Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.4, August : 2024

CLOUD BASED ON DATA INTEGRITY SUBSTANTIATION USING BLOCK CHAIN TECHNOLOGY

Dr.N.C. Sachithanantham, Mr.D.Rajkumar, Assistant Professor, Department of Information Technology, Dr.SNS Rajalakhsmi College of Arts and Science (Autonomous), Coimbatore - 641049, Tamilnadu, India
Dr.K.Sasirekha, **Dr.P.Sedhupathy**, Assistant Professor, Department of Computer Science with Artificial Intelligence and Data Science, Dr.SNS Rajalakhsmi College of Arts and Science (Autonomous), Coimbatore - 641049, Tamilnadu, India

Abstract **--** Cloud computing has gain fabulous recognition in current years. By outsourcing working out and storage requirements to public providers and paying for the services used, customers can delight in upon the recompense of the new paradigm. Cloud computing provide with a comparably lower-cost, scalable, a location-independent platform for supervision clients data. Compared to a conventional model of computing, which uses devoted in-house infrastructure, cloud computing provides unique reimbursement about cost and reliability. Cloud storage is a latest cost-effective model that aims at providing high availability, reliability, massive scalability and data sharing. The cloud storage service provides the storage and access utility for massive data, reducing the management cost for huge amounts of data. The data integrity authentication scheme in cloud storage can be occupied to help users confirm the integrity of outsourced data. This paper is consistent exploration of existing system for the guaranteeing the information fidelity in cloud and another strategy is proposed. This paper is consistent analysis of obtainable mechanism for the ensuring the data integrity in cloud. In this paper, to proposed a lattice signature algorithm to refuse to recognize quantum computing and introduce cuckoo filter to construct simpler the computational overhead of the user verification phase.

Keylkwords—Cloud; Data Integrity; Computing; Reliability; Sacalable; Lattice;

I. INTRODUCTION

With the rapid expansion of network and communication technology, cloud computing has been broadly functional in recent years. Cloud storage is a service provided by cloud computing, which allows users to way in the network and use storage resources. The cloud storage service provides the storage and access function for immense data, falling the supervision cost of users for huge amounts of data. Cloud storage services greatly reduce the burden of cloud users, but also bring some security risks to cloud data. On the one hand, compared with conventional storage methods, data stored in the cloud may be vanished or spoiled due to the spoil of attackers or hardware and software failures, such as the outsourced data integrity damage event of Tencent Cloud in 2018.

Data Integrity is the fundamental key component in acquiring the in sequence Security. The Data Integrity is simply termed as no corruption in the data that can be sure with regularity and precision over the time. Every technique of data integrity ensure the no loss in flood of data. Cloud Computing is the most recent and current trending visualize design of IT Enterprise. It increases the capacity and adds capabilities to the purpose what industries are in required.

II.CHALLENGES FOUND ON CLOUD

Though having many advantages it also having a lot of concerns in the cloud. The issues were stated below:

Accessibility: Information should be accessible for clients all over the time. There shouldn’t be any issues that would direct to data storage trouble and leads to the collapse/loss of user data.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.4, August : 2024

Network Load: The over load ability may effect in not make the grade of data integrity. There will be problem in move of Information between systems and servers

Integrity (No Corruption): Reliability and correctness of the information is endangered with the loops having in the cloud techniques

Data Location: Some of the storages follow will be like Centralized storage process. If it fails, there will be no option of rescue of data

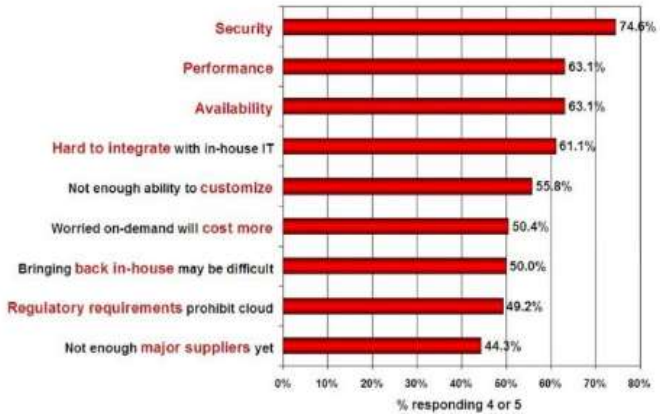


Fig. 1. Challenges Found on Cloud

. Cloud storage is valuable for both users and service providers. Cloud users acquire minimum capital investment and are reassured from infrastructure preservation responsibility. By utilizing cloud storage, a user is provided location-independent right to use to services. Meanwhile, a CSP gains high profits over obtainable infrastructure by sharing it along with multiple users. This high level of resource exploitation leads to optimized energy consumption.

