International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Based De-Duplication Analysis of Cloud Data with Data Integrity using Policy Based Encryption Technique in Cloud Storage

Badari narayan V S[1], Mr. Akash Kumar Bhagat[2], Chethan C[3], Badria Sulaiman Alfurhood[4], Aditya Pratap Singh[5], Dr. Mahesh T R[6]

Submitted: 04/11/2022 **Accepted:** 01/02/2023

Abstract: Cloud computing is one of developing areas of innovation, which permits capacity, access of information, programs, and ir execution over web while supplying an assortment of data relevant administrations. With cloud data administrations, it is fundamental for data must be kept safely and to be circulated securely throughout various clients. This research propose novel technique in cloud data based de-duplication analysis and data integrity by policy based encryption in cloud storage. Here cloud based data analysis and storage analysis has been carried out. data analysis for de-duplication is carried out using blockchain technique and data integrity is carried out using policy based encryption. experimental analysis shows parametric analysis in terms of data integrity, storage analysis, throughput, end-end delay and packet delivery ratio.

Keywords: *Cloud computing, de-duplication, cloud data, data integrity, blockchain, encryption.*

1. Introduction

Cloud computing is a flourishing worldview because of tremendous on-request administrations to end-clients over web. Cloud computing has furnished clients with creative highlights, like accessibility, adaptability, and economy, that assistance to fulfill significant interest for capacity and calculation assets [1]. End-clients re-appropriate ir information to center organization on cloud for handling and stockpiling. Be that as it may, re are numerous obstructions confronting information proprietors. In first place, reaction time among clients and cloud is high in light of fact that information are put away far away from information proprietors. Second, end-clients' information security and protection are powerless to infringement in violation of fact that semi-believed outsider controls cloud. exploration local area has concentrated on information security and protection issues in cloud computing by taking on and applying progressed cryptographic strategies [2]. Be that as it may, interest to design ano r innovation to determine cloud dormancy issue is as yet present. Blockchain technology is a promising development for the future. It can assist us in creating systems that are more dependable and safe. No matter the nature of the data, same systems will still apply. In other words, we may utilise it for electronic papers, multimedia material, etc. This massive quantity of data should not be stored directly on blockchain since doing so would increase chain length and block size. Records will thus be maintained on the cloud, and data on the blockchain will be used to identify and track document tampering. [3].

2. Related Works

Researchers guarantee that this approach is more skilled and secure than 'CP-ABE (Ciphertext-Policy AttributeBased Encryption)' plot subsequent to leading various trials. Likewise, when quantity of encoded documents of information was expanded, AHAC's speed improved fundamentally. Work [4] proposed a highlight guide decentralized computing model that permits various ga rings

[1] *Sri Siddhartha Academia of Higher Education, Computer science and engineering, Sri Siddharth Institute of technology, Tumakuru.*
badarivs@gmail.com
0000-0003-3039-6993
[2] *Assistant Professor, Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India.*
Id-akash.b@arkajainuniversity.ac.in,
0000-0001-8717-764X
[3] *Assistant Professor, Information Science & Engineering, Sri Venkateshwara College of Engineering, Bengaluru, India.*
chethanc123@gmail.com
0000-0002-2706-5977
[4] *Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia.*
bsalfurhood@pnu.edu.sa
[5] *Department of IT, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India.*
singhaditya@akgec.ac.in
0000-0002-2349-3739
[6] *Assistant Professor, Department of Computer Science Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India.*
t.mahesh@jainuniversity.ac.in
0000-0002-5589-8992

toward store and run information toge r while keeping information totally hidden. This model accomplishes programmed control of individual information by wiping out requirement for confided in outsiders. Creator [5] presented a decentralized access control mechanism based blockchain. Work [6] introduced an information dividing model among cloud specialist co-ops based blockchain. Creator in [7] proposed a decentralized limit based access control mechanism (BlendCAC), which can successfully safeguard security of hardware, administrations and data in enormous IoT (Internet of things) framework. Work [8] plan a structure utilizing shrewd agreements and blockchain innovation for following, overseeing and upholding such information sharing arrangements. Creator [9] present a blockchain-based framework for secure common validation to implement fine-grained access control strategies, which give protection and security ensures. For instance, writing [10] utilizes blockchain innovation to store client's access control records, writing [11] utilizes blockchain innovation for biomedical and medical care applications, [12] involves three brilliant agreements for access control for Internet of Things.

