cannot be fully understood by all participants due to a lack of openness and traceability.

Blockchain is a fresh and promising distributed computing paradigm and decentralized framework. The integrity, veracity, and security of the transaction data are ensured by its special characteristics in operating rules and record-tracking capabilities. As a result, building a distributed and decentralized trust architecture is a great use case for blockchain. This study conducts a thorough analysis of blockchain-based trust methodologies in cloud computing platforms. It outlines the open difficulties and provides guidelines for further study in this area based on a unique cloud edge trust management architecture and a double-blockchain structure-based cloud transaction model.

**Introduction:**

Cloud computing has emerged as one of the most popular IT research topics in recent years because of its indefinite extension of resource sharing and improved user experience, and its enormous commercial potential is progressively becoming more apparent.

However, there are significant security and trust issues with cloud computing platforms. For instance, in 2016, the well-known cloud security service provider Cloudflare disclosed that a serious flaw in its code had caused the privacy data of at least 2 million websites, including services from numerous well-known Internet companies like Uber and 1password, to be exposed.

Failures in the public cloud storage component of Microsoft Azure in March 2017 had a more than 8-hour impact on linked cloud operations. 200 million US voters' personal information was made public in June 2017 due to a security flaw in Amazon Web Services. Up to 88% of cloud clients are concerned about data security and want to know what is occurring on the actual servers, according to a Fujitsu poll.

In general, the cloud computing platform poses three main trust problems.

Loss of control - Once users upload their data, code, and operating processes to remote cloud servers, they no longer have control over such resources.

Lack of transparency—Without knowing the fundamental workings, cloud computing is essentially a mystery to its users, raising their suspicions about invasions of privacy.

Many academics have started doing studies on trust.

An innovative trust approach, for instance, was developed by Li et al. and used to assess and forecast users' cognitive actions [3]. Evolutionary algorithms and trust models were introduced in [4, 5], along with a number of useful tactics to boost service management effectiveness [6–10]. The traditional trust approach, on the other hand, frequently relies on a single point of failure, congestion, and delay in a centralized third-party trust management center. Additionally, in a centralized trust framework, not all participants fully believe the conclusions of the trust evaluation because the proof of trust is not accessible to all users.

Blockchain technology has attracted a lot of attention as an emerging decentralized framework and distributed computing paradigm, and its use has seen a meteoric rise along with the acceptance of virtual cryptocurrencies. Blockchain is based on a decentralized P2P architecture, in which every node is equal and there is no central command. The advantages are:

* The chain data structure and consensus mechanisms ensure the integrity, credibility, and security of trust evidence.
* Maintenance of trust relationships no longer depends on a third-party center, and the damage from a few nodes cannot destroy the robustness of the system.
* The operating rules and data records are also open, transparent, and traceable.

**Background (Objectives**):

We will perform a thorough analysis of blockchain-based trust strategies used in cloud computing environments.

We will go beyond the confines of cloud computing to examine how blockchain might be applied in the many cloud implementation modes, such as P2P, IoT, edge computing, etc. It also suggests a taxonomy of blockchain-based schemes and provides a detailed analysis of the current methods.

For flexible trust management, it suggests a brand-new cloud-edge hybrid structure and a double-blockchain-based transaction model and directions for blockchain-based cloud computing trust management research.

**Methodology:**

Trust research classification: The sociology discipline gave birth to the idea of trust, which through time spread to the fields of management, finance, and computer technology. To address concerns with Internet security, M. Blaze et al. [37] initially suggested trust mechanisms in 1996. An innovative approach to addressing security issues in heterogeneous, open, dispersed, and dynamically changing network settings is trust management. The extent of the investigation is depicted in Figure 1.

The study of the notion of trust and its categorization based on particular traits is at the heart of the first branch, which is the essential component of trust research. Based on several classification techniques, trust can be split into the following categories, as depicted in Fig. 1 [9].

Depending on the manner used to acquire trust, there are three types of trust: integrated, direct, and indirect (recommended).

Identities and behaviors that can be trusted (based on the identity) [38]

Function and experience of trust (based on the moment of its occurrence)

Trust can be subjective or objective (depending on how it is portrayed).