III.DATA INTEGRITY SCHEMES

Data Integrity schemes for impulsive data are out of the extent of this survey. There are three entities in a data integrity scheme: (i) Data proprietor who outsources his data, (ii) a cloud storage provider (CSP) to whom data are outsourced and (iii) an auditor who verifies the reliability of the data.

Data integrity refers to the reality that data have not been tampered with or smashed without endorsement, to ensure that the data subsist in an entire and true manner according to the wishes of the data owner. It introduces data mining technology to extract latent information levels to meet different needs and different levels of learners. The requirements also supply users with decision-making support and decrease the possibility of risk incidence and accounting informatization to assist corporate managers support in management. Research on cloud data integrity verification algorithm is under the circumstances of accounting informatization.

IV. GENERAL TECHNIQUES USED TO MAINTAIN DATA INTEGRITY

A. Generating Hashes

Comparing the hash values can check/verify the uniformity ofdata. Ahashvalue also known as message digest. The hash valueis calculated based on the chosen mathematical function. The input will be the length of the string that as to be transmitted. Some techniques like sha and md5 are used to generate hashes and verify integrity. This was the basic and common methodology to ensure the client's data integrity

B. *Using Trusted Third parties(TTP)*

Trusted Third Parties (TTP) like are the supporting vendors that take care of our data transmissions. We can fully rely on them. The existing were more secure but if we go with new TTP it may have some risks. It is secure and more expensive. Some of TTPs are VISA, Bradstreet,Banks etc

V. CLOUD DATA INTEGRITY VERIFICATION BASED ON DATA MINING AND ACCOUNTING INFORMATIZATION

A. Data Mining Technology: Data mining frequently refers to the detection of inbuilt laws and expensive information from enormous, outwardly unequal, and unmethodical data, and is commonly combined with statistical software or modern computer technology. The application of data mining is wider and wider, and the latent level of information to be mined is deeper. It meets the necessities of learners with different needs and different levels. It also provides users with decision-making support and reduces the possibility of threat**.**

The process of data mining usually needs to go through the four stages of obtaining data, preparing data, mining data, and expressing and explaining mining results, as shown in Figure 2:

B. Accounting Informatization. The meaning of accounting informatization can be viewed from two perspectives. Generally speaking, accounting informatization refers to all tasks connecting accounting informatization. From the choice and customization of accounting information systems, what software to use and how to use them, to managers views on accounting informatization and the enduring education and guidance of relevant accounting personnel, all belong to the scope of accounting informatization**.**

V. TECHNIQUES IN CLOUD TO ENSURE INTEGRITY

There are few techniques that are better and more secure with some drawbacks/limitation so far that could maintain the Stability of information in the online storage. The fundamental procedure for information consistency in cloud are Proof of Retrievability (POR) and Provable Data Ownership Possession (PDP) that are most normally used for ensuring data dependability.

A. Provable data possession (PDP)

It assures no occurrence of corruption of data even the data stored in unfaithful storage. It is done with the remote server. The principle behind PDP involves in 2 stages:

1. Setup Stage
2. Challenge Stage

B. PDP based on MAC

The information proprietor registers a Message Authentication Code (MAC) of the entire record with an arrangement of mystery keys and stores them locally before outsourcing it to CSP.

C. Scalable PDP

The primary contrast is Scalable PDP utilizes while unique PDP utilizes open key to lessen calculation over-head. Adaptable PDP can have active operation on distant information

D. Proof of retrievability (POR)

POR is strategy without keeping a duplicate of the client's unique records in nearby capacity.

E. High Availability and Integrity Layer (HAIL)

HAIL enables the client’s Information on various servers so there is a repetition of the information.

