Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

Blockchain-Based Trust Management Systems in Cloud Computing

Manoj Prajapati,
M.Tech. Scholar,
Department of Computer Science & Engineering,JBIT,
Dehradun

Dr. Vishant Kumar,
Guide,
Department of Computer Science & Engineering,
JBIT, Dehradun

Abstract:
Through Virtualization and Resource Integration, Cloud Computing Has Enlarged Its Spot and Offers a Far Better User Expertise than the Standard Platforms, Beside Its Business Operation Model Transportation Vast Economic and Social Benefits. However, An Oversized Quantity of Proof Shows That Cloud Computing Is Facing with Serious Security and Trust Crisis, And Building Trust-Enabled Dealings Setting Has Become Its Key Factor. The Traditional Cloud Trust Model Sometimes Adopts a Centralized Architecture That Causes Large Management Overhead, Network Congestion and Even Single Point of Failure. Furthermore, Thanks To an Absence of Transparency and Traceability, Trust Analysis Results Can't Be Totally Recognized by All Participants. Blockchain May Be a New and Promising Redistributed Framework and Distributed Computing Paradigm. Its Unique Options in In Operation Rules and Traceability of Records Make Sure the Integrity, Undesirability and Security of The Dealings Data. Therefore, Blockchain Is Incredibly Appropriate for Constructing Distributed and Decentralized Trust Architecture. This Paper Carries Out a Comprehensive Survey on Blockchain Based Trust Approaches in Cloud Computing Systems. Supported A Unique Cloud Edge Trust Management Framework and A Double-Blockchain Structure Primarily Based Cloud Transaction Model, It Identifies the Open Challenges and Provides Directions for Future Analysis During This Field.

***Keywords*: Decentralized Trust Management, Blockchain Technology, Cloud Computing, Distributed Ledger.**

1.0 INTRODUCTION:

Cloud Computing Has Become One of the Newest Research Problems in Recent Years, and Its Massive Business Fee Is Steadily Emerging [1, 2]. With the Virtually unlimited Extension of Useful Resource Sharing and A Better Customer Experience, Cloud Computing Has Become One of The Newest Research Problems in Developing Countries, and Its Massive Business Fee Is Steadily Emerging [1, 2]. Cloud Computing Structures, on the other hand, have encountered numerous consensus and security issues. For example, in 2016, Cloud Flare, a well-known cloud security service provider, discovered that a significant malicious programme in its software had resulted in private information leakage, affecting at least 2 million websites, including services from many well-known internet companies such as Uber and 1password. Microsoft Azure Public Cloud Garage Mistakes Affected Associated Cloud Commercial Enterprise for the 8th Time in March 2017. In June 2017, Amazon suffered a security breach On the inside of the Publicity of Private Records of 200 Million US Voters Resulted through Web Services. According to a survey conducted by Fujitsu, as much as 88 percent of cloud clients are concerned about data security issues and need to know what is going on at the physical servers.

1.1 In General, There Are Three Major Trust Risks in Cloud Computing Platform- ▪ Loss of Control: When users submit their data, code, and running processes to remote cloud servers, they lose control of them.
▪ Lack Of Transparency: Cloud Computing Is Like A Black Box To Its Users Because They Don't Understand The Internal Operation Mechanisms, Raising Their Concerns About Privacy Manipulation. Although most cloud service providers declare their Service Kind Agreements (Slas), attempting to offer a few really level of commitment to service reliability, security, and confidentiality, the specifications on Service level agreement are always vague and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

abstract. Many students have started to agree with the recommendations of related research. Li et al., for example, included a singular agreement with method that allowed them to assess and predict users' cognitive behaviour [3]. Approve with Models Mixed with Evolutionary Algorithms Were Added In [4, 5], But So were Some Of The Most Valuable Techniques To Improve Provider Control Performance [6–10]. However, the traditional agreement version is usually based on a prores agreement control centre, which can result in delays, congestion, or even a sense of powerlessness. Secondly, In A although proof of cooperation isn't always available to the public, the outcomes of agreement evaluations aren't completely reliant on all participants. Blockchain Generation Has Attracted Significant Attention As A Rising Decentralized Framework And An Allotted Computing Paradigm, And Its Utility Has Proven A Blowout Improvement With The Recognition Of Virtual Cryptocurrencies. Blockchain Is Primarily Based On A Decentralized P2P Architecture, In Which All Nodes Are The Same And There Is No Managed Middle. The Blessings A rend Must Recognize What Is Taking Place At

1.2 The Bodily Servers:

• Trust Relationship Maintenance Is No Longer Reliant On A Following Center, And Destruction From Several Nodes Isn't Enough To Eliminate The System's Robustness. • The Operating Rules and Data Records are transparent, open, and traceable, and the Integrated supply Database Model and Consensus Mechanisms ensure the integrity, credibility, and security of trust evidence.

The Decentralization Property Of Blockchain Is Especially Appropriate For Creating A New Distributed And Decentralized Acceptance Model. With-Enabled Cloud Buying And Selling Environments, Blockchain Provides A New Way To Acquire Accept As True. To date, a number of blockchain-based accept as true with control procedures have been proposed [11]. The Overwhelming Benefits Of Blockchain-Primarily Based Totally Schemes Have Been Proven In New Research. For example, the Blockchain-based Detection Set of Rules improved accuracy from 5% to 15% [12]. The Benefits of NFV (Dispensed Network Characteristic Virtualization) In MEC Environments Have Been Extended To 6 7 Instances That Used a Block chain Enhanced Approach [13]. The put off of the Blockchain-Primarily Based Totally Approach Is Only 1/5 That Of Conventional Strategies When Processing Large Capability Statistics Requests.