Depending on the trust connection, there is both intra-domain and inter-domain trust**.**

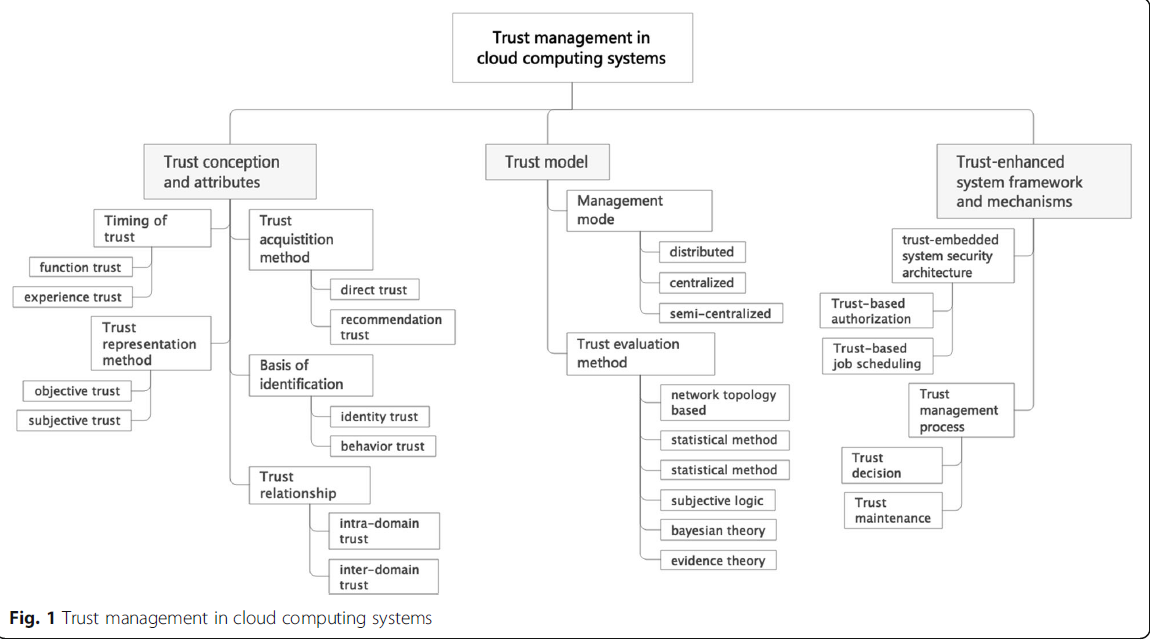
In order to provide a trust-enabled platform or trading settings, the modeling, evaluation, and management of trust are at the center of the second study subfield known as trust models. A trust model can be classified as either centralized or decentralized depending on the trust management mechanism. A central trust server, which is a centralized trust architecture is considered to be entirely credible and never hacked, is in charge of gathering, analyzing, and storing trust evidence from all parties. The two most prevalent centralized trust models are Taobao and eBay [39]. However, employing a centralized trust model could result in abnormal latency, blocking, or even a single point of failure, lowering the quality of service (QoS) of cloud services. As a result, decentralized trust frameworks were selected by other researchers. According to the trust evaluation method, trust

models can be divided into the following different types.

-network topology-based model

-statistical-based model.

An implementation of a trust-enabled system security framework is made possible by layering a trust management layer on top of the conventional cloud security architecture.

For cloud connectivity and engagement, trust mechanisms may offer protection. The common study challenges include job scheduling and trust-based permission. The design of trust-based decisions and the effective upkeep of trust are the fundamental components of trust-based mechanisms.

The study of trust-based methods for cloud computing still has a long way to go in terms of theory and application.

The majority of trust models are centralized, and even those that advertise being decentralized still require a third-party certification or trust center. This poses a number of security problems, including single points of failure, overload, and credibility loss.

Trust evaluation results are not persuasive or totally trusted because the trust evidence is not accessible to all participants and cannot be tracked.

Less flexible -

less flexible Expert scoring and averaging are two examples of subjective techniques used in trust decision-making.

technique, which renders the models arbitrary, unscientific, and unadaptable. Especially when it comes to bad recommendations, trust models are not strong enough to withstand malicious attacks (collusion).

huge man-

huge man It restricts trust-based software for complex network applications.

lack of a platform and prototype-

The majority of performance assessments for trust models are produced via simulation trials, which still require further analysis.