VI. DATA TIME CONSUMING: PROGRAM FLOW ANALYSIS

A. Data Program Flow Design Analysis.

The main functions of the system consist of users moving files to the cloud for online hosting, checking the integrity of files in the cloud when users acquire them, and performing online operation on files in the cloud.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.4, August : 2024

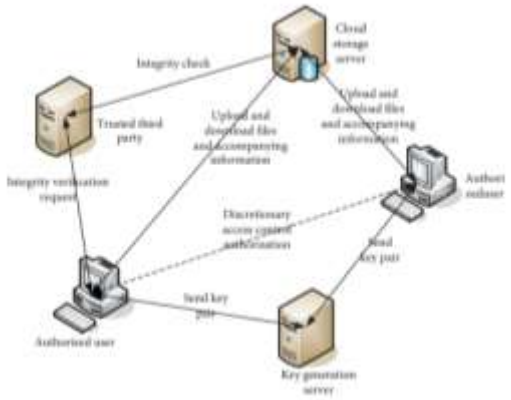


Fig. 2. Secure Cloud Storage Model

B. Time-Consuming Analysis of File Data Insertion Operation

Test the time devoted by erratically inserting file blocks at any position in the file for authentication.

VII. RESEARCH AIM AND OBJECTIVES

The purpose of the study is to identify the use of blockchain technology in the field of cloud computing and to identify the possible threats and challenges in the application of blockchain technology when useful in the area of cloud computing. The following objectives are stated below:

- To identify the scope of blockchain technology and its application on the area of cloud computing.
- To identify the security significance of blockchain technology on its application to cloud computing.
- To analyse the latest solution in the context of security aspects by maintaining privacy, integrity and authentication of public information.

A. Blockchain Technology:

Blockchain technology is a sort of dispersed architecture that makes use of cryptographic signed transactions. It operates in block-wise manner. Each block is linked with cryptographic systems. Authenticity of the transactions should validate and evaluated at each single point of failure. It employs several features of the Peer to Peer (P2P) .Most of the nodes in blockchain networks owned by dissimilar organizations. It is a kind of network environments where transaction data and the parameters are close to business logic. Asymmetric Key Cryptography is broadly used for blockchain transactions.

Fig.3. Generic blockchain model

B.Authentication- Insight on cloud computing:

An incentive and attractive computing services delivered by the cloud computing via resource pooling and Techniques. Security as a service is a new unease in cloud computing paradigms.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.4, August : 2024

C. Integration of Blockchain in cloud computing and its security:

Cloud computing composes large networks of virtualized services, namely, hardware resources and the software resources. Any sort of services belong to data centres and known as data farms.

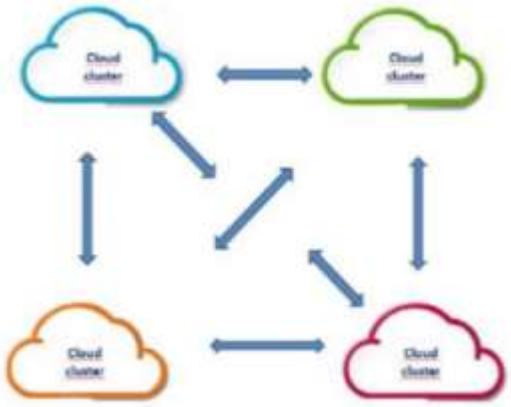


Fig.4. P2P Based Cloud Architecture

D. Lattice Signature-Based Work:

In recent years, lattice cryptographic schemes have been really developed in cryptography theory and achieved a series of research results. One of the major public problems of lattice signature schemes is to decrease the size of the verification key while implementing short signatures lattice signature scheme that can verify secure under the standard model with only O (log n) matrices for verification keys but also achieved existential enforceability beside chosen message attacks, that is, a completely secure lattice signature scheme, but the security of the scheme is imperfect by the number of message queries.

The mainly divided into three parts: the background associated to the lattice signature algorithm, the background of blockchain, and the background of the cuckoo filter. To eliminate the situation that the distribution of the signature results associated to the user's private key distribution and also need to use rejection sampling theorem**.**