3. System Model

This article presents innovative methods in cloud data based de-duplication analysis and data integrity by policy based encryption in cloud storage. Here cloud based data analysis and storage analysis has been carried out. data analysis for de-duplication is carried out using blockchain technique and data integrity is carried out using policy based encryption.

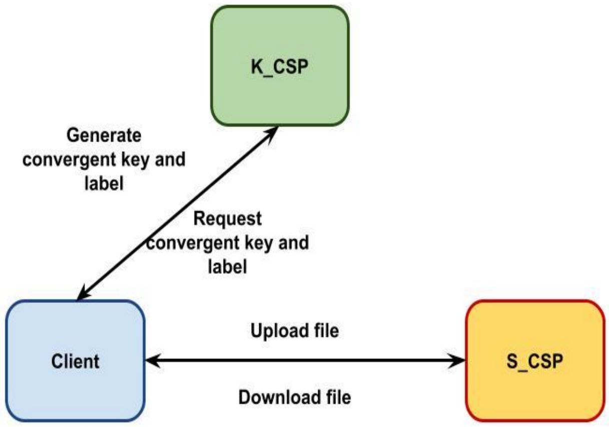
K_CSP
Generate convergent key and label
Request convergent key and label
Client
Upload file
Download file
S_CSP

Fig. 1 data de-duplication and data integrity model

To circulate portions of expert marking key, an assistant DC can be inconsequentially utilized to accomplish errand. In any case, conveyance community may likewise be a pothole where key might be revealed. For each key server KSi , it randomly picks a key offer SKi along with a confidential number Ai fulfilling as displayed in eq. (1).

$$0 < SKi < [\frac{q}{n}] \quad (1)$$

n, at that point, it works out aij = SKi + Aiq mod dj for j = 1, 2, • • • , n and conveys m to relating servers. In wake of getting all aij from different hubs, offer Lj for server KSj can be straightforwardly registered as eq. (2)

L_j=∑_(i=1)^n a_ij modd_j

≡∑_(i=1)^n (SK_i+A_i q).□
(2)

PK=∏_(j=1)^n▒〖〖PK〗_j mod q〗
(3)

All more critically, information clients and information proprietors use E reum shrewd agreements to store and recover ciphertext information to run encryption and unscrambling calculations. Each agreement call is recorded on blockchain. In this manner, data moved between information clients and information proprietors is non-mess with and non-renouncement. re are four elements in our plan, in particular brilliant agreements is of connection points to store information and get information; Data Owner(DO): Responsible for making and conveying shrewd agreements, transferring scrambled documents, characterizing access control approaches, appointing characteristic sets and adding legitimate access periods to information clients;