In this paper, the maximum number of consultants was set at 35. Analyzed, classified, and compared are these essential techniques. Currently, Blockchain-Primarily Based Totally Believe Control has significant challenges, such as believe dating production and maintenance, green believe assessment techniques, successfully responding to attacks, unacceptable delays in real-time transactions, and so on. This paper identifies viable destiny research directions for the benefit of destiny studies.

1.3 The Major Contributions Of This Paper Are Listed Below:

The Decentralization Characteristic Of Blockchain Is Especially Appropriate For Creating A New Distributed And Decentralized Acceptance Model. With-Enabled Cloud Buying And Selling Environments, Blockchain Provides A New Way To Acquire Accept As True. To date, a number of block chain-based accept as true with control procedures have indeed been proposed [11]. The Overwhelming Benefits Of Blockchain-Primarily Based Totally Schemes Have Been Proven In New Research. For example, the Blockchain-based Detection Set of Rules improved accuracy from 5% to 15% [12]. The Benefits Of NFV (Dispensed Network Characteristic Virtualisation) In MEC Installations Have Been Increased To 6 7 Instances Using A Block Chain Enhanced Approach [13]. The Put Off Of The Blockchain-Primarily Based Total Approach Is Only 1/5 Of That Of Conventional Approaches When Processing Large Capability Statistics Requests.

In this paper, the maximum number of consultants was set at 35. Analyzed, classified, and compared are these priceless techniques. Currently, Blockchain-Primarily Based Totally Believe Control has significant challenges, such as believe dating production and maintenance, green believe assessment techniques, successfully responding to attacks, unacceptable delays in real-time transactions, and so on. This paper identifies viable destiny research directions for the benefit of destiny studies.

1.4 Related Surveys

Some Few Surveys On Agree With Schemes In Cloud Computing Environments Have Already Been Conducted. A. Horvath III et al. [15] looked into the issues with customer agreement in cloud computing structures in order to help providers improve their behaviour. By declaring the professionals and cos of the associated researches, S.Harbajanka and P. Saxena [16] performed an overview on agree with procedures in cloud computing. Rawashdeh et al. [17] Gave An In-Depth Introduction To Modern Cloud Structures Fashions. J. Huang and D. Nicol [18] carried out a survey on prevailing satisfaction with mechanisms and highlighted their findings. Limitations. T. Nooret al. [19] Provided An Outline Of Cloud Offerings Agree With Control And Mentioned The Open Issues. M. Monir et

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

al., M. Monir et al., M. Monir [20] Provided a survey of agreeable answers in cloud computing to assess provider carriers' overall performance. [21] M. Chandni et al. Mentioned the Possibilities of Assaults on Cloud Structures, then provided an outline of the most common agreement-based total techniques. A. Sunyaev and J. Lansing [22] A Conceptual Version Was Developed To Describe Agree With In A Cloud Context, And A Survey Of Forty Three Associated Procedures Was Conducted. [23, 24] C. Matin et al. In Cloud Computing Structures, The Ultra Modern Agree With Assessment Techniques Was Examined. R. Ingle and S. Deshpande [25] In Cloud Paradigm, a taxonomy and type of agreement with fashions are provided, as well as evaluation techniques. M. Alhanahnah et al. [26] completed a survey on the taxonomy of agreement with elements and assessment strategies in order to assist cloud customers in choosing trustworthy carrier providers. Mostly because of the sharing economy's attitude, F. Hawlitschek and Others [27] The Ability To Assemble Agree With-Unfastened Systems Using Blockchain Generation was mentioned. The Concept, Evaluation, Construction, And Software Of Agree With Were Mentioned In Paper [28] In Order To Make The Most Of The Characteristic Of Agree With In Choice Making. J. Granatyr and Others [29] Conducted a research on multi-agent systems' consensus and recognition strategies (Mass).

The emergence of block chain technology, particularly its reputation in the field of e-currency, has piqued researchers' interest. Currently, we can also find a lot of block chain reviews. For example, Y. Xiao, et al. [30] specialise in the block chain's allotted consensus protocol. [31] Paper It may seem as a block chain manual, allowing customers to determine if, what type of block chain to use, and how to use it. M. Ali, et cetera. [32] I looked at the block chain packages in IoT systems. [33] Paper A comprehensive survey of aggregate studies of block chain and device learning in communique and community systems was provided. K. Gai and others [34] The Blockchain-based Totally Cloud Carrier Infrastructure was mentioned, as well as the overall performance of each software programme and hardware component. [35] M. Saad et al. A Comprehensive Discussion Of Blockchain Assaults And Current Solutions [36] Paper A survey of aggregate studies of block chain and area computing, including the concept, requirements, framework, and challenges, was conducted.

The concept of agreeing with came from sociology, and it has steadily expanded its boundaries to include control, economics, and computer science. M. Blaze Et Al. [37] Added Agree With Mechanisms To Address Internet Protection Issues for the first time in 1996. In heterogeneous, open, dispersed, and dynamically converting community environments, Trust Control provides a unique option for resolving security issues. Figure 1 shows the results of the studies. The Center Is To Observe The Idea Of Accept As True With And Its Class Primarily Based On Precise Attributes, And The Scope Of Agree With The First Department Is The Essential A Part Of Accept As True With Research, And The First Department Is To Observe The Idea Of Accept As True With And Its Class Primarily Based On Precise Attributes As shown in Fig. 1, Accept As True With Can Be Divided Into The Following Classes, Mostly Based On Exceptional Performance.

• Direct Agree With, Indirect (Recommendation) Accept As True With, and Incorporated Consider (In Step With Consider Acquisition Method).
• Identification Believe And Conduct Agree
• Function Trust And Experience Trust (According To The Timing Of The Occurrence Of Trust) • - Domain Trust

Objective Trust and Subjective Trust (According To the Representation Of Trust) □ Intra

And Inter-Domain Trust (According To Trust Relationship).

