Building Secure Clouds by Perpetual Auditing using Blockchain Technology

Balamurugan N[1], Bhuvanesh R[1], Lathapriya K M[1], Sharmasth Vali Y[2], Shakkeera L[3]
balaeng98@gmail.com, bhuvaneshadijnru@gmail.com, mohansita03@gmail.com, vali566@gmail.com, shakkeera841@gmail.com

[1] *Student, Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai-601 301*
[2] *Assistant Professor, Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai-601 301*
[3] *Assistant Professor, Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai*

Abstract - The modern method of storing the data is a cloud server. But due to security and privacy concerns about the dependability of their CSP, consumers of Cloud service are irresolute to select cloud services. Hence, avoid this circumstance, we bring in an in-built verifier to validate the data regularly in the cloud. Cloud service mainly approached these matters by building assurance and enhancing the clarity of the cloud service provider. Along with CS, Perpetual Auditing (PA) of the cloud server is determined to increase the reliability of the certificates. Also, by implementing the blockchain technology, the user's data will be split into blocks and stored in different servers which makes the data more secure. It also audits the transactions in the cloud by the users.

Keywords— cloud computing, cloud service provider, continuous auditing, blockchain, integrity checking, file allocation table

I. INTRODUCTION

Cloud Service is the on-demand availability of system supplies, especially information depository and computing capability, without personal and active surveillance by the user. If the connection to the user is moderately compressed, it may be qualified an edge server. Clouds may be confined to a single company (as enterprise clouds), or be open to many companies (as the public cloud). Cloud computing based on the distribution of sources to accomplish integration also economics. Cloud service providers practice a "pay-as- you-go" model, which can traverse toward unanticipated functioning expenses if administrators not familiarized with cloud-pricing standards. A rising number of companies outsource their information, applicability and enterprise processes to the cloud, enabling them to accomplish fiscal and professional gains due to on-demand and pay-per-use price system. Though, companies are still irresolute to operate cloud-based service because of security, privacy, and reliability matters concerning provisioned cloud services as well as insecurities of the integrity of their CSP. Cloud services strive to ensure a tremendous level of protection and acquiescence. We insist that perpetual auditing is needed to ensure stable and defended cloud services, and whereby enhance the trustworthiness of user's data. Perpetual Auditing of the cloud is yet in its outset moreover, we unveil that utmost of the current methodologies is not relevant for 3rd party auditing purposes. The Blockchain technology also used to distribute the data in multi-cloud Environment as various blocks. Blockchain defined as a decentralized, distributed ledger which has the source of a digital asset. Blockchain Technology is also called as Distributed Ledger Technology (DLT). Figure 1 illustrates to understand the process taken place in the blockchain. A simple example of blockchain technology is Google Document.

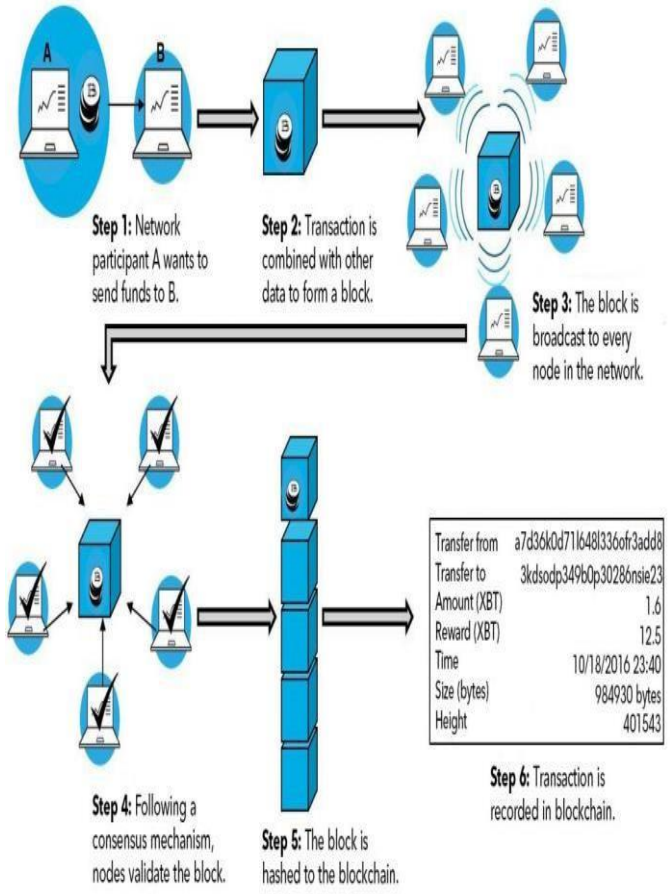

Figure 1 Overview of Blockchain

It develops a decentralized distribution chain which provides access to everyone at the same time. When we create a report and distribute it with an assemblage, the report is distributed instead of reproduced or conveyed. They have three main elements which are

1. Blocks
2. Miners
3. Nodes

Blocks:

The initial chunk or block in a chain is formed,

then the nonce was generated by the cryptographic hash. The information in the chunk is held secured and perpetually bounded with the nonce and hash value until it is mined.

