International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.8 January - February – 2024
DOI:10.46647/ijetms.2024.v08i01.037 ISSN: 2581-4621

Trust Management in Cloud Computing Using Blockchain Technology: a taxonomy, review & future directions

[1] Meenal Sachdeva, [2]Dr Reena
[1] *Research Scholar (Computer Science & Applications), Baba Mastnath University, Rohtak*
[2] *Assistant Professor, Baba Mastnath University, Rohtak*

Abstract
Through visualization and resource integration, cloud computing has expanded its service its service area and offers a better user experience than the traditional platform, along with us business operation model bringing huge economic and social benefits. However, a large amount of evidence shows that cloud computing is facing with serious security and trust crises, and building a trust / enabled transaction environment has become its key factor. The traditional cloud trust model transparency and traceability trust evolution results cannot be fully recognized by all participants. Its unique features in operating rules and traceability of records ensure the integrity, undesirability and security of the transaction data. Therefore Blockchain is very suitable for constructing distributed and decentralized trust architecture. Based on a novel Cloud- Edge trust management framework and a double Blochkchain structure based cloud transaction model , it identifies the open challenges and gives direction for future research field.

Keywords: Decentralized trust management, Blockchain technology, Cloud computing, Distributed ledger

Introduction

With the unlimited extension of resource sharing and a better user experience, cloud computing has become one of the hottest IT research issues in the recent years .However, cloud system have encountered serious trust and security problems.

In general, there are three major trust risks in cloud computing platform.

- **Loss of control**. Cloud users loss control of their own data, code and running process once submitting them to remote cloud servers.
- **Loss of transparency**. Not knowing the internal operation mechanism, cloud computing is just like a black box to its users, raising their concern about privacy mechanism.
- **Loss of clear security assurance**. Although most cloud providers declare their Service Level Agreement service (SLAs) , trying to offer a certain degree of commitment to service reliability, security and privacy.

Our contributions

The vital offering of this paper are mentioned below:

- It conducts comprehensive reviews of blockchain- based trust approaches in cloud computing environment.
- It expands boundaries of cloud computing to analyze the application of blockchain in different implementation modes of cloud, including P2P, IoT, edge computing etc.

- It proposes a novel cloud-edge hybrid framework and double- blockchain based transaction model for the flexible trust management.

Related Surveys

There are already some surveys on the trust schemes in cloud computing environment. A. Horvath IIIet al. explored the issues of consumers trust in cloud computing system to help service providers improve their behaviors. S Harbajanka and P Sexena conducted a review on trust approach in cloud computing by pointing out the pros and cost of the related research. Same wise many more researchers have introduced many more survey and experiences on clod computing and Blockchain technology.

However, to the best of our knowledge still very few surveys have focused on blockchain- based trust solutions in cloud computing system

Therefore this paper chooses another prospective, which not only enhance the previous survey but also focuses on the blockchain based approach for trust-enabled service in cloud system.

Trust research in cloud computing systems

Trust research classification

The concept of trust originated from sociology, and gradually extended its boundaries to areas . of management, economics and computer science. Trust management provides a novel solution to solve security problem in heterogeneous, open, distributed and dynamically changing network environment.

As shown in fig 1. Trust can be divided into following categories based on different classifications methods:

- Direct trust, indirect trust and integrated trust.
- Identity trust and Behavioral trust.
- Function trust and experience trust.
- Objective trust and subjective trust.

According to the trust evolution method, trust model can be divided into following different types:

- Network-topology based model
- Statistical – based model
- Fuzzy logic-based model
- Subjective logic- based model
- Bayesian theory –based model

The last research branch is trust-enhances system framework and mechanism. By adding a trust management layer on the top of the traditional cloud security model , a trust-enabled system security frameworks implemented. Trust management provides possible protection for cloud interconnection and interaction.

Recent Research Result

In recent year , trust-enabled cloud service management strategies have been intensively studied.