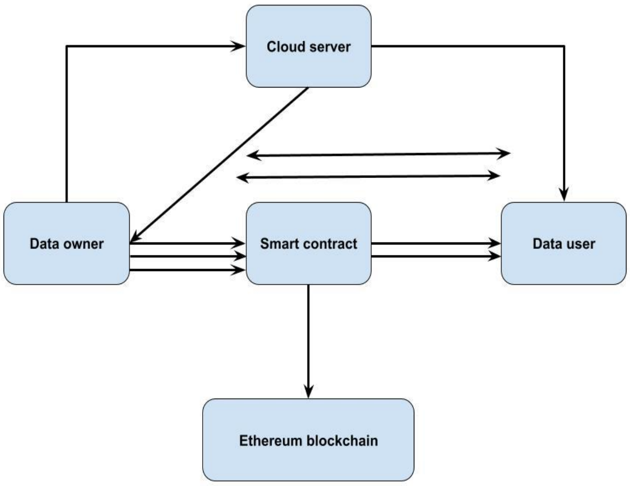

Fig. 2 blockchain based de-duplication analysis and data integrity

ciphertext and individuals from ga rings ought to be changed to guarantee an obscurity in future, and in reverse in complicated proprietorship board tasks. Thorough systems are done under specific situations: Community Key CKj doesn't immediately redesign subsequent to adding µj to update list Lj . At point when specialist organization records Lj to specialist co-op, specialist co-op can initially approve Lj 's redesign records. On off chance that µj is available, specialist co-op will direct updates and pull toge r tasks for local area key. It clears rundown a short time later. This empowers m to lessen size of ga ring tasks while guaranteeing retroactive privacy. Coming up next are thorough systems for significant overhauls and reencryption activities: CKj has been utilized for scrambling encoded information C 1 j 0 and relating altered information C 1 j . An inconsistent local area key CK0 j has been picked and encryption interaction must be done. specialist organization n, at that point, utilizes encryption cycle for getting every one of related information values saw as in table related with clients U1 j .

4. Performance Analysis

In this part, we give trial examination of our plan. particular arrangement of trial stage and exploratory climate. Programming language is java and strength. Outside aide is JPBC and web3j. execution of this paper is based on two working frameworks, E reum blockchain is conveyed in Linux ubuntu16.04 LTS laid out in virtual machine, and principal encryption calculation is carried out in Windows10 framework. After accumulation is fruitful, utilize web3j to produce JavaBean from brilliant agreement to Maven project in obscure. In Maven project, quality encryption calculation is composed utilizing shroud by presenting container bundle of JPBC. By depending on some container bundles of web3j, cooperation between information proprietor and information shopper for shrewd agreement is understood, which makes access control calculation of this paper better by consolidating characteristic encryption calculation with intense contract.

Table-1 Overall parametric comparison between proposed and existing technique

Specifications	Overall performance		
	100 Users	**300 Users**	**500Users**
Au ntication	55	66	72
Security	69	74	81
False Classification Ratio	52	56	61
Time Complexity	71	76	82

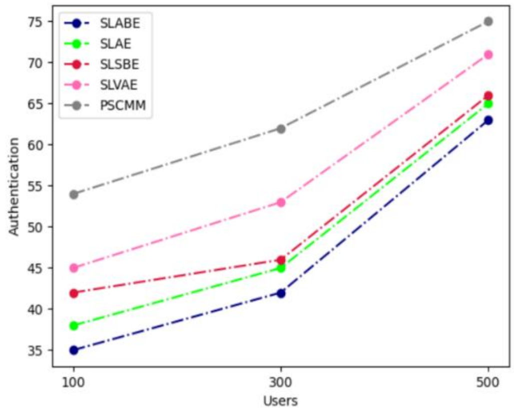

Fig. 3 Performance Evaluation on Au ntication

au ntication execution as displayed in above figure-3 created by various calculations have been estimated and contrasted and consequence of different techniques. proposed calculations have created higher confirmation execution of 72% than o r strategy.

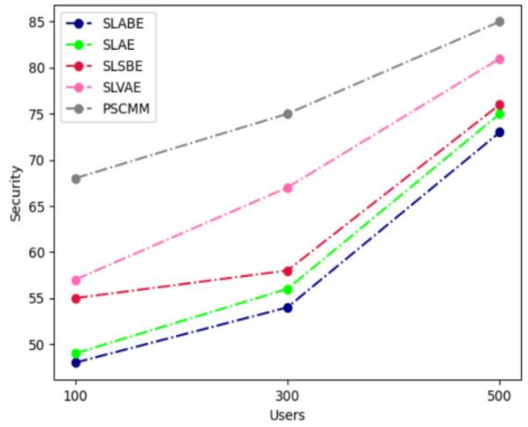

Fig. 4 Overall security performance

security execution as displayed in figure-4 created via several strategies is estimated and analyzed. proposed De_Blo_PE algorithm have created higher security execution of 81% than different techniques.

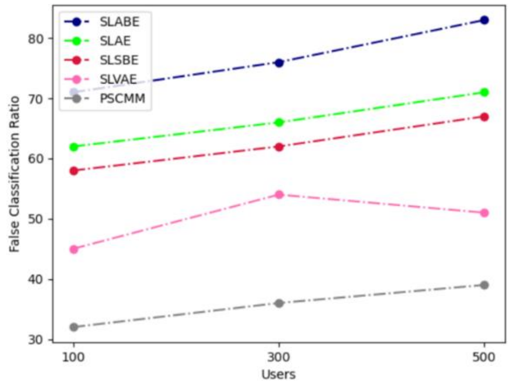

Fig. 5 Overall false classification ratio

proportion of false order as displayed in figure-5 is estimated on various techniques at various amount of clients requirements. envisioned calculation have delivered less false proportion of 61% contrast with other techniques.

