Group Data Management For Cloud Computing Based on Public Auditing

A. R. Sunil Kumar [1], Mr. C.Bastin Rogers[2]
[1, 2] Dept of CSE
[1, 2] Stella Mary's College of Engineering

Abstract- *Cloud storage has been widely used to team work or cooperation development. Data owners set up groups, generating and uploading their data to cloud storage, while other users in the groups download and make use of it, which is called group data sharing. As all kinds of cloud service, data group sharing also suffers from hardware/software failures and human errors. Provable Data Possession (PDP) schemes are proposed to check the integrity of data stored in cloud without downloading. However, there are still some unmet needs lying in auditing group shared data. Researchers propose four issues necessary for a secure group shared data auditing: public verification, identity privacy, collusion attack resistance and traceability. However, none of the published work has succeeded in achieving all of these properties so far. In this paper, we propose a novel blockchain-based ring signature PDP scheme for group shared data, with an instance deployed on a cloud server. We design a linkable ring signature method called Linkable Homomorphic Authenticable Ring Signature (LHARS) to implement public anonymous auditing for group data. We also build smart contracts to resist collusion attack in group auditing. The security analysis and performance evaluation prove that our scheme is both secure and efficient.*

Keywords- Provable data possession; data integrity; blockchain; ring signature.

I. INTRODUCTION

Number of companies and developers turning to cloud service has been growing rapidly in recent years. Other than individual users, these enterprise and corporate customers usually work in groups, sharing data with each other. What is more, this exchange of data may sometimes occur among entities across various domains for co-operated research, making use of cloud storage service. One of the most compelling topics for cloud data is its integrity. Group sharing makes it even more complicate. One group member, which we call it data owner, generates some dataset and uploads it to cloud.

The applications of blockchain in cloud computing are linked to the Cloud of Things (CoT), a combination of cloud computing and the Internet of Things (IoT). So, before we dive into blockchain cloud computing and blockchain-based cloud, let's first discuss what exactly the Cloud of Things is.

Cloud of Things provides a powerful and flexible cloud computing environment to manage IoT services more efficiently. This means CoT enhances the performance of an IoT system.

IoT is a system of numerous interconnected devices, such as sensors, home appliances, vehicles, etc. The devices in an IoT system can connect and exchange data over the internet without any human intervention.

Many industries use IoT systems to collect data from surroundings and store and analyze it to get valuable information for taking the right action. However, IoT devices have limited storage capacity, so they use the cloud to store large sensor data, and this is what forms CoT. There are different cloud service options available, such as public clouds, private clouds, and hybrid clouds.

The others can access the data and make use of it, which are called data users. To data users, they cannot ensure whether data corruption is due to hardware/software failure, human errors of data owner or some malicious attacks. What makes things even worse, cloud service providers may conceal corruptions from users, to avoid their responsibilities and maintain business reputation. Thus, group data sharing brings in more variables for trust between members. A method for group data verification is much needed. There has been a few of works focusing on checking data correctness in cloud storage. An intuitive approach easy to call up is to retrieve the datasets from cloud and verify some kind of signatures (e.g., RSA) or collision-resistant hash values (MD5, SHA-256, etc.). Recently, blockchain-based PDP schemes noticed the risk brought by untrusted TPA, but they made a mistake in the smart contract design that allowed CSP to perform replay attacks.

Identity-based cryptography into blockchain-based PDP scheme, to avoid the complex certificate management

caused by the public key infrastructure. To add cryptocurrencies to PDP scheme to promote TPA to be more active. And work made some fine attempts in cloud-edge computation scenario. These works proved that blockchain-based PDP is practical, but lacked a full-featured solution to solve the problem of group data auditing. To solve aforementioned problems, we design a novel blockchain-based anonymous public auditing scheme for group shared data. Choose ring signature for block tag construction to achieve fully privacy-preserving data auditing, and smart contracts to reduce manual intervention and possible repudiation. Utilize distributed ledger to store block tags for better reliability, and more impartial verification. Contribution of this work is introduce a construction of blockchain-based PDP scheme, which enables anonymous integrity verification via smart contract. Propose a novel linkable ring signature tag generation method to protect identity privacy. Analyze the security of our proposed scheme and evaluate its performance.