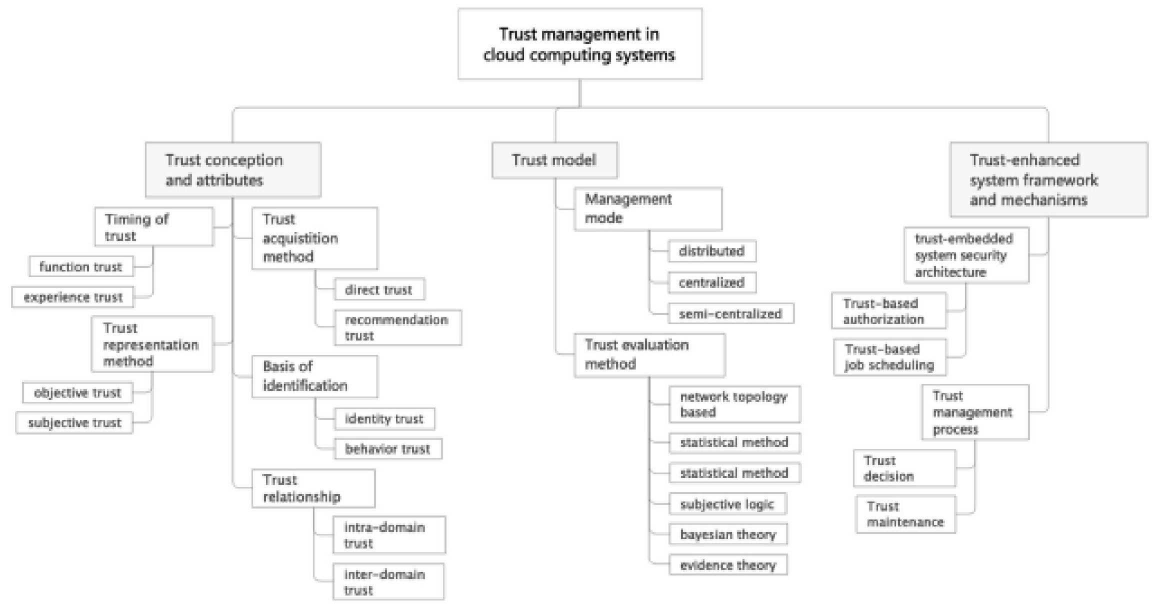


Fig. 1 Trust management in cloud computing systems

Research Challenges

At present, the research of trust-based approaches in cloud computing still faces huge challenges in theory and implementation.

- Most trust models are centralized And even those claim to be decentralized mode still needs third party trust and certification center.
- Inaccuracy of trust evaluation result.
- Less adaptive.
- Huge management overhead.
- Lack prototype and protocols.

Literature selection and methodology

Search method

We searched for relevant literature in the mainstream academic databases, namely ACM Digital Library, IEEEXplore, Springers.

We used two-stage literature search method in the first stage the world “trust”, “ blockchain”, and “cloud computing” were used to search the title keywords and abstract of research paper.

Even after doing so , not many more articles were found. As there are many practical form of cloud computing, such as P2P, wireless cloud/ cloud IoT Integration etc, in the second phase we adjusted the search strategy and only used keyword “trust” and “blockchain”;

Phases taxonomy and reviews of Blockchain-based trust approaches

In this section , we provide a comprehensive review on the blockchain – based trust approaches for credible interaction in cloud computing environments.

Our basis for document classification is the basis research taxonomy of trst and the blockchain methods in the different firlds of trust-nased cloud computing applications .Thus the related solutions are classified into three categories:

- Blockchain- based basic trust framework
- Blockchain-enhanced trust interaction framework and mechanism
- Blockchain-enhanced cloud data management