They Consider Version Is The Second Research Branch, In The Middle Of Which Is The Consider Modelling, Comparing, And Control Approach With The Goal Of Assisting Consider-Enabled Platforms Or Buying And Selling Environments. Consider Versions Can Be Divided Depending On the Consider Control Mode

You can choose between a centralised and a decentralised version. A Critical Consider Server Is Responsible For Collecting, Comparing, And Saving Consider Proof From All Parties In A Centralized Consider Version, Who Are Assumed To Be Absolutely Credible And By No Means Be Compromised. The Standard Centralized Consider Models are Taobao and E-bay [39]. However, using a centralised consider version may cause unusual latency, blocking, or even a single point of failure, lowering cloud provider Qos as a result. As a result, some researchers advocated for a decentralised consideration framework. The famous Distributed Consider Models, for example, are Eigentrust [40] and Peertrust [41].

According To the Agree With Assessment Method, Agree With Fashions May Be Divided Into The Subsequent Extraordinary Types.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

- **Network Topology-Based Model**
- **Statistical-Based Model**
- **Fuzzy Logic-Based Model**
- **Subjective Logic-Based Model**
- **Bayesian Theory-Based Model**
- **Evidence Theory-Based Model**

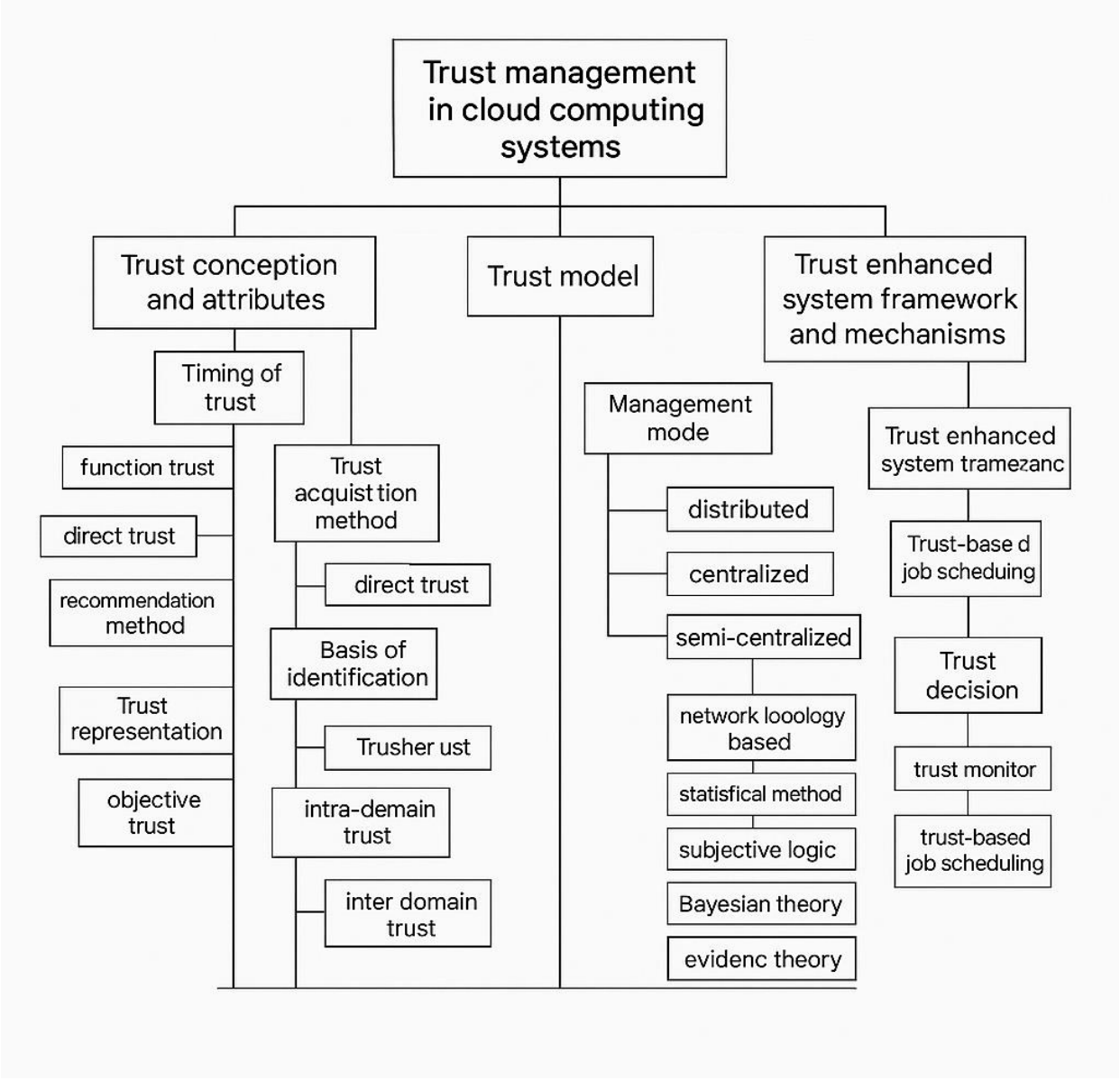

Fig: 1 Trust management in cloud computing systems

Improved Device Framework And Mechanisms Have Been Accepted By The Ultimate Studies Department. A Agree With-Enabled Gadget Safety Framework Is Implemented By Incorporating An Agree With Control Layer To The Pinnacle Of The Conventional Cloud Safety Model. For cloud interconnection and interaction, trust mechanisms provide a feasible level of security.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

2.0 RECENT RESEARCH RESULTS

Trust-Enabled Cloud Service Management Techniques Have Been Intensively Researched in Recent Years. Li Et Al., for example, designed a Cloud Provider Brokering Model based on [43] in order to improve the overall performance of provider matching. Mrabet & Co. [44] T Broker is a brand new version of the Consider Assessment that we recommend. Abdallah et cetera. [45] Trust-Cap is a completely cloud-based application protocol that was designed with consideration in mind. Singh and his associates [46] Developed a collaborative consideration calculation scheme that is mostly based on fuzzy logic. Nagarajan and his associates [47] A Comparable Consider Assessment Version was also provided. For Cloud Duplication Protection And Performance, Zahra and her friends [48] Level is a new encryption protocol that has been proposed. Zhang and colleagues [49] A Domain-based Consideration Scheme For Public Clouds was proposed.