**Phases, taxonomy, and review of Blockchain-based**

**trust approaches**

In this section, we provide the fundamental trust research taxonomy and blockchain techniques in the many trust-based cloud computing applications that serve as our foundation for document classification.

As a result, the linked solutions are divided into three groups: a blockchain-based fundamental foundation for trust, a framework and mechanisms for trust interaction, and a blockchain-enhanced cloud data management system.

There are two sub-research modules in the fundamental trust framework: Identity authentication and access control, followed by behavior monitoring and management. Four sub-research modules make up the blockchain-enhanced trust interaction framework and mechanisms: 1) Blockchain-based cloud transactions; 2) blockchain-enhanced resource allocation and job offloading; 3) blockchain-enhanced resource offloading, and 4) trust-enabled cloud virtualization. And the three key sub-research topics for blockchain-enhanced data management are 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.

**Framework for basic trust based on blockchain:**

The classic trust frameworks always use a centralized paradigm, with the center node bearing a heavy burden of processing and computing overhead. This can easily lead to possible problems like a single-point failure and deliberate fraud, and they cannot adapt well to a real-time application environment. Additionally, trust judgments are not fully acknowledged because the center can only see the trusted proof.

The trust authentication process can be decentralized according to the blockchain's inherent decentralization characteristic, which solves the aforementioned centralization-related issues.

Identity verification and access management

**The foundational component of trust-based cloud computing is identity management:**

Identity identification makes ensuring that all cloud market participants, including service providers and clients, are verified, legitimate nodes. The traditional identity management approach typically calls for a third-party management center, which poses security issues such as the certification center's excessive authority and single point of failure.

Identity federation is another option for big distributed systems to address security and trust issues across various domains, but it complicates system design and operation.

**The restrictions are listed below:**

It was solely concerned with safeguarding CSPs and their assets, oblivious to the security and privacy needs of users. It is merely a theoretical model that hasn't been put into practice in a real cloud system.

Diagram

Description automatically generated with low confidence

Fig 2: Blockchain acting as an identity access platform.

**Behavior management and evaluation**:

The four service categories that Saranyu intended to provide are identity management, authentication, authorization, and billing. Public-private key pairs were used to manage the first two services. A smart contract enabled authorization.

Through the payment channels, charging was carried out in accordance with service or resource utilization.

Saranyu is an example of a distributed application built using the Web3 JavaScript library. To get services and earn properly from the platform's operation, tenants and users create accounts through the Saranyu DApp. Saranyu's architecture is depicted in Figure 3.

The paper makes two contributions: it implemented a range of services using smart contracts, such as service management and tenant management, which could somewhat guarantee transaction fairness; and it was a novel blockchain-based distributed App that combined open-source Quorum and smart contracts.

Diagram

Description automatically generated

Fig 3 – Architecture of Saranyu.

The work's limitation is that it can only be used in a distributed ledger that has a license and in which only legitimate entities are permitted to participate. Additionally, the App hadn't yet undergone a performance test in a setting for large-scale applications.

**Blockchain-enhanced resource allocation and task**

**offloading mechanisms:**

Building a distributed, decentralized framework for trust is possible with the help of blockchain technology. The consensus process, however, consumes a lot of energy, which prevents it from working to its full potential in a hybrid cloud-edge service paradigm. One of the potential answers to the paradox is cloud mining, which encourages miners to buy or rent resources from cloud providers.

The performance of blockchain applications based on cloud mining must be optimized.

The PoW offloading to the cloud or edge servers is depicted in Figure 4. The unique aspect of this research is that it took a different approach than other blockchain-based apps to examine how the blockchain consensus mechanism performed effectively on terminal devices with limited resources.

The resource rivalry and allocation issue in the situation of multiple suppliers and multiple miners was also resolved using the multi-leader multi-follower game theory.

The efficiency of the model in a real system cannot be validated as it only addressed the profit problem of task execution, and the size of the test nodes is quite tiny.