Miners:

Miners build new chunks in the blockchain by a process named as mining.

Nodes:

Nodes may be any variance in electronic equipment that keeps copies of the blockchain and retains the network functioning.

Therefore, we suggest a conceptual CA architecture and implementation of Blockchain Technology.

II. EXISTING SYSTEM

In cloud computing, indirect data probity checking is a critical protection dilemma. The customer's extensive information is outside his control. The spiteful cloud systems may alter the customer's data to earn more gains. Despite, cloud-based services are part of an ever-changing situation, rising from agile technology life periods and integrate cloud computing (CC) features, like on-demand providing and entangled stock successions. Therefore, so continued validity duration may plant into dilemma the authenticity of conserved data. And also CSP's customers do not long maintain their data regionally, promising that their data is being precisely stored and probity is preserved in cloud service circumstances is of critical concern. It is inadequate to determine data was modified or deleted when accessing the data. It may be late to retrieve lost or corrupted data. Data loss could befall in any base, besides the high degree of strong measures CSP would exercise. It neglects some dispersion delays in distributed systems and leads to transient deviations. The cloud system and this verifier, thus annulling the outsourced information probity affirmation. Most of these systems are weak in the case that verifiers are malicious. Various users frequently depend on compact appliances that have bounded computational capability, or sway not ever possess web access.

Disadvantages:

The high validity times may put in distrust the reliability of cloud service provider. The Data Consistency is also an issue in the existing system. The Third-party Verifiers are also involved which involves the data privacy.

III. LITERATURE SURVEY

Kan Yang introduced an effective and safe active auditing protocol which is wanted to change the customer's mind that their data correctly stored within the cloud system. It is an effective and privacy-preserving auditing protocol **[1] [2]**. The Fog-assisted secure data deduplication scheme used to hide the user's identities during data collection.

The repository storage needs assure about their authenticity of information on storage **[3] [4]**.Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou proposed users can remotely store their data. Empowering user based auditing for cloud storage is one of the crucial distinction. A whole of those community-driven, non-commercial systems enhanced popular and comprehensive **[5] [6] [7]**. We deduced from Florian Tschorsch Björn Scheuermann that the elemental compositions and acumens at the essence of the Bitcoin protocol and its uses. Bit-coin used to build impartial challenging communications to impede the collusion between spiteful auditors and cloud systems **[8] [9]**. Frederik Armknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu, Christian A. Reuter proposed Lessens user trial, acquires negligible burden on the verifier and considerably enhances over existing publicly verifiable Proof of Retrievability [10]. Outsourced proofs of Retrievability are technically and economically feasible. The security model yielded by the proof-of-work **[11] [12]**.

IV. PROPOSED SYSTEM

In Versatile Cloud conditions, the remote data probity inspecting requires to ensure the consumer's data. The admin configures the server and set the audit time initially. Then the customer will upload the data to the Cloud Server. The uploading data may be in either format, such as a document or audio or video. This data is divided into blocks practicing the Dynamic Block generation Algorithm and stored in a various cloud system. The File Allocation Table (FAT) File System holds proper Indexing and Metadata for the various Chunks in the Cloud system. Here the verifier accepts to investigate logs, which are continuously done during monitoring procedures by CSPs. If outsider alters any data in any of the cloud systems, the perpetual auditing process helps the verifier to perform Block level and File-level checking for obscure data Probity Checking utilizing VDIC Algorithm. Verification Schemes allows a customer to exercise a 3rd person verifier to validate the data integrity on behalf of her/him, whereas existing verification methods are weak to delaying verifiers who might not conduct verifications on time. Besides, a maximum number of the verifying methods are developed based on PKI, also whereby suffer from document management difficulty. The ultimate intention is to order verifiers to register each verifying event into blocks or chunks in blockchain technology. The events in this technology are time-sensitive. After all, transactions are time-based events, following the analogous transactions are recorded into the blockchain. It will empower users to verify whether auditors conduct the affirmations at the designated time. There exists no Third party verifier elsewhere there is the admin who verifies the data. The server renders arbitrary chunks to Verifier for Probity inspection to defend user secrecy even of admin. Information retrieval is achieved by the verifier automatically if the data goes altered during verification of data blocks. Users can complain about the cloud for file recovery. And also we append all the data related to auditing record in blockchain for security purpose.