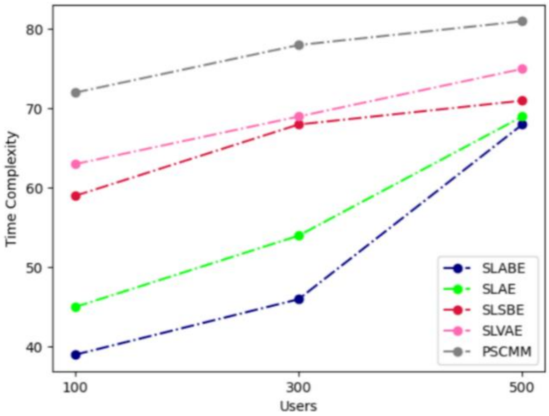

Fig. 6 Overall time complexity performance

time complexity as displayed in above figure-6 presented by techniques have been estimated and contrasted and aftereffect of different strategies. proposed algorithm have created less time intricacy of 82%than different techniques.

5. Conclusion

This study offers an innovative method in cloud data based de-duplication analysis and data integrity by policy based encryption in cloud storage. To ensure deduplication is safe, prior research ordinarily host presented third-ga ring examiners for information honesty check, however it could be experienced information spill by outsider inspectors. And furthermore standard strategies couldn't confront more troubles in large information deduplication to consider two clashing points of high copy end proportion and deduplication throughput accurately. This study presents an enhanced blockchain-based secure information deduplication is given effective cryptographic strategies to safely save distributed storage. It has been determined through experimental investigation that Authentication, Security, False Classification Ratio, Time Complexity. proposed technique attained Authentication of 72%, Security of 81%, False Classification Ratio of 61%, Time Complexity of 82%.

References

[1] Venkatachalam, K., Prabu, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric au ntication with de-duplication on distributed cloud storage. *PeerJ Computer Science*, *7*, e569.

[2] Almrezeq, N. (2021). An Enhanced Approach to Improve Security and Performance for Deduplication. *Turkish Journal of Computer and Ma matics Education (TURCOMAT)*, *12*(6), 2866-2882.

[3] Gnana Jeslin, J., & Mohan Kumar, P. (2022). Decentralized and Privacy Sensitive Data De-Duplication Framework for Convenient Big Data Management in Cloud Backup Systems. *Symmetry*, *14*(7), 1392.

[4] Rao, K. P. (2021). Efficient and Reliable Secure Cloud Storage Schema of Block chain for Data De-duplication in Cloud. *Turkish Journal of Computer and Ma matics Education (TURCOMAT)*, *12*(9), 1547-1556.

[5] Ruba, S., & Kalpana, A. M. (2021). An Improved Blockchain-Based Secure Data Deduplication using Attribute-Based Role Key Generation with Efficient Cryptographic Methods.

[6] Kalpana, A. M. An Improved Blockchain-Based Secure Data Deduplication using Attribute-Based Role Key Generation with Efficient Cryptographic Methods.

[7] Abdmeziem, F., Boukhedouma, S., & Oussalah, M. C. (2021, September). On data security of information systems: Comparison of approaches and challenges. In *International Conference on Computational Science and Its Applications* (pp. 240-255). Springer, Cham.

[8] Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, *164*, 152-167.

[9] Rajkumar, K., & Dhanakoti, V. Fuzzy-Dedup: A secure deduplication model using cosine based Fuzzy interference system in cloud application. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-14.

[10] Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Security and Privacy*, *4*(5), e162.

[11] Shaikh, A. H., & Meshram, B. B. (2022). Cloud Attacks and Defence Mechanism for SaaS: A Survey. In *Intelligent Computing and Networking* (pp. 43-52). Springer, Singapore.

[12] Anil Kumar, G., & Shantala, C. P. (2022). Novel Modeling of Efficient Data Deduplication for Effective Redundancy Management in Cloud Environment. In *Expert Clouds and Applications* (pp. 479-490). Springer, Singapore.