Diagram

Description automatically generated

Figure 4: PoW offloading to edge servers.

The above-given model, which utilizes an economic approach (game theory) for pricing when miners acquired resources, concentrated on how to assist miners in working efficiently in a resource-constrained environment. However, it missed the potential security and credibility analysis of their models.

**Data storage:**

An essential category of cloud services is data storage. Researchers have developed numerous distributed and blockchain-based methods in response to the data application security, privacy leakage, and trust crisis, as well as the performance bottleneck and single point of failure in the centralized data management center.

In order to address the copy distribution issue and enhance the performance and security of storage management, a blockchain-based distributed cloud storage security architecture was created. The user files in the suggested architecture were split into equal-length file blocks, encrypted, digitally signed, and then stored in the P2P network. Additionally, blockchain-based transactions were created, allowing users to rent out their own free space or cloud storage. Each file block's storage-related operations were meticulously recorded in the block's body in a secure, organized, and traceable manner.

The model has the following benefits.

It provided a thorough and in-depth analysis of how to choose the number of copies in a distributed storage system.

It maintained a very low level of file loss rate and transmission delay by using a generic method to handle the issue of copy replacement between different users and multiple data centers.

The model's weakness is that it does not explain how to configure related parameters, such as how to establish the trust threshold, which has a significant impact on whether malevolent vehicles may be successfully apprehended.

**Cloud computing transactions powered by blockchain**:

Since cloud computing is a type of business model that offers IT services, service transactions make up the core of it all. Untrusted computing environments cannot, of course, guarantee a secure transaction. A Cleanroom Security Service Protocol (CSSP), which is essentially a bilateral agreement based on a consortium blockchain framework, was presented in order to distribute and utilize software in a secure and tamper-resistant manner. CSSP was primarily created for the SaaS computing environment.

**The limitations of the model are**:

It did not make clear how to evaluate nonquantitative indicators like data integrity in the reputation computation model, it skipped the demonstration on the theoretical basis

of the new calculation model, with no details given on how to use the natural language

interpretation method for user feedback analysis.

**Summary:**

These blockchain-based approaches to managing trust are the outcomes of three years of research, demonstrating how the blockchain-based system is relatively new and represents the most recent development in creating decentralized and distributed trust. According to the distribution of the countries, 18 were from China, 5 were from the United States, 4 were from Singapore, and the remaining 8 were from Australia, Germany, India, Argentina, Netherlands, Algeria, Switzerland, and France, showing that the scheme has received widespread acclaim from international research institutions.

A paradigm of trust management based on a hybrid cloud-edge architecture:

This review suggests a novel cloud-edge hybrid trust management framework in order to take advantage of the massive computing and processing power of a traditional cloud computing data center without sacrificing the benefits of the end-to-end, decentralized, data preservation features of blockchain technology.

**Blockchain-based decentralized trust framework:**

A naturally decentralized and peer-to-peer consensus framework is blockchain. However, cloud computing systems can 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 manifestation. Therefore, a blockchain-based trust framework must think about how to adapt to various cloud application scenarios and offer a specialized and adaptable trust authentication architecture.

**Data Privacy:**

Another important problem that needs to be addressed is data privacy.

Blockchain offers benefits such as data transparency and traceability, but these features also increase the danger of privacy violations and data abuse. Future research must strike a balance between user privacy and disclosure.

**Conclusion:**

The taxonomy and a study of blockchain-based trust management strategies in cloud computing systems are presented in this article. Three phases—blockchain-based fundamental trust framework, blockchain-improved trust interaction framework and mechanisms, and data management—are used to categorize these techniques into several taxonomies. Then, it gives an in-depth evaluation and comparison of the current blockchain-based trust strategies. A novel cloud-edge hybrid trust management framework and a cloud transaction model based on double blockchain are suggested to increase the effectiveness and adaptability of trust-enabled cloud computing**.**

The article also makes clear that there is a significant disconnect between the method's theory and its actual execution.

In conclusion, an interesting study area is using the blockchain approach to create a more reliable and secure cloud transaction environment.