Advantages:

The Certificate-less verifier scheme is created on not necessary for certificates and also freedom of the document management problems. The events are time-stamped, following the analogous transactions are recorded into the blockchain.

V. SYSTEM DESIGN

System design is the technique for determining the infrastructures, units, connections, and information for a system to reach the required specifications. The figure 2 illustrates the system architecture. After analyzing the system, they are four modules have been identified which are the following:

A. Admin Configuration and User Registration

B. File Upload and block splitting using DBG algorithm

C. Verification of data using VDIC algorithm

D. Attacker Scenario and Data Recovery

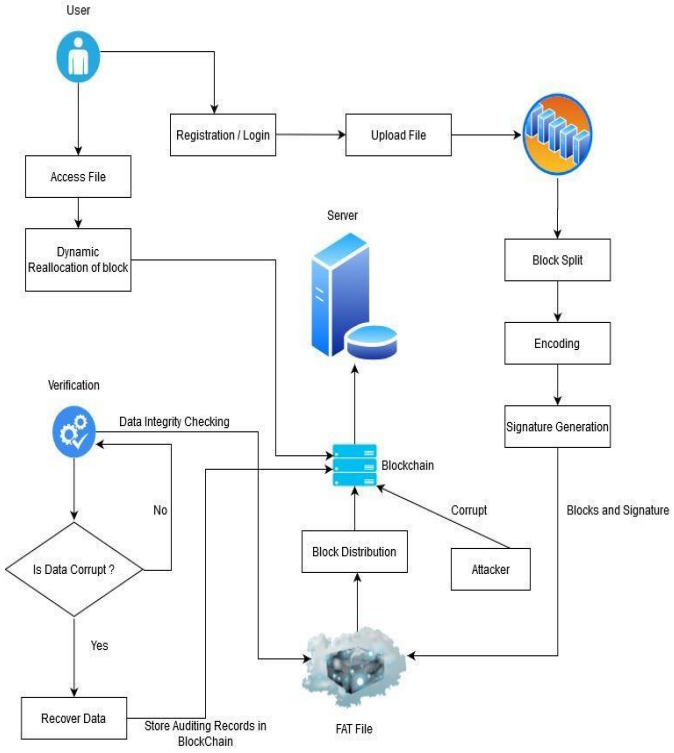

Figure 2 System Architecture

A. Admin Configuration and User Registration:

The administrator configures the Multiple Cloud system configuration. For each system, the admin assigns an IP address and port number. Now a System Architecture is built for Versatile Cloud systems.

An administrator can also employ the old Multiple Cloud system configuration if needed. During the system configuration, the FAT file can be altered or prevail the alike. The administrator shall fix specific audit time during configuration for Data Integrity checking process. User must go through a primary level of Enrollment at the webpage. The users give their particular information at this registration process. Every user should give the username and password in a preferred manner by the webpage. The login information which in turns stores in the server. After Registration, user can log in into the web-end whenever the need to upload files to the server.

B. File Upload and block splitting using DBG algorithm:

The user uploads the file in any format which stores in the server. The data is divided into complex chunks of data using the Dynamic Block Generation Algorithm. The blocks are append using Linked Hash Map which is like Hash Map with an additional feature of maintaining an order of elements inserted into it. Hash Map provides the quick insertion, search and deletion but it never maintains the track and order of insertion. Then the blocks of data are stored in a different server. Then every chunk will be affixed with signs ere saving the data in File Allocation Table FS. The MD5 message-digest method is a hash function producing a 128-bit hash value. It is being used as a value to inspect data probity, but only against unthinking exploitation. Base64 Algorithm used to encrypt the information into a sequence of 64-printable characters. FATFS has precise Indexing and Metadata for the various blocks of the information which are being given by the consumer.

C. Verification of data using VDIC algorithm:

The auditor conducts Remote Integrity Monitoring on customer's information. The server designates an arbitrary succession of all the chunks to the auditor or verifier. Instead of retrieving the entire file through probity inspection. Hence, user privacy remains protected even from the administrator. The VDIC algorithm has two levels of inspection which are

1. Block-level inspection
2. File-level inspection

In the first level of inspection, they are three signs generated which are given below.