II. LITERATURE SURVEY

Data sharing is one important service provided by cloud storage. In order to share data conveniently and securely, Shen et al. proposed a cloud storage auditing scheme for data sharing, which uses the sanitizable signature to hide sensitive information. However, it may cause unauthorized access to the data, since anyone can access the data stored on the cloud server. This article proposes a privacy-preserving cloud storage auditing (PP-CSA) scheme for data sharing, where only authorized users can access the data. Furthermore, PP-CSA adopts the Diffie–Hellman protocol to avoid the secure channel between the data owner and the sanitizer. Finally, the security analysis and the experimental results prove that the security and efficiency of PP-CSA can be accepted. This article proposed a PP-CSA scheme for data sharing, which effectively supports the sensitive information hiding. In PP-CSA, only the authorized user can access the file stored in the CS to protect the interests of the DO. The medical doctor first blinds patient's sensitive information in the EHR, and generates auditing authenticators for the blinded EHR.

Cloud storage auditing schemes for shared data refer to checking the integrity of cloud data shared by a group of users. User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for user revocation in such schemes is linear with the total number of file blocks possessed by a revoked user. The overhead, however, may become a heavy burden because of the sheer amount of the shared cloud data. Thus, how to reduce the computational overhead caused by user revocations becomes a key research challenge for achieving practical cloud data auditing. In this paper, we propose a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, we realize user revocation by just updating the nonrevoked group users' private keys rather than authenticators of the revoked user. The integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated.

With the widespread application of cloud storage, users could obtain many conveniences such as low-price data remote storage and flexible data sharing. Considering cloud service provider (CSP) is not full-trusted, lots of cloud auditing schemes are proposed to ensure the shared data security and integrity. However, existing cloud auditing schemes have some security risks, such as user identity disclosure, denial of service attack and single-manager abuse of power. To solve the above issues, we use certificateless signature technology to construct a privacy-preserving cloud auditing scheme for multiple users with authorization and traceability in this paper. Unlike the traditional schemes, our scheme realizes user identity anonymity without group signature and ring signature techniques, which guarantees the tag is compact. Meanwhile, our scheme supports that at least d managers could trace the identity of malicious user collaboratively, which avoids the abuse of single-manager power and provides non-frameability.

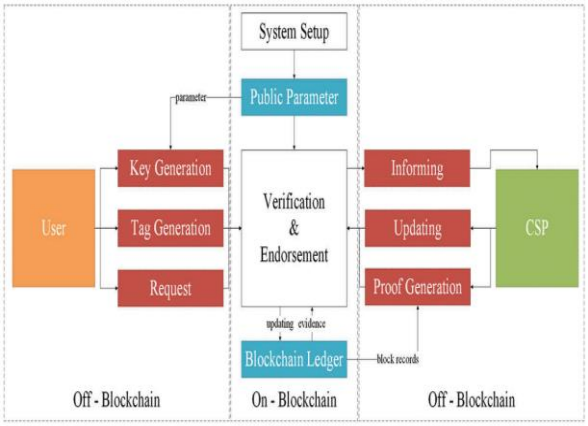
Key-exposure resilient cloud storage auditing can create a secure cloud storage during before and after the key-exposure period. However, the malicious cloud server can still tamper with and even discard the client's files which are uploaded during the key-exposure period without being detected. So as to cope with this problem, we propose an intrusionresilient public cloud auditing scheme, in which auditing authenticators are updated periodically to prevent the malicious cloud from tampering with these files using the exposed key. In addition, our scheme is secure unless the client and TPA (Third Party Auditor) are compromised in the same time period. This is different from Yu et al.'s scheme proposed in TIFS 2017, which is not secure if the client and TPA are compromised in different periods. Finally, the scheme can protect the client's file privacy, and prevent a curious TPA from recovering the file. The security analysis and the results of the experiment indicate that the security and performance of the scheme are acceptable. Cloud storage outsourcing services have many advantages, such as stability, convenience and computational efficiency, so many

enterprises or personal clients choose to store files on the cloud server.