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/1

0.1186/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. Yin Y, Li Y, Ye B, Liang T, Li Y (2021) A Blockchain-based incremental update

supported data storage system for intelligent vehicles. IEEE Trans Veh

Technol:1. https://doi.org/10.1109/TVT.2021.3068990

12. Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-based secure and

trustworthy internet of things in SDN-enabled 5G-VANETs. IEEE Access 7:

56656–56666. https://doi.org/10.1109/ACCESS.2019.2913682

13. Fu X, Yu FR, Wang J, Qi Q, Liao J (2019) Resource Allocation for Blockchain-

Enabled Distributed Network Function Virtualization (NFV) with Mobile Edge

Cloud (MEC), IEEE INFOCOM 2019. In: IEEE conference on computer

Communications workshops (INFOCOM WKSHPS), Paris, France, pp 1–6

14. Yang C, Tan L, Shi N et al (2020) AuthPrivacyChain: a Blockchain-based

access control framework with privacy protection in cloud. IEEE Access

2020(8):70604–70615

15. Horvath A III, Agrawal R (2015) Trust in Cloud Computing: a User’s

perspective. Proceedings of the IEEE SoutheastCon 2015. IEEE 2015:1–8

16. Harbajanka S, Saxena P (2016) Survey paper on trust management and

security issues in cloud computing. Symposium on colossal data analysis

and networking (CDAN). IEEE 2016:1–3

17. Rawashdeh E, Abuqaddom I, Hudaib A (2018) Trust models for Services in

Cloud Environment: a survey. In: In proceedings of 9th international

conference on information and communication systems (ICICS), IEEE 2018,

pp 175–180

18. Huang J, Nicol D (2013) Trust mechanisms for cloud computing. J Cloud

Comput Adv Syst Applications 2(9):1–14

19. Noor T, Sheng Q, Zeadally S, Yu J (2013) Trust management of services in

cloud environments: obstacles and solutions. ACM Comput Survey 46(1):1–

30

20. Monir M, AbdelAziz M, AbdelHamid A et al (2015) Trust Management in

Cloud Computing: a survey. In: In proceedings of IEEE seventh international

conference on intelligent computing and information systems (ICICIS'15),

IEEE 2015, pp 231–242

21. Chandni M, Sowmiya N, Mohana S et al (2017) Establishing trust despite

attacks in cloud computing: a survey. In proceedings of WiSPNET 2017. IEEE

2017:712–716

22. Lansing J, Sunyaev A (2016) Trust in Cloud Computing: conceptual typology

and trust-building antecedents. ACM SIGMIS Database 47 2(2016):58–96

23. Matin C, Navimipour J, Jafari N (2018) Cloud computing and trust

evaluation: a systematic literature review of the state-of-the-art mechanisms.

J Electrical Syst Information Technol 5(3):608–622

24. Matin C, Navimipour J, Jafari N (2017) A comprehensive study of the trust

evaluation mechanisms in the cloud computing. J Service Sci Res 9(1):1–30

25. Deshpande S, Ingle R (2017) Trust assessment in cloud environment:

taxonomy and analysis. In: Proceedings of international conference on

computing. IEEE 2017, pp 627–631

26. Alhanahnah M, Bertok P, Tari Z (2017) Trusting cloud service providers: trust

phases and a taxonomy of trust factors. IEEE Cloud Computing 4(1):44–54

27. Hawlitschek F, Notheisen B, Teubner T (2018) The limits of trust-free

systems: a literature review on blockchain technology and trust in the

sharing economy. Electron Commer Res Appl 29(2018):50–53. https://doi.

org/10.1016/j.elerap.2018.03.005

28. Cho J, Chan K, Adali S (2015) A survey on trust modeling. ACM Computing

Surveys 48(2):1–40

29. Granatyr J, Botelho V, Lessing O et al (2015) Trust and reputation models for

multiagent systems. ACM Comput Surveys 48(2):1–42

30. Xiao Y, Zhang N, Lou W, Hou Y T (2020) A Survey of Distributed Consensus

Protocols for Blockchain Networks, IEEE Communications Surveys &

Tutorials, 22(2):1432–1465

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

Li et al. Journal of Cloud Computing: Advances, Systems and Applications (2021) 10:35 Page 32 of 34

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 2003:640–65