To Protect Cloud Carriers And Clients From Capability Attacks, Yefeng and Durresi [50] Designed A Three-Stage Consider Control Framework. Fiorese and Felipe [51] For Cloud, I Developed

A Recognition Framework That Combines Both Objective And Subjective Considerations. Zhu and his associates [52] For The Cc-Wsn Integration Platform, BroughtA UniqueConsider Calculation Version Named Atrcm In order to ensure the security of Iaas cloud computing systems, Kashif and his associates [53] A New Dispensed Consideration Framework Was Designed. Keep Away from Buying and Selling with Malicious Services to Assist Customers Et cetera. [54] Recommend a Cloud Carrier Interaction Version That Is Mostly Based On Consideration And Spanning Tree. For Secure And Powerful Cloud Transactions, Wang Et Al. [55] Proposed A Consider and Desire Conscious Carrier Choosing Version Known As Cc-Psm. [56] Meng et al. Customers can use a -Layer Carrier Search Protocol to find the most trustworthy and cost-effective carrier. [57] Yan et al. A Consider-Enabled Cloud Carrier Framework was created. In order to work in a Service-Oriented Computing (Soc) environment, [58]

Hang et al. Recommend a set of carrier/useful resource selection strategies based entirely on a discarded version. In Paper [59–63], the Consider and Qos Conscious Carrier Choice or Composition Techniques were proposed.

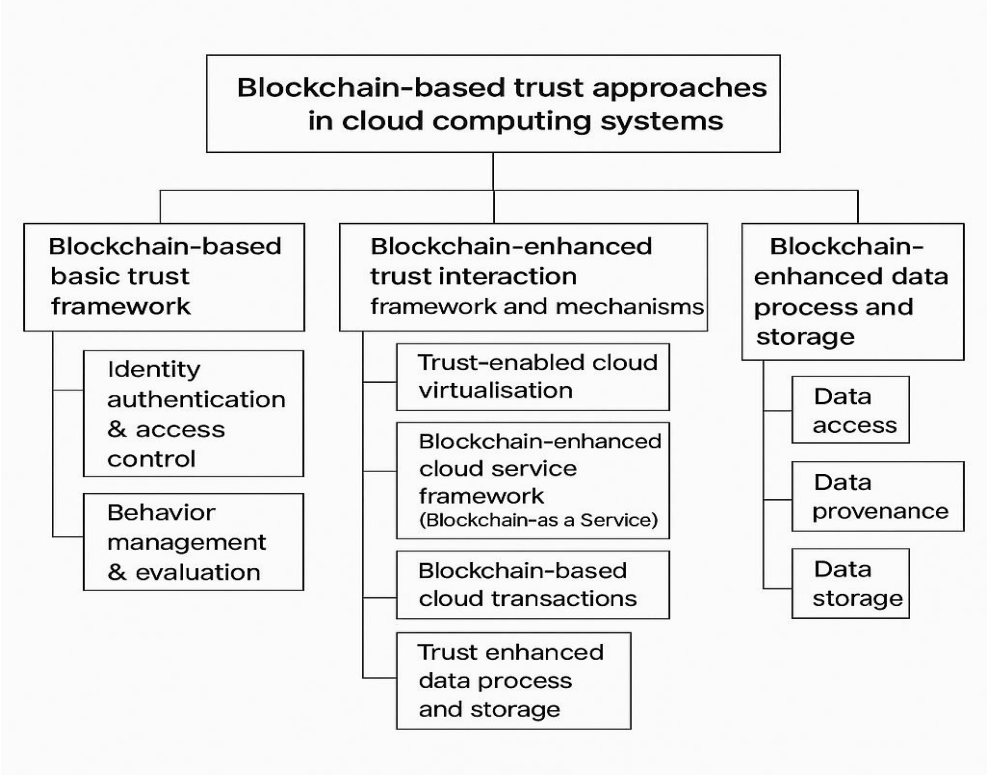

Fig. 2 Phases of block-chain-based trust approaches in cloud computing systems

2.1 Research Challenges

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 that claim to be decentralized models still need a third-party trust or certification centre, which may result in many security risks such as single point of failure, over-load and credibility loss, etc.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

- Trust evidence is not open to all participants and not traceable, so trust evaluation results are not convincing nor are they fully trusted.
- Inaccuracy of trust evaluation results. The existing trust models lack a sufficient description capability (trust data mostly in the form of numerical scoring), which is insufficient in real applications, such as ecommerce, where people's feedback often includes multiple data types such as numeric and characters.
- Less adaptive. Trust decision-making uses subjective methods, such as expert scoring and the averaging method, which makes the models subjective and lack scientific and adaptability. Trust models are not robust enough to deal with malicious attacks (collusion), especially malicious recommendations.
- Huge management overhead. It limits trust solutions in large-scale network applications. Lack prototype and platform. Performance tests of trust models are mostly achieved by some simulation experiments, needing further evaluation.