Storage and maintenance of the data are provided as service to the client. When the clients store and maintain their data at their own server, the data are dynamic in nature and are often shared among groups of users. The clients desire the traditional flexibility when they shift their data to the Cloud. Introducing the flexibility of sharing dynamic data with storage outsourced to the Cloud needs addressing new security challenges and requires the provision for user revocation. Presents a secure and effective scheme for storage of shared dynamic data in untrusted cloud servers with provisions for privacy preserving integrity check by third-party auditor and for addition and revocation of users. Proposed scheme is based on CDH-based ring signature and vector commitment. Performance analysis, we show that our proposal outperforms more efficient than proposals using ring signatures, at auditing process and communication overhead. These protocols based on ring signatures support identity privacy of users, they are not efficient to be applied in cloud-assisted IoT applications. As we will show that in the performance analysis when the number of users of the group is 1000, the cost of tag generation is improved by an average of 48.8% as compared to that of those schemes using ring signatures.

III. PROPOSED SYSTEM

In proposed system is using blockchain-based PDP schemes. A group member send an auditing request to cloud service provider by invoking functions defined in smart contracts. The public verifier, playing the role of endorsement node in blockchain network, validates the request, including whether challenged data exists. After auditing request is accepted by blockchain network, cloud service provider compute integrity proof and send it by invoking smart contracts. The submission of integrity proof is wrapped as some kind of blockchain transaction, thus its verification can be naturally imbedded in the process of endorsement. Once public verifiers verify the integrity, they attach their endorsement to the proof, promoting the whole network accept it. In this way, the challenge-response PDP scheme has been transformed into the execution process of smart contracts.



1. System Architecture

Each member of group should invoke KeyGen to generate their own private and public keys. Before uploading a data block, data owner uses SigGen for generating ring signature (called "tags"). The algorithm of Update is the complement of SigGen, for deleting or adapting data blocks. The tags, used as evidence for checking integrity proof, are stored in blockchain ledger. ProofGen is algorithm operated by cloud service provider in order to generate aggregated signature proof in response to challenge. Public verifiers can check the correctness of proof by invoking ProofVerify. There are also request and informing modules in the figure, which are system service used by user and CSP provided by blockchain platform.

There are three kinds of entities and a blockchain network involved in group data auditing: a group of users, cloud service provider and public verifiers. Our scheme does not need to divide users into the original one and newcomers. All the users work in one group and each of them is allowed to access the shared data. Public verifier, role often taken by third-party auditor, can also be any other entities that have no interests involved in data to be audited. Cloud service provider offers storage for shared data, but not like previous works, it does not store meta data used for verification. Distributed ledger of blockchain network take over this duty instead. All of the three entities join in blockchain network and manage shared data via smart contracts.

SYSTEM MODULES

- KeyGen
- SigGen
- Modifying
- Deleting

MODULE DESCRIPTION

KeyGen

Let G_1 and G_2 be multiplicative cyclic groups of prime order q and g_1, g_2 be their generators respectively. Let e: $e: G_1 \times G_2 \rightarrow G_2$ be bilinear map. Choose two different collision-resistant hash functions that fulfill $H_1:(0,1)^* \rightarrow Z_q$ and $H_2:(0,1)^* \rightarrow G_1$. The group chooses a private-public key pair for submission $\pi \leftarrow Z_q, \rho = g_2^{x_i}$. For each user u_i, pick random element $x_i \leftarrow Z_q$ as its own private key, and compute the public key following $y_i = g_1^{x_i}$.

SigGen

Denote the total number of current members in group as d. The public keys of group members are $(y_1, y_2, \ldots, y_d)$. Given a data block m to be uploaded, its owner u_j computes its ring signature in following way:

1) Pick (n-1) users randomly from all the group members to form a n-member ring $L = (u_1, u_2, \ldots, u_n), 1 \leq j \leq n.$
2) Compute $h = H_2(L).$ And $\tilde{y} = h^{x_j}$.
3) Choose random element $\lambda \leftarrow y_q$, and compute $c_{i+1} = H_1(L, \tilde{y}, g_1^{\lambda}, h^{\lambda})$
4) For other $u_i, i \neq j$ j in ring L, pick random element $s_i \leftarrow Z_q$, and compute $c_{i+1} = H_1\left(L, \tilde{y}, g_1^{s_i} y_i^{c_i}, h^{s_i} \tilde{y}^{c_i}\right).$
5) Finally, compute

$S_i = \lambda - x_i c_i$

$t = (c_1 g_1^m)^{\pi}$

Finally, the signature for data block m is $\sigma = (c_1, s, \ldots, s_n, \tilde{y}, t)$