- A Sign of a segment recovered from a File Allocation Table FS.
- A Sign recovered from these blocks and added to the sign saved in the system.
- A new sign generated should be verified.

Thus the preceding signs are twice checked for Block level Probity Inspection. The contents of the chunks are affixed to check with File-level Probity inspection and update all auditing aspects in the blockchain.

D. Attacker Scenario and Data Recovery:

An outsider can alter data in either one of the cloud systems. On data probity inspection done by the Auditor, it notifies forged blocks to the admin. After verifier finish, the auditing Recovery Process will be taken place automatically when information in chunks gets altered. Customer can complain to the Admin if their data gets damaged. When the consumer accesses the record, then chunks will be reallocated dynamically to present access confidentiality. Then the FATFS should be improved or upgraded. The verifier should observe cloud system perpetually.

VI. RESULTS

The proposed system is implemented using java and struts framework. The figure 3 illustrates admin configuration which is the method of connect the multi-server and to set auditing time period. The user login and registration implied at this step. For a new user, user registration is also possible.

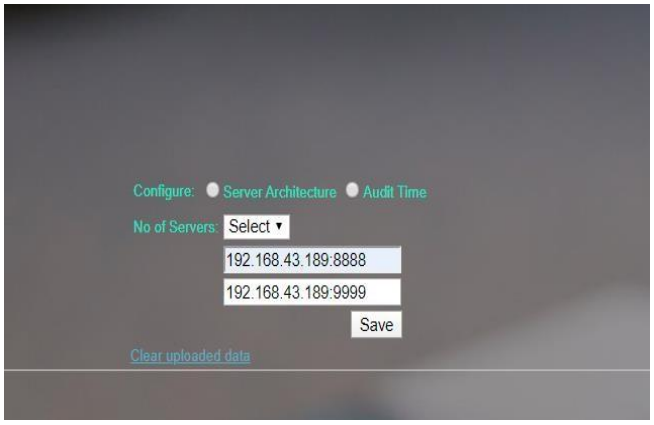

Figure 3 Admin configuration

In the below figure 4, the uploaded data are split into multiple blocks and dynamically stored in the server

Figure 4 File Upload

In the below figure 5, the public auditing is done, where the auditor checks the blocks for every particular auditing time duration.

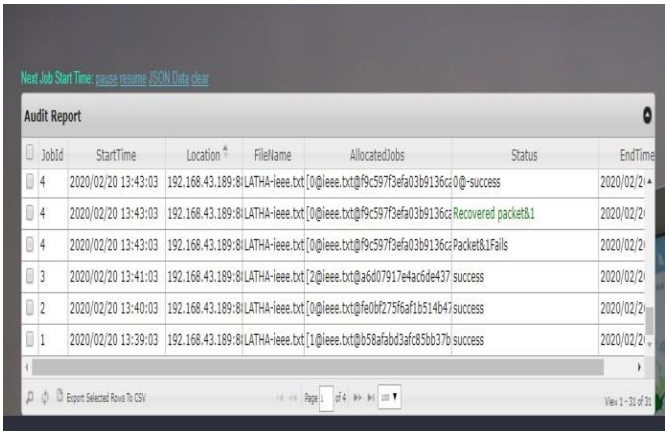

Figure 5 Data Integrity Checking (Public Auditing)

If there any attacker scenario occurs like shown in figure 6, then the user receive the message about data corruption and also the data will be retrieved by the auditor as shown in above figure.