2.2 Phases, Taxonomy and Review of Blockchain- Based Trust Approaches We Present A Comprehensive Overview Of The Blockchain-Primarily Based Totally Consider Methods For Credible Interactions In Cloud Computing Environments.
Our Basis For Document Classification Is The Simple Research Taxonomy Of Considering And The Blockchain Techniques In The One-Of-A-Kind Fields Of Consider-Primarily Based Totally Cloud Computing Applications. Thus, The Associated Answers Are Categorized Into Three Types: Framework, Blockchain-Better Consider The Interaction Framework And Mechanisms, And Blockchain-Better Cloud Facts Management, As Illustrated In Fig.2.

2.2.1 The Basic Trust Framework Contains Two Sub Research Modules:
Orthodox theology frameworks often follow a systematic and disciplined approach, with the middle node bearing a significant amount of compute and processing overhead, which may easily lead to errors such as single point failure and deliberate fraud, and cannot adapt to a real-time software environment. And they feel assessments aren't entirely noticed since they consider as true that the proof is best viewed in the middle. The block chain's herbal decentralisation feature may decentralise the process of belief authentication, addressing the aforementioned problems caused by centralization. Controlling access and verifying identities Identity management is a key component of cloud computing that is built on trust. Individuals in cloud marketplaces, such as service providers and customers, are protected by identity authentication, are authenticated legitimate nodes.
The traditional identification control technique usually necessitates the use of such a third birthday celebration control middle, which can introduce security problems such as the certification middle's excessive authority and a single point of failure. Identification federation is another option for overcoming security and accepting difficulties across several domains in large distributed systems, but it will raise the complexity of device structure and operation. N. Alexopoulos et al. [64] looked at the possibility of using open distributed ledgers, such as block chain generation, to boost authentication for trust management (tm) systems. They presented a summary authentication version and investigated how it works using the block chain architecture and graph theory. Identity Authentication & Access Control,
[1] Behaviour Management & Evaluation.
The Blockchain enhanced Trust Interaction Framework and Mechanisms Include Four

2.2.1.1 Sub Research Modules:
- ❖ Blockchain enhanced Cloud Service Framework (Blockchain-As-A-Service),
- ❖ Blockchain-Based Cloud Transactions,
- ❖ Blockchain-Enhanced Resource Allocation And Task Offloading,
- ❖ Trust-Enabled Cloud Virtualization.

2.2.1.2The Blockchain-Enhanced Data Management Mainly Has Three Sub Research Areas:
- ❖ Data Access Model,
- ❖ Data Provenance,
- ❖ Data Storage.

In a encrypted block-chain architecture, five prevalent attacks could be successfully alleviated. K. Bendi ab et al. [65] proposed a unique identification control version based entirely on block chain technology for the powerful to agree on cloud computing system governance. In a distributed, decentralised, and dynamic way, the suggested version enabled carrier firms to successfully regulate their agreed-upon behaviours and connections with customers or other vendors. The middle approach is a credible inter-area agreement with block chain network control. The version

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

includes the definition and computation method for three key parts of agreement, namely, individual credibility, authentication, and satisfaction. Figure 3 depicts the proposed block chain-based complete identity authentication system's structure.

2.2.1.3 The following are the paper's contributions:

❖ It Analyzed and Explained the Limitation of Identity Federation In Trust Management.

❖ It Introduced the Implementation Mechanism of Blockchain In Building Identity Management And Designed A Cross-Domain Authentication Procedure, Taking Into Account The Dual Role Of CSP (As Service Provider And Recommender).

2.2.1.4 The Paper's Major Contributions Include:

❖ It Pointed Out the Limitations of Current Work In Balancing Data-Related Mechanisms, Including The Protection Of Data Security And Privacy, Node Authentication And Trust Management.

❖ It Proposed to Use a Blockchain-Based Data Structure to Store Distributed Authentication and Trust Information, And It Introduced a humanlike Knowledgebase Trust Model.

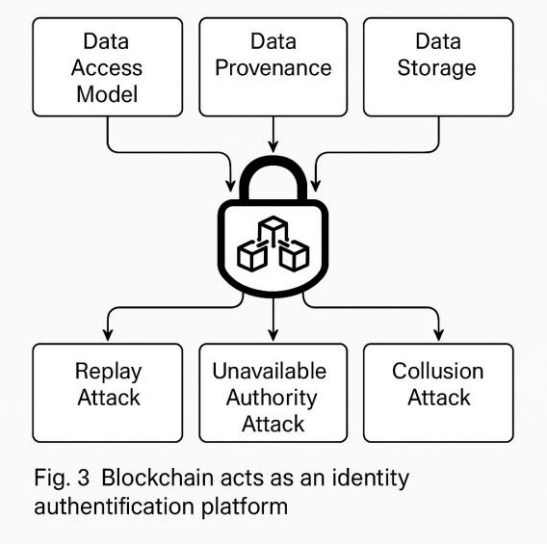

Fig. 3 Blockchain acts as an identity authentication platform

3.0 BEHAVIOUR MANAGEMENT AND EVALUATION:

A further important thing to consider when assessing and predicting the credibility of entities' actions is their demeanour. [68] S. Nayak et al. Clever Contracts Were Used to Recommend Saranyu, A Proposed Version For Green Useful Resource Control In Cloud Computing Systems. Saranyu has evolved to provide four different types of services, including identification control, authentication, authorization, and charging. Public-Non-Public Key Pairs have been used to deal with the first offerings. A Clever Contract Is Used To Carry Out Authorization. Charging Is Discovered Through Fee Gateways Based On Carrier Or Useful Resource Usage. Saranyu will be described as a moderately distributed application that uses the Web3 java script library.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