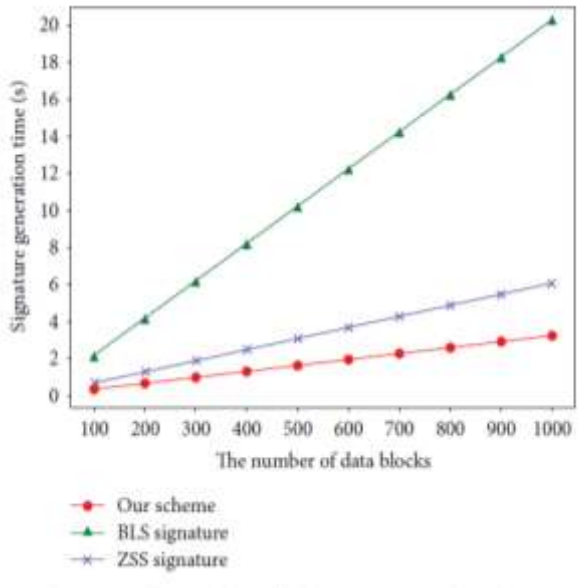


Fig.5. Comparison of signature generation time

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.4, August : 2024

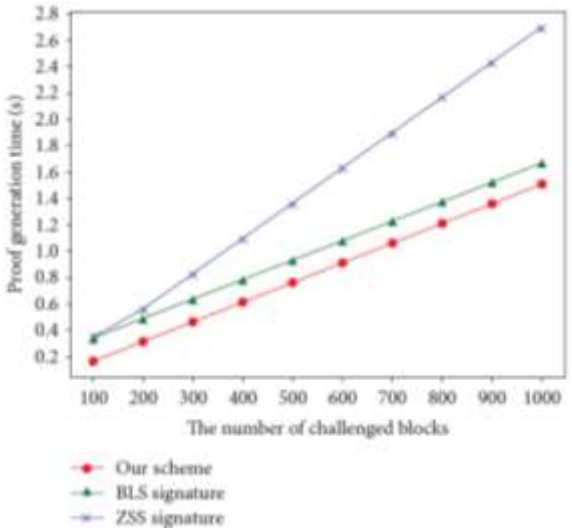
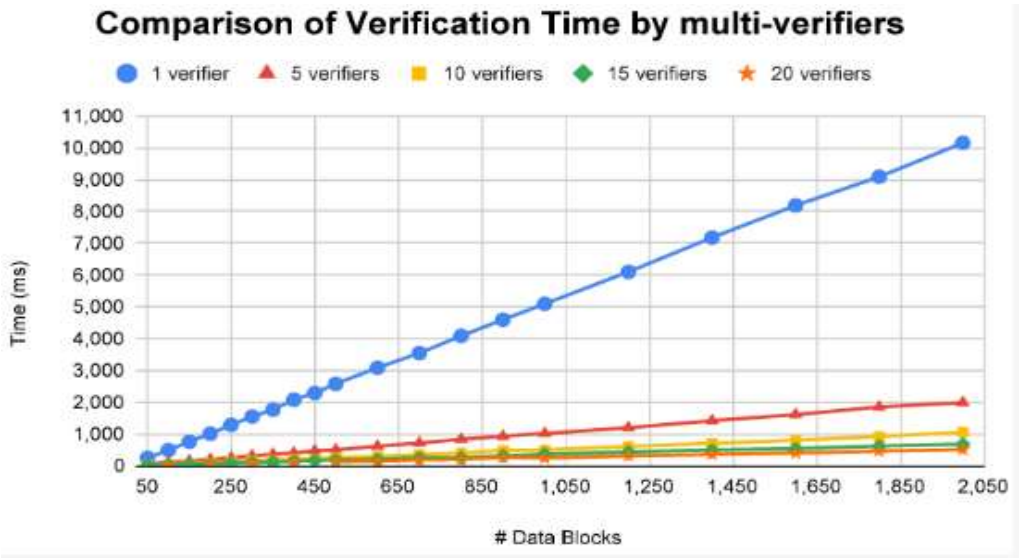


Fig.6. Comparison of proof generation time

E. Cloud Data Integrity Verification

This is scheme first calculates a partial number of verification tokens, and each token is associated to some data blocks, thereby ensuring that the scheme can support the revision of data in a prescribed manner, but the number of verifications and data updates performed by the verifier is partial, and only extra operations are supported. Each update requires recreating the enduring substantiation tokens. In this solution, the time complexity of the computational overhead of the CSP and the data owner is O(t), and the time complexity of the communication overhead is O(1). After that, a sequence of improvements has been proposed.