Modifying

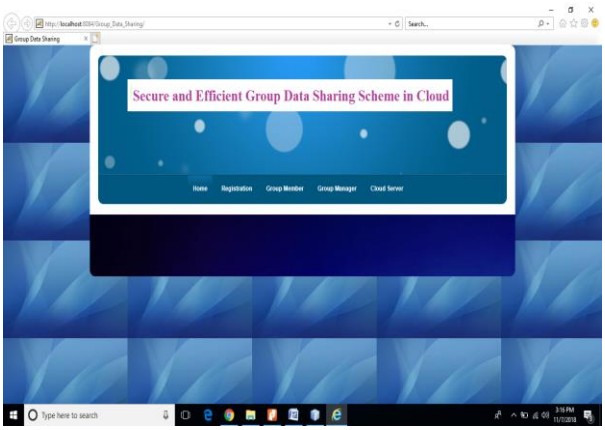
Procedure of modifying a block can be seen as uploading a new block m0 to replace the original m. To prove ownership of original block m, data owner only needs to offer the new tag σ' for checking whether $\tilde{y} = \tilde{y}^j$ holds. In this way, we ensure data sovereignty of owners without adding too much extra computation and communication overhead.

Deleting

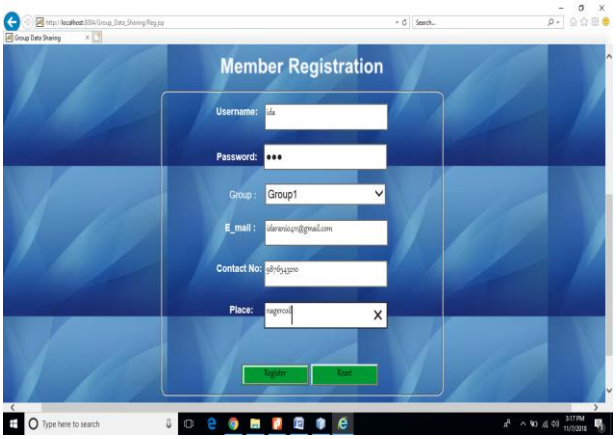
There is no new block to be uploaded in the case of deleting. Therefore, data owner needs to generate a temporary signature to prove its ownership. Data owner should choose a random message m' and generate σ' following the method in SigGen. If $\tilde{y} = \tilde{y}^j$ holds and σ' is a valid tag, the deleting request can be identified as coming from the real data owner.