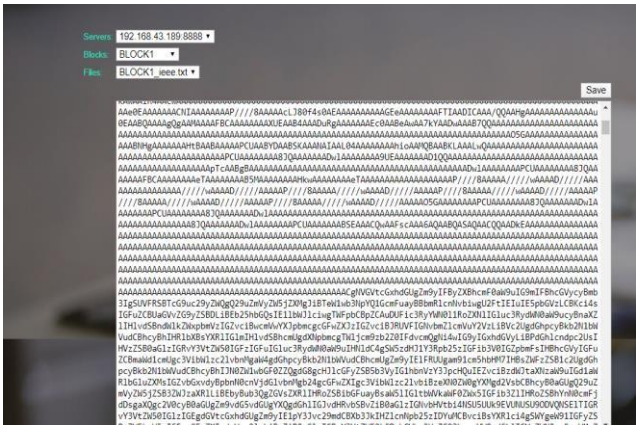

Figure 6 Attacker Scenario

VII. CONCLUSION AND FUTURE WORKS

The dynamic cloud system background and the escalating choice regarding crucial purposes based on business from CSP oblige deeply secure cloud services. Our conceptual architecture uses the on-chain money, wherever any affirmation made by the verifier is combined into an event on the blockchain technology. The security analysis proves that verifier affords the most effective security guarantee contrasted with existing schemes. Continuously auditing cloud services can provide immense protection and dependability to CS adopters as per our study. Continuous audit of cloud service can only increase the trustworthiness of certifications with our study, by conceptualizing and architecture discussions exposed that maximum of the current techniques was not applicable for 3rd party assistance verification goals. Since the study of trials unveils, there exists yet an abundance of analysis to accomplish.

Future Enhancement

Besides study is concentrated toward improving auditing methods adapted by some conditions, notably involving the inspection of safety standards and adherence to significant CS innovations.

The cloud certifications should be provided to the user whereas the user can utilize it to make sure the cloud secure to store its information. Furthermore, a prospective study must review how unparalleled CC highlights overpower ceaseless verifying utilization. Distinguished techniques require the implementation to show their functioning and fiscal applicability in cloud systems. Hence, recognized and future techniques require to be combined with Cloud Service guidelines to measure patterns compliance. Besides future study should demonstrate to contrive certification breaches, and whereby to notify customers regarding certification compliance.

.

REFERENCES

1. K. Wang, J. Yu, X. Liu and S. Guo, "A Pre-Authentication Approach to Proxy Re-encryption in Big Data Context," in IEEE Transactions on Big Data.
2. K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, Sept. 2013.
3. Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to- Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.
4. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, third quarter 2016.
5. Shacham H., Waters B. (2008) Compact Proofs of Retrievability. In: Pieprzyk J. (eds) Advances in Cryptology - ASIACRYPT 2008. ASIACRYPT 2008. Lecture Notes in Computer Science, vol 5350. Springer, Berlin, Heidelberg
6. Wood, Daniel Davis. "Ethereum: A Secure Decentralised Generalised Transaction Ledger." (2014).
7. Frederik Armknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu, and Christian A. Reuter. 2014. Outsourced Proofs of Retrievability. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 831–843. DOI: https://doi.org/10.1145/2660267.2660310
8. Yang, Kan & Zhang, Kuan & Jia, Xiaohua & Hasan, M.Anwar & Shen, Xuemin. (2016). Privacy-Preserving Attribute – Keyword Based Data Publish-Subscribe Service on Cloud Platforms. Information Sciences. 387. 10.1016/j.ins.2016.09.020.
9. C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," in IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013. doi: 10.1109/TC.2011.245
10. Ateniese, Giuseppe & Burns, Randal & Curtmola, Reza & Herring, Joseph & Kissner, Lea & Peterson, Zachary & Song, Dawn. (2007). Provable Data Possession at Untrusted Stores. Proceedings of the ACM Conference on Computer and Communications Security. 598-609. 10.1145/1315245.1315318.
11. J. Ni, K. Zhang, Y. Yu, X. Lin and X. S. Shen, "Providing Task Allocation and Secure Deduplication for Mobile Crowd sensing via Fog Computing," in IEEE Transactions on Dependable and SecureComputing. doi: 10.1109/TDSC.2018.2791432
12. Pham, Hoang & Woodworth, Jason & Salehi, Mohsen. (2018). Survey on Secure Search Over Encrypted Data on the Cloud.
13. Y. Yang , X. Liu , X. Zheng , C. Rong and W. Guo ,"Efficient Traceable Authorization Search System for Secure Cloud Storage," in *IEEE Transactions on Cloud Computing*. doi: 10.1109/TCC.2018.2820714.
14. J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.
15. H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.
16. J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, "Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2018, pp. 187–206.
17. L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.
18. G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870–885, 2019.
19. W. Shen, B. Yin, X. Cao, Y. Cheng, and Shen, "A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds," IEEE Trans. Cloud Computing, to appear, doi: 10.1109/TCC.2016.2647718.
20. H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing -centric networks with content-based encryption," Journal of Network and Computer Applications, vol. 128, pp. 21–32, 2019. [23]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS, 2009, pp. 355–370.
21. X. Zhang, H. Wang, and C. Xu, "Identity- based key-exposure resilient cloud storage public auditing scheme from lattices," Information Sciences, vol. 472, pp. 223–234, 2018.
22. Y. Zhang, C. Xu, X. Lin and X. S. Shen, "Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors," in *IEEE Transactions on Cloud Computing*.