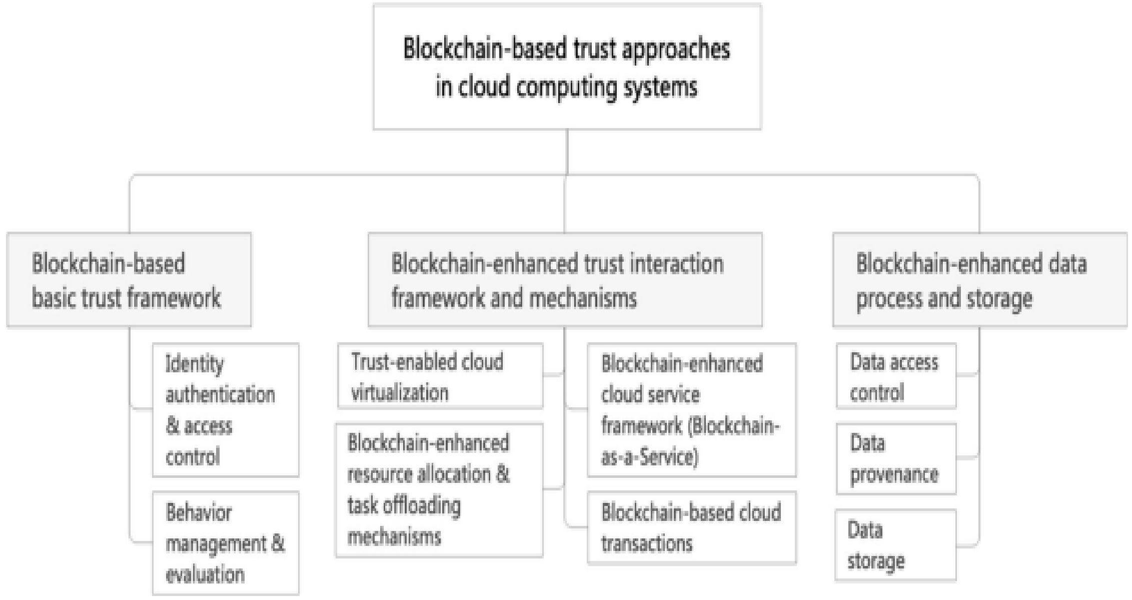

Blockchain-based trust approaches in cloud computing systems
Blockchain-based basic trust framework
Identity authentication & access control
Behavior management & evaluation
Blockchain-enhanced trust interaction framework and mechanisms
Trust-enabled cloud virtualization
Blockchain-enhanced resource allocation & task offloading mechanisms
Blockchain-enhanced cloud service framework (Blockchain-as-a-Service)
Blockchain-based cloud transactions
Blockchain-enhanced data process and storage
Data access control
Data provenance
Data storage

Fig. 2 Phases of blockchain-based trust approaches in cloud computing systems

Blockchain-based basic trust framework

The traditional trust framework always adopt a demoralized model with the center node suffering from huge burden of computing and processing overhead, which may easily leads to possible failures such as single point of attack and malicious froud and cannot adapt to a real time applications scenario.

The natural decentralized features of blockchain can decentralize the process of trust authentication, thereby overcoming the above problems caused by centralization.

Identity authentication and access control.

Identity management is the elementary chunk of Trust-based cloud computing. Identity authentication ensures that the participants of cloud markets, including service providers and consumers are authenticated.