IV. RESULT AND DISCUSSION

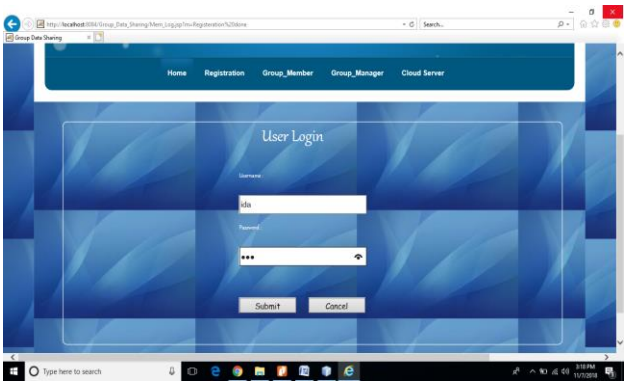
4.1 SIMULATION OUTPUT



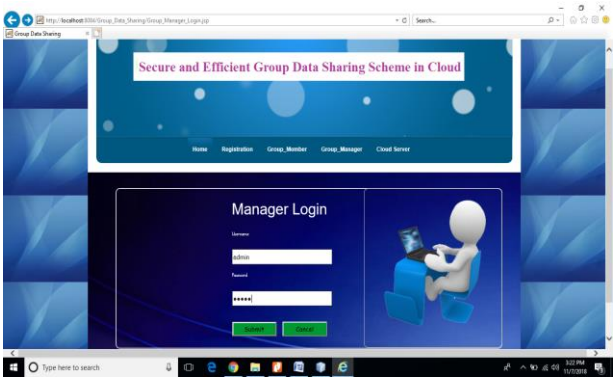
2. Home Page



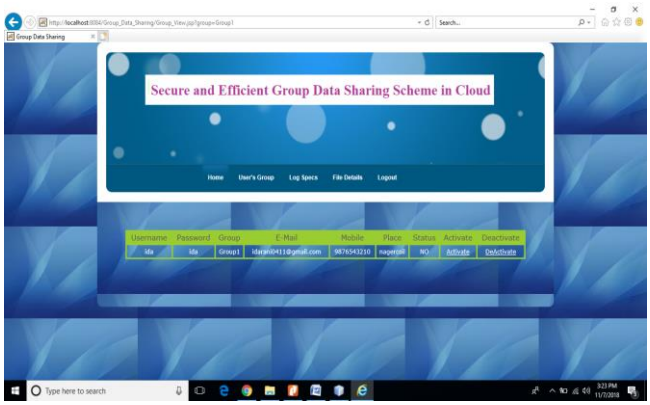
3. Data Member Registration Form



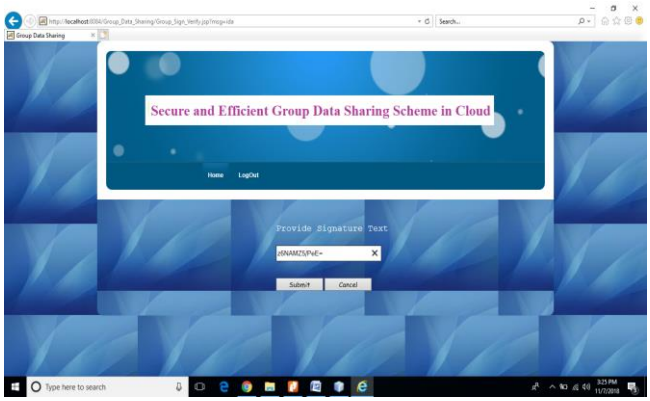
4. Data user Login Page



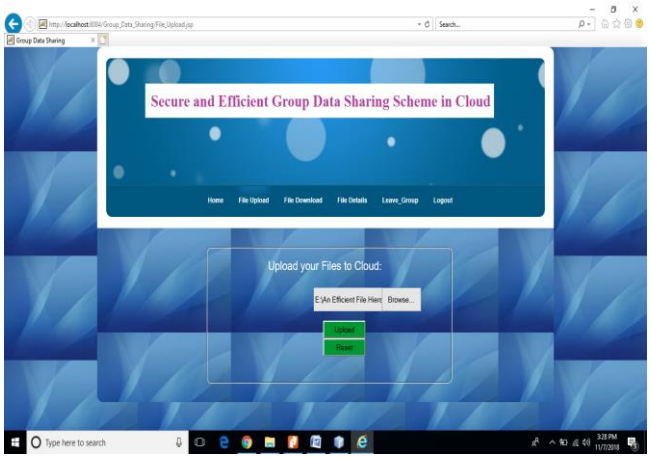
5. Manager login page



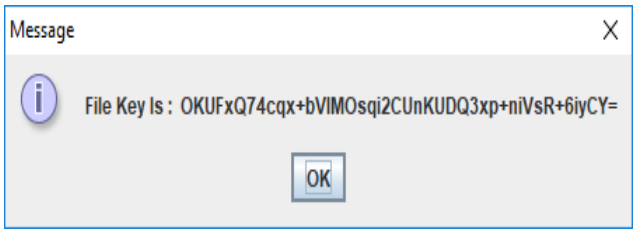
6. Group data details



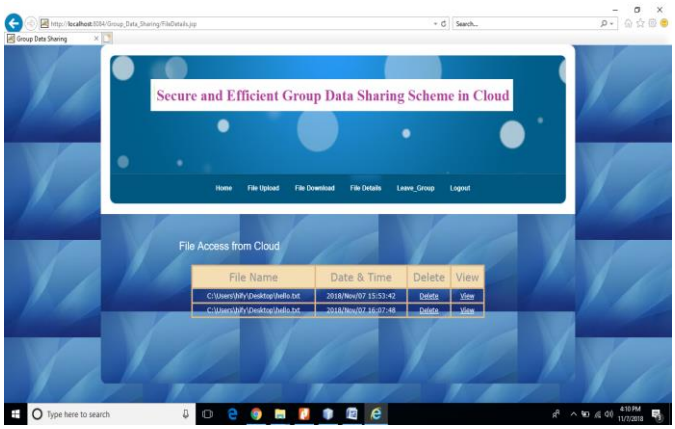
7. Provide Signature Text



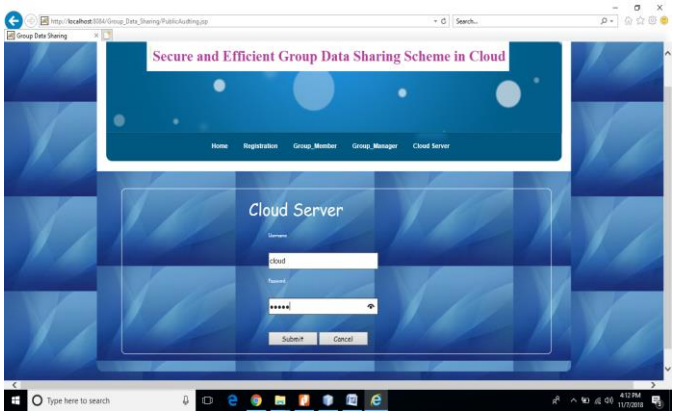
8. Upload File



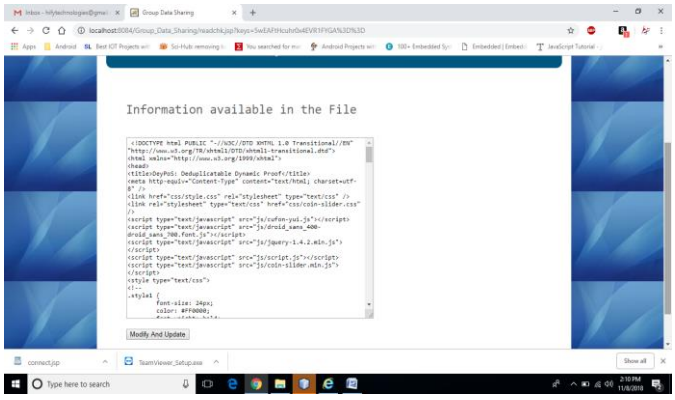
9. File Key



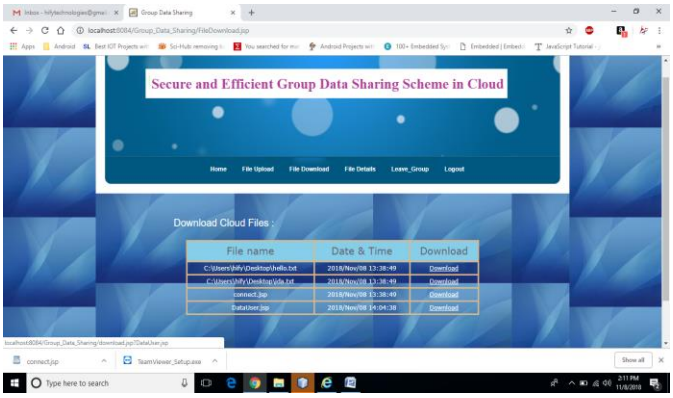
10. File Access from the Cloud



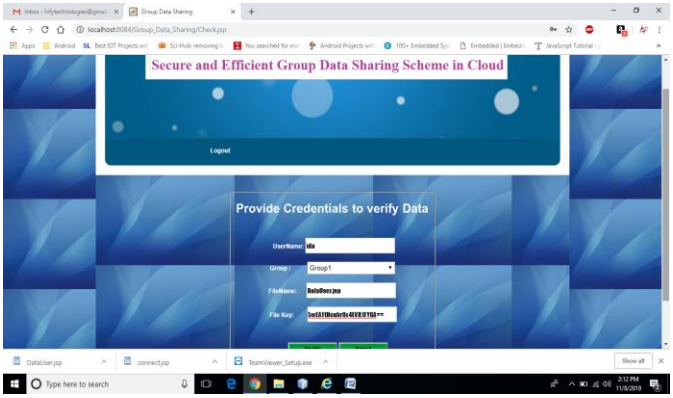
11. Cloud server login Page



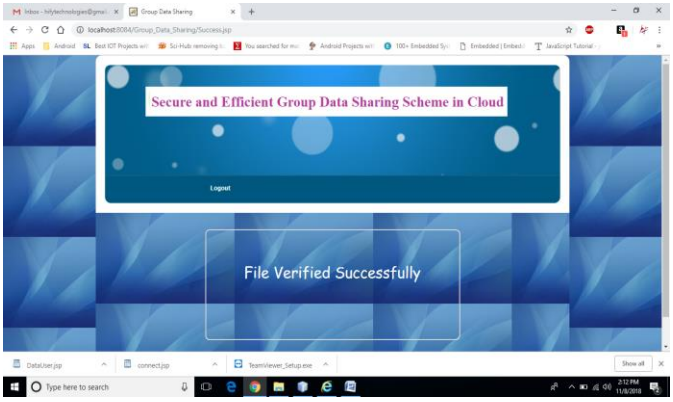
12. File Information



13. Cloud files



14. Verify data



15. Verified File

V. CONCLUSION

This paper focuses on exploring a blockchain-based PDP scheme for group shared data. We analyze the needs of group data auditing and find that resisting collusion attacks and identity privacy are the most important two issues. Blockchain network and smart contracts offer a potential solution of reliable outsourced computation, which makes tag generation and integrity verification free from collusion attack, and linkable ring signature provides support for anonymous data auditing. We design a novel method of LHARS scheme as well as a blockchain-based PDP scheme. Security analysis and performance evaluation prove that our scheme is both secure and efficient.