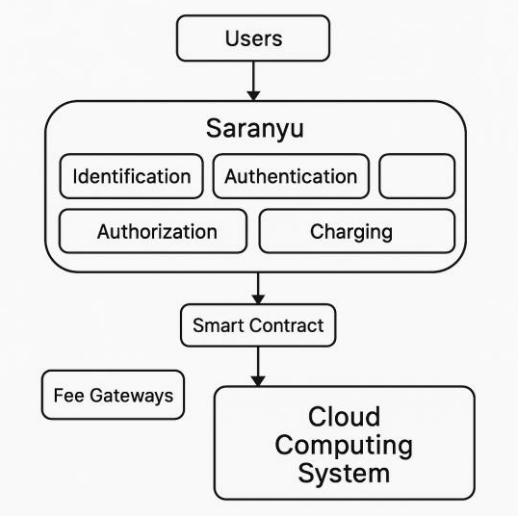

Fig. 4 Architecture of Saranyu

3.1 The Paper Makes the Following Contributions:

It used the smart contracts to realize a variety of services, including service management and Tenant management, which could ensure the fairness of transactions to a certain degree. It was a novel block chain-based distributed app that combined open source quorum and smart contracts. the limitation of the work is that it can only be implemented in a licensed distributed ledger, in which only entities with legal credentials are allowed to participate. Also, the app had still been under development without a performance test in a large-scaled Application environment.

The focus of the paper was to analyze and implement data credibility. And the main processes include: data reliability assessment, information source rating (1 or $^{-1}$), miner selection (capability proof), blocks generation and verification, distributed consensus, and reputation calculation. The service level agreements (slas) sometimes are not credible and automatically executed as required. to this end, h. zhou, et al. [70] added a new role "witness "to the traditional SLA service model to detect service violations and thus ensure the credibility. The Nash equilibrium theory of game theory was also used to help cloud providers and users negotiate and reduce the gas consumption. in the proposed model, witnesses were the ordinary nodes in block chain network, who gained profits by supervising cloud transactions. They helped the transactions proceed as agreed and forced all the parties to ful fill their money obligations. The system contained two types of smart contracts, including the witness pool contract and the SLA contract. During the transactions, customers and providers first negotiated the implementation details of SLA (including service duration, service Fees, service compensation and witnesses to be co employed, etc.), and then randomly selected a certain number of witnesses through the execution of the witness pool smart contract. the details of the service interaction are shown in fig. 5. this is one of the earliest documents that convert the problem of trust management into economics. however, it just used the theoretical methods for demonstration, which is difficult to prove its efficiency in the real transactions. in response to the severe security issues faced by traditional centralized cloud computing architectures, p. fernando, et al. [71] proposed a hybrid cloud service architecture based on block chain and SDN.

Proposed architecture contained a block chain security management layer and a multi controller SDN network layer.

3.2 The Main Contributions of This Paper Are as Follows.

❖ It Proposed A Novel Cloud Computing Service Architecture Based On An Add-In Blockchain Security And Autonomous Management Layer.

❖ It Designed a Blockchain-Based Bandwidth Provision Protocol To Strengthen End-To-End Connectivity, And The Performance Of The New Model Was Verified By Bandwidth Occupancy Rate, Resource Availability, And Packet Loss Rate.

The Main Contribution of The Work Is That It Introduced Blockchain Technology into Cloud Manufacturing to Realize the Decentralized Interaction Without a Third-Party Trust Entity. However, In the Proposed Scheme, the Private Data Might Be Exposed in the Internet Environments, It Could Not Correct the Wrong Operations, and All

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

Operations, Even the Write Operation, Need Payment. L. Xie Et Al. [12] Proposed a Semi-Decentralized Trust Model Based on Blockchain Technology For The Vehicular Iot Environment In SDN-Enabled 5GVanets. The Proposed Scheme Also Used a Joint Proof-Of-Work and Proof-Of-Stake Mechanism To Elect Suitable Miners And Eliminate Malicious Traffic Broadcasting. Based On A Centralized Controlled Authentication Mechanism And A Decentralized Trust Management Framework, It Set Up A Semi-Centralized Trust Model For Road Condition Management.

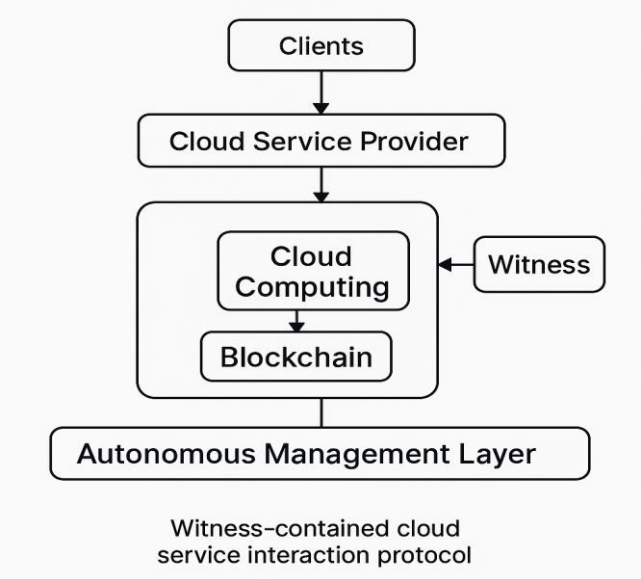

Fig. 5 Witness-contained cloud service interaction protocol

4.0 CONCLUSION

This study gives an overview of block chain-based trust management approaches in cloud computing systems and therefore taxonomy. Three phases are used to characterise these approaches into different taxonomies: Data Management, Blockchain Enhanced Trust Interaction Framework and Mechanisms, and Blockchain-Based Basic Trust Framework The report then goes on to present a thorough examination and comparison of existing block chain-based trust approaches. A Novel Cloud

Edge Hybrid Trust Management Framework, as well as a Double-Blockchain Based Cloud Transaction Model, are proposed to improve the efficiency and adaptability of trust-enabled cloud computing. Finally, we discuss future directions and open challenges associated with block chain-based trust management schemes. This paper is unique in that it examines the use of block chain from the standpoint of trust.