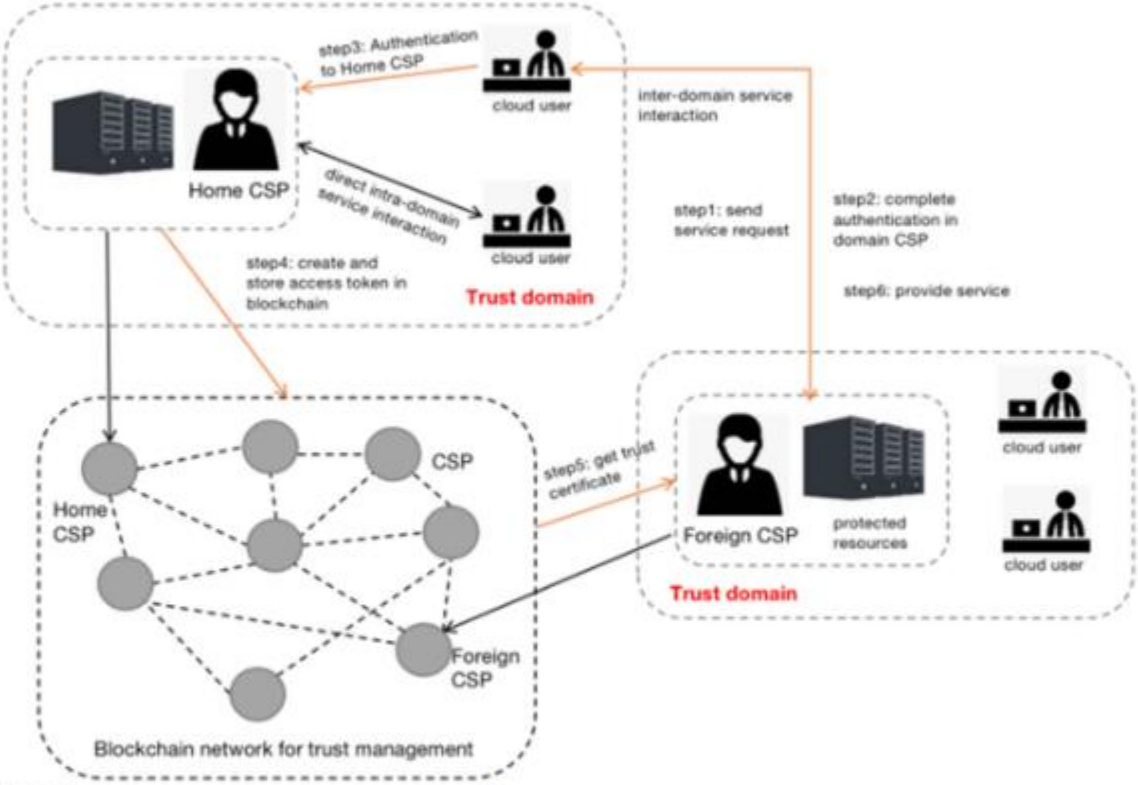

step3: Authentication to Home CSP
cloud user
inter-domain service interaction
Home CSP
direct intra-domain service interaction
cloud user
step1: send service request
step2: complete authentication in domain CSP
step4: create and store access token in blockchain
Trust domain
step6: provide service
CSP
Home CSP
step5: get trust certificate
Foreign CSP
protected resources
cloud user
cloud user
Trust domain
Foreign CSP
Blockchain network for trust management

Fig. 3 Blockchain acts as an identity authentication platform [65]

Behavior management and evaluation

Behavior trust is another key factor in accessing and predicting the credibility of entities behaviours. S.Nayak et at. Utilized smart contracts to propose Saranyu , a trust model for the efficient resource management in cloud computing system. Saranyu was designed to deliver four types of services: Identity management, authentication, authorization and charging.fig 4

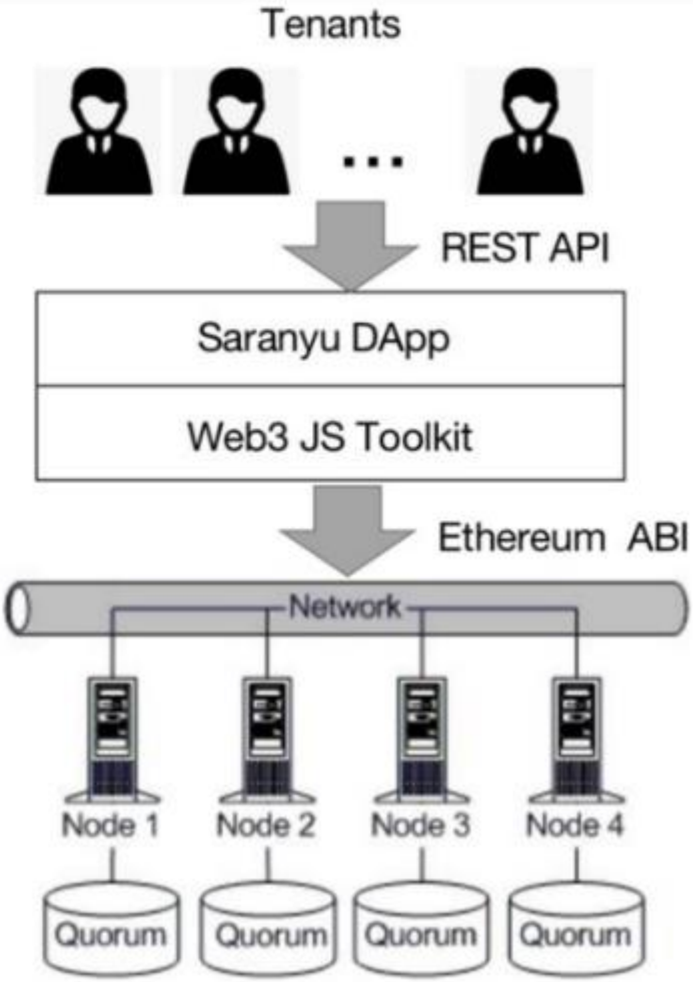


Fig. 4 Architecture of Saranyu [68]

Blockchain –based cloud service framework (lockchain-as-a-service)

In practical level, the Service Level Agreement (SLAs) sometimes are not credible and automatically executed as required. To this end , H Zhou added a new role " witness" to additional SLAs service model to detect service violation and thus ensure the credibility.