Our main aim is to securely save the data on the cloud and access it securely. This can be used in the business organizations . As efficient access control is achieved with respect to group signature technique. Like in the business organization there are various departments so any confidential file can only be sent to the selected users and this will be anonymous to the others.

REFERENCES

[1] Dongmin Kim , Kee Sung Kim X "Privacy-Preserving Public Auditing for Shared Cloud Data With Secure Group Management", Volume 10, April 29, 2022.

[2] Rudniy, "Data warehouse design for big data in academia," Computers, Materials & Continua, vol. 71, no. 1, pp. 979–992, 2022.

[3] Berguiga and A. Harchay, "An IoT-based intrusion detection system approach for TCP syn attacks," Computers, Materials & Continua, vol. 71, no. 2, pp. 3839–3851, 2022.

[4] R. Jia, Y. Xin, B. Liu and Q. Qin, "Dynamic encryption and secure transmission of terminal data files," Computers, Materials & Continua, vol. 71, no. 1, pp. 1221–1232, 2022.

[5] M. Naor and G. N. Rothblum, "The complexity of online memory checking, " Journal of the ACM, vol. 56, no. 1, pp. 1–46, 2009.

[6] Oprea, M. K. Reiter and K. Yang, "Space-efficient block storage integrity," in Proc. of 12th Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, 2005.

[7] J. Almutairi and M. Aldossary, "Exploring and modelling IoT offloading policies in edge cloud environments," Computer Systems Science and Engineering, vol. 41, no. 2, pp. 611–624, 2022.