Our Analysis Shows That Using Blockchain Technology to Construct a Decentralized Trust Management Framework Has the Following Benefits:

It eliminates a single point of failure and eliminates data leakage, Identity and trust behaviour evidence is traceable and interpretable, trust evaluation results are convincing and malicious data use is avoided, and It's especially well-suited to building IoT trust relationships.

REFERENCES

1. Abdallah, E., Zulkernine, M., Gu, Y., et al. (2017). TrustCap: A trust model for cloud-based applications. In Proceedings of IEEE Computer Software & Applications Conference, IEEE.

2. Alexopoulos, N., Daubert, J., Muhlhauser, M., & Habib, S. (2017). Beyond the hype on using blockchains in trust management for authentication. Proceedings of IEEE TrustCom/BigDataSE/ICESS, IEEE.

3. 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 Communications Surveys & Tutorials, 21(2), 1676–1717.

4. 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.

5. Almutairi, A., Sarfraz, M., Basalamah, S., Aref, W., & Ghafoor, A. (2012). A distributed access control architecture for cloud

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

computing. IEEE Software, 29(2), 36–44.

6. Belotti, M., Bozic, N., Pujolle, G., et al. (2019). A vademecum on blockchain technologies: When, which and how. IEEE Communications Surveys & Tutorials, 21(4), 3796–3838. https://doi.org/10.1109/Comst.2019.2928178

7. Bendiab, K., Kolokotronis, N., Shiaeles, S., et al. (2018). WIP: A novel blockchain-based trust model for cloud identity management. Proceedings of 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, IEEE, 724–729.

8. Bhushan, B., & Sahoo, G. (2015). Trust management based security model for cloud environment. International Journal of Computer Applications, 119(14), 24–30.

9. Cao, B., Li, B., & Liu, J. (2013). An on-demand service composition method based on trustworthy quality of service. Journal of Xi'an Jiaotong University, 2, 131–138.

10. Chandni, M., Sowmiya, N., Mohana, S., et al. (2017). Establishing trust despite attacks in cloud computing: A survey. Proceedings of WISPNet 2017, IEEE, 712–716.

11. Chang, H., & Hussain, F. (2020). Trust cloud: A cloud-based framework for trust management in social Internet of Things. IEEE Internet of Things Journal, 7(7), 5833–5842.

12. Chen, C., & Ye, Y. (2018). A blockchain-based trusted data management scheme in edge computing. Journal of Communications and Networks, 20(5), 502–508.

13. Cho, J., Chan, K., & Adali, S. (2015). A survey on trust modeling. ACM Computing Surveys, 48(2), 1–40.

14. Cole, J., Milosevic, Z., & Raymond, K. (2011). Decentralized trust management. In H.C.A. van Tilborg & S. Jajodia (Eds.), Encyclopedia of Cryptography and Security. Springer.

15. Deshpande, S., & Ingle, R. (2017). Trust assessment in cloud environment: Taxonomy and analysis. Proceedings of International Conference on Computing, IEEE, 627–631.

16. Du, R., Tian, J., & Zhang, H. (2013). Cloud service selection model based on trust and personality preferences. Journal of Xi'an Jiaotong University, 1, 53–61.

17. Fernando, P., & Wei, J. (2020). Blockchain-powered software-defined network enabled networking infrastructure for cloud management. IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). doi:arXiv:1909.01851

18. Fu, X., Yu, F. R., 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 Workshops, Paris, France, 1–6.

19. Gai, K., Guo, I., Zhu, L., & Yu, S. (2019). Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/Comst.2020.2989392

20. 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 Transactions on Internet Technology, 21(1), 1–23. https://doi.org/10.1145/3391198

21. Granatyr, J., Botelho, V., Lessing, O., et al. (2015). Trust and reputation models for multiagent systems. ACM Computing Surveys, 48(2), 1–42.

22. Gupta, A., & Sandhu, S. (2015). Review of trust models in cloud computing. International Journal of Computer Applications, 121(23), 22–25.

23. Habib, S., Ries, S., & Muhlhauser, M. (2011). Towards a trust management system for cloud computing. Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 933–939.

24. Hang, C., & Singh, M. (2011). Trustworthy service selection and composition. ACM Transactions on Autonomous and Adaptive Systems, 6, 1.

25. 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, 1–3.

26. Horvath, A. III., & Agrawal, R. (2015). Trust in cloud computing: A user's perspective. Proceedings of the IEEE SoutheastCon 2015, IEEE, 1–8.

27. Huang, J., Xu, H., Li, D., & Deng, S. (2014). Trust evaluation mechanism for service selection in mobile cloud computing. IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 637–644.

28. Hussain, M., & Abdullah, A. (2012). Taxonomy of trust models for mobile ad hoc networks. Journal of Network and Computer Applications, 35(3), 1231–1241.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

29. Jiang, Q., Ma, J., Wei, F., et al. (2018). An efficient authentication and key agreement scheme with user privacy preservation for cloud computing. Future Generation Computer Systems, 88, 660–669.

30. Josang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2), 618–644.

31. Khan, A., Zhang, L., & Teng, L. (2017). A security framework for cloud data storage and computation. Procedia Computer Science, 122, 1047–1054.

32. Ko, R., Jagadpramana, P., Mowbray, M., et al. (2011). TrustCloud: A framework for accountability and trust in cloud computing. 2011 IEEE World Congress on Services, 584–588.