Blockchain –based cloud transaction

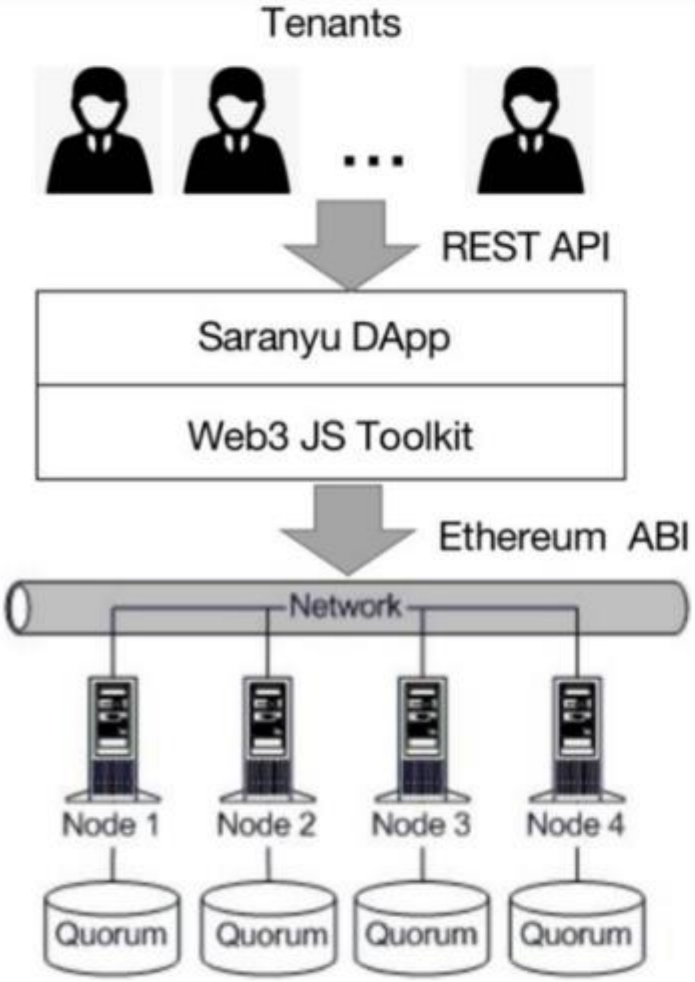
Cloud computing is a kind of business mode that provides IT services , ths service transaction are its Kernel affairs.Tp deploy and use software in a secure and tamper-resistant manner , Zhou proposed a Cleanroom Security ServiceProtocol(clssp), which actually a bilateral agreement based on a consorfium blockchain framework.

CSSP was mainly designed for the SaaS computing environment.

Blockchain-enhanced resource allocation and task offloading mechanism:

It is an effective way to construct distributed and decentralized trust framework. However, the consensus mechanism requires a lot of energy consumption, preventing it from the best effect in hybrid cloud-edge service model. Cloud mining which encourages miners to purchase from cloud providers has become one of the possible solution to the contradictions.

shown in fig below:



Future scope & Conclusion

The main objective of our paper is to resolve the problems occurred like security issues in cloud computing. for this we had tried to integrate double blockchain structure with the edge computing . As the security is an key term of blockchaining to record transaction at specific period of time and use different hash which cannot break easily by intruders. One other term terminology of blockchain is virtualization, Which also provide safety to no. of users. So both the terminology resolve the issue. Although many researchers have proposed strategies for blockchain-based trust management, there are still huge gap between theory and practical applications .The future research directions are listed below and classified into four modules according to the different trust research branches as Trust Robustness, Trust aided decision, Trust framework, Trust evaluation.

References

1. 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

2. 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

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

4. 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

5. Xiong L, Ling L (2004) PeerTrust: supporting reputation-based Trust for Peerto-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

6. 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

7. 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