[8] B. Han, H. Li and C. Wei, "Blockchain-based distributed data dntegrity auditing scheme," in Proc. of 2021 IEEE 6th Int. Conf. on Big Data Analytics (ICBDA), Xiamen, China, pp. 143–149, 2021.

[9] Y. Yuan, J. Zhang, W. Xu and Z. Li, "Identity-based public data integrity verification scheme in cloud storage system via blockchain," the Journal of Supercomputing, vol. 78, pp. 8509–8530, 2022.

[10] Y. Li, Y. Yu, R. Chen, X. Du and M. Guizani, "IntegrityChain: Provable data possession for decentralized storage," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1205–1217, 2020.

[11] Q. Mei, H. Xiong, Y. C. Chen and C. M. Chen, "Blockchain-enabled privacy-preserving authentication

mechanism for transportation CPS with cloud-edge computing," IEEE Transactions on Engineering Management, in press, DOI 10.1109/TEM.2022.3159311.

[12] J. K. Liu, V. K. Wei and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in Proc. of Australasian Conf. on Information Security and Privacy, Sydney, Australia, pp. 325–335, 2004.

[13] C. Li, Y. Tian, X. Chen and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," Information Sciences, vol. 546, pp. 253–264, 2021.

[14] C. Li, G. Xu, Y. Chen, H. Ahmad and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled internet of things," Computer, Material & Continua, vol. 61, no. 2, pp. 711–726, 2019

[15] L. Jiang and Z. Fu, "Privacy-preserving genetic algorithm outsourcing in cloud computing," Journal of Cyber Security, vol. 2, no. 1, pp. 49–61, 2020.

[16] Y. Su, Y. Li, K. Zhang, and B. Yang, ''A privacy-preserving public integrity check scheme for outsourced EHRs,'' Inf. Sci., vol. 542, pp. 112–130, Jan. 2021.