33. Li, H., Dai, Y., Tian, L., & Yang, H. (2009). Identity-based authentication for cloud computing. CloudCom 2009, LNCS, 5931, Springer, 157–166.

34. Liang, X., Shetty, S., Tosh, D., et al. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. IEEE/ACM Symposium on Cluster, Cloud and Grid Computing (CCGRID), IEEE, 468–477.

35. Lin, H., & Zhu, L. (2018). Blockchain-based secure sharing of healthcare data in cloud computing. Journal of Medical Systems, 42(8), 1–9.

36. Liu, Y., & Dong, M. (2020). Secure and privacy-preserving data sharing in cloud computing. IEEE Transactions on Services Computing, 13(2), 284–297.

37. Liu, Z., Xiang, Y., Wang, L., & Zhou, W. (2014). A trust management model for cloud computing. Proceedings of the 12th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 244–251.

38. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. V. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38–54.

39. Moniruzzaman, M., & Hossain, S. A. (2013). Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications, 6(1), 25–36.

40. Mousannif, H., Khalil, I., & Kotsis, G. (2013). Trust management in cloud computing: A survey. International Journal of Cloud Applications and Computing, 3(2), 1–18.

41. Mukherjee, M., Shu, L., & Wang, D. (2017). Survey of fog computing: Fundamental, network applications, and research challenges. IEEE Communications Surveys & Tutorials, 20(1), 46–70.

42. Nkenyereye, L., Kang, S., & Kim, H. (2019). Blockchain-based trust model for cloud service selection. IEEE Access, 7, 113871–113888.

43. Noor, T. H., & Sheng, Q. Z. (2011). Trust as a Service: A framework for trust management in cloud environments. Proceedings of the 12th IEEE International Conference on Mobile Data Management, IEEE, 121–130.

44. Noor, T. H., Sheng, Q. Z., Yao, L., & Dustdar, S. (2013). CloudArmor: Supporting reputation-based trust management for cloud services. IEEE Transactions on Parallel and Distributed Systems, 27(2), 367–380.

45. Patel, P., & Borisaniya, B. (2015). Trust based security model for cloud computing. International Journal of Computer Applications, 116(19), 16–20.

46. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69–73.

47. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. EUROCRYPT 2005, LNCS 3494, Springer, 457–473.

48. Salman, T., & Jain, R. (2019). A survey of blockchain-based distributed trust models. Computer Communications, 146, 1–17.

49. Saloni, G., & Singh, P. (2020). Trust evaluation model for cloud computing using fuzzy logic. Procedia Computer Science, 167, 958–967.

50. Sharma, P., & Sood, S. K. (2011). Trust evaluation mechanism in cloud computing: A systematic review. International Journal of Computer Applications, 36(8), 15–21.

51. Shen, H., & Wang, G. (2011). A fault-tolerant and secure reputation system for mobile ad hoc networks. IEEE Transactions on Parallel and Distributed Systems, 22(8), 1221–1234.

52. Shi, Y., & Chen, M. (2010). A trust-based service management approach in mobile cloud computing. Proceedings of the IEEE Asia-Pacific Services Computing Conference, IEEE, 120–127.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 04, April-2025

53. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88–115.

54. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269–284.

55. Sookhak, M., Gani, A., Talebian, H., et al. (2017). Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues. ACM Computing Surveys, 47(4), 1–34.

56. Subramanian, G., & Kanniga Devi, A. (2016). A comprehensive trust model for cloud computing. International Journal of Computer Applications, 145(1), 27–32.

57. Sun, D., Chang, G., Sun, L., & Wang, X. (2010). Surveying and analyzing security, privacy, and trust issues in cloud computing environments. Procedia Engineering, 15, 2852–2856.

58. Sultana, S., Ghinita, G., & Madria, S. (2019). A secure and trustworthy framework for data sharing in cloud computing. Future Generation Computer Systems, 94, 453–468.

59. Syalim, A., Nishide, T., & Sakurai, K. (2011). Realizing secure and practical access control in cloud computing. Proceedings of the 2011 IEEE 3rd International Conference on Cloud Computing Technology and Science, IEEE, 455–462.

60. Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24–31.

61. Tehrani, S. R., & Manasrah, A. (2018). A comprehensive survey on trust management in cloud computing. Procedia Computer Science, 130, 312–319.

62. Tian, Y., & Huang, C. (2018). A trust-based and privacy-preserving customer selection mechanism for cloud service. IEEE Access, 6, 45665–45677.

63. Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. IEEE INFOCOM 2010, IEEE, 1–9.

64. Wang, Y., Vassileva, J., & Zheng, Y. (2007). Trust-based service selection in virtual communities. Web Intelligence and Agent Systems: An International Journal, 5(1), 59–70.

65. Wei, J., Zhang, X., Ammar, M., & Zegura, E. (2009). Cloud computing security: A survey. IEEE Communications Surveys & Tutorials, 13(4), 746–767.

66. Wu, H., & Zhou, J. (2012). Trust and reputation evaluation for cloud service providers. Journal of Computer and System Sciences, 78(5), 1475–1490.

67. Wu, H., Ding, Y., & Zhang, H. (2013). Towards cloud service selection: A trust-based approach. Proceedings of the IEEE International Conference on Cloud Computing Technology and Science, IEEE, 284–291.

68. Xu, Z., & Zhang, X. (2014). Trust evaluation in cloud computing. Future Generation Computer Systems, 28(4), 622–631.

69. Yang, J., & Li, Z. (2016). Design and implementation of a blockchain-based data integrity protection mechanism for cloud storage. Proceedings of the International Conference on Cloud Computing and Big Data, IEEE, 299–303.