Comparisons of different lattice signature schemes

Public-key length	Private key length	Signature length	Whether sampled	Random oracle model
$(nm+(\|\mu\|+2)n^2k+n)\log q$	$mnk \log q$	$m+2nk \log q$	Yes	No
$nk \log q$	$mk \log(1+2d)$	$2m \log(12\sigma)+2k \log b$	No	Yes
$(nn+dm)\log q$	$m^2 \log q$	$m \log q$	Yes	No
$nm \log 2q$	$nm \log 2q$	$m \log(12\sigma)$	No	Yes

Table 1.1 Comparisons of different lattice signature schemes

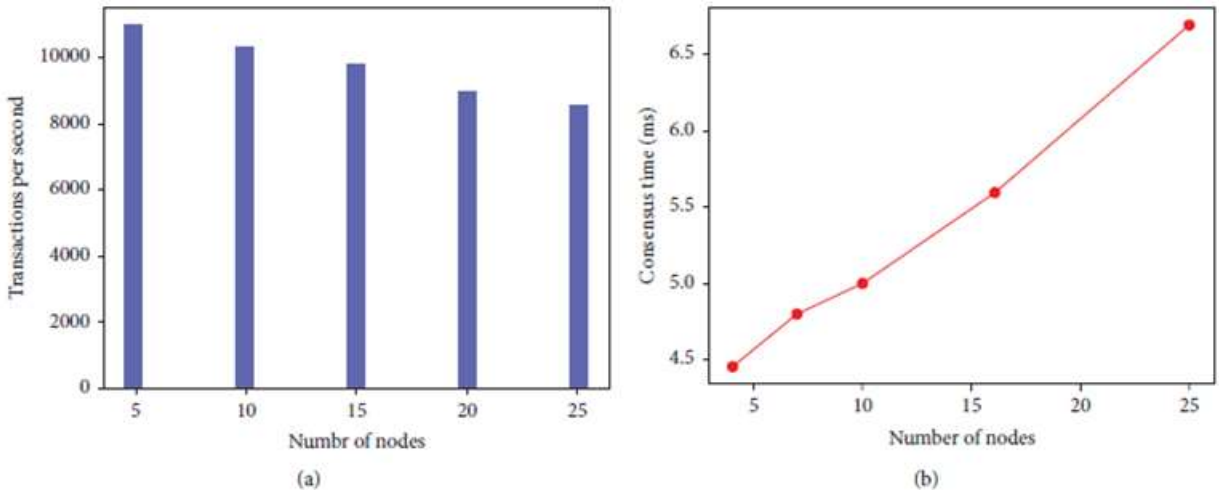


Fig.3. Generic blockchain model **Fig.7.** Performance evaluation of blockchain. (a))Throughput. (b) Consensus time.

VIII. CONCLUSION

Cloud Computing provides the interaction along with user and cloud servers via the service layers which are mentioned in cloud computing architecture. People pay more
and more notice to data security in the cloud storage environment, and integrity verification is the basis of data security. The cloud storage service provider can act out of its own. It is special to cover or even trick users due to the reflection of interests. Therefore, in the cloud storage environment, the view of service providers aggressively launching attacks should also be considered when checking the integrity of files. The main aim of this integrated system is to ensure and develop the trust between data server, data users and the data security. A review of prior techniques has been analyzed for identifying the challenges implicated in this integration. In the future work, will consider optimizing the scheme to resist replay attacks and increase the security of the scheme and the closer combination of blockchain and integrity verification scheme needs to be explored and more inclusive characteristics of the scheme need to be satisfied.

IX. REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564.
[3] Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In IEEE 13th International Conference on Service Systems and Service Management (ICSSSM). 1-6, 2016.
[4] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, 2018.
[5] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, et al., "BigchainDB: a scalable blockchain database," white paper, BigChainDB, 2016.
[6] M. S. Sahoo and P. K. Baruah, "HBasechainDB–A Scalable Blockchain Framework on Hadoop Ecosystem," in Asian Conference on Supercomputing Frontiers, 2018, pp. 18-29.
[7] Jiangsu and Nguyen Khoi Tran, “Application of Blockchain Technology in Sustainable Energy Systems: An Overview, 2 August 2018; Accepted: 26 August

[8] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology:Architecture, consensus, and future trends, in Big Data (BigData Congress), 2017 IEEEInternational Congress on, IEEE, 2017, 557–564.
[9] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, 2019.
[10] A.S.Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research, 5 (2014), 491–497
[11] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp. 1545-1550.
[12] Ms. Ketki R. Ingole , Ms. Sheetal Yamde, " Blockchain Technology in Cloud Computing : A Systematic Review", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 04 | Apr-2018