CERTIFICATELESS PUBLIC VERIFICATION SCHEME AGAINST PROCRASTINATING AUDITORS

Department of Computer Science And Engineering,
Santhiram Engineering College, Nandyal, A.P, India.

J.David Sukeerthi Kumar,Asst Prof **david.cse@srecnandyal.edu.in**
V.P.Bharathi **bharathi22031998@gmail.com**
P.Alekhya **alekhyapaluru501@gmail.com**
K.Hemantha Sandhya **hemanthasandhya741@gmail.com**
B.Latha Shravani **lathashravani22@gmail.com**
M.Asmitha **asmitha.asmi31@gmail.com**

Abstract **- Cloud storage services provide several significant benefits for managing and deploying the data by users. But there are some security concerns. One among them is data integrity. Usually, a third-party auditor is employed to verify the data integrity on behalf of the users. However, these schemes are vulnerable to some procrastinating auditors who may delay the verifications. Basically, these schemes are constructed on the public key infrastructure (PKI), and they face the problem of certificate management. This paper focuses on certificateless public verification scheme against procrastinating auditors (CPVPA) by using block chain technology. Main idea is to allow the auditors to verify each transaction and record them into a block chain. Basically, transactions on the block chain are time-sensitive; the verification is going to be time-stamped after the corresponding transaction is recorded. Hence, it ensures the users to know whether the verifications are done at the prescribed time. In addition to this, CPVPA is built on certificateless cryptography, and it is free from the problem of certificate management. We proposed rigorous proofs to explain the CPVPA security and evaluated the performance to show the efficiency of CPVPA.**

Index Terms - Cloud computing, Data integrity, Certificateless public verification, Procrastinating auditors, Block chain.

I. INTRODUCTION

Because of the various cloud services provided, users usually outsource and access their data whenever required. However, there are some security issues. One among them is data integrity. Users worry about their data whether it is well outsourced and maintained on cloud servers. The outsourced data is always put at the risk of data integrity. One such example is, the data may be corrupted or some part of data may be deleted to decrease the storage costs. In addition this, the attackers may tamper the outsourced data for their personal reasons. Hence data integrity is the need of the hour and it should be verified periodically.

There are several Public verification techniques that enable users to outsource the data integrity verification via dedicated third-party auditor. The auditor periodically checks the data, and informs the users about the integrity. Usually in these public verification schemes, the auditor is assumed to be honest and reliable. If the auditor is compromised, these schemes would be invalidated. For example, a procrastinating auditor may always generate a good integrity report without performing the verification to avoid the verification costs. In such a way, the auditor is virtually non-existent.

II. LITERATURE SURVEY

Homomorphic encryption has been used previously for third-party cloud-computing services. More recent studies have considered challenges associated with the use of homomorphic encryption in closed-loop control of physical systems, such as maintaining stability and performance, albeit without considering timing concerns [1]. Most query service providers, including the big ones (e.g., Google, Amazon, and so on) are suffering from intensive attacks launched by insiders or outsiders. As a consequence, processing various queries in IoT without compromising the data and query privacy is an urgent and challenging issue [2]. To deal with the privacy challenges, differential privacy has been widely discussed as one of the most popular privacy-enhancing techniques. However, with today's differential privacy techniques, it is impossible to generate a sanitized dataset that can suit different algorithms or applications regardless of the privacy budget. In other words, in order to adapt to various applications and privacy budgets, different kinds of noises have to be added, which inevitably incur enormous costs for both communication and storage. To address the above challenges, in this, they propose a novel scheme for outsourcing differential privacy in cloud computing, where an additive homomorphic encryption (e.g., Paillier encryption) is employed to compute noise for differential privacy by cloud servers to boost efficiency [3]. Ever-increasing transaction costs, serious network congestion, and low transaction rates in the current block chain systems restrict their extensive use. The SVLP merely employs a digital signature algorithm and a one-way function and has similar security comparing to existing block chain systems, such as Bit coin and Ethereum. It is of ultra-low power consumption, since the payers and payees only need one-way functions to achieve multiple transactions, instead of the costly digital signature algorithms [4]. Few papers proposed an efficient and geometric range query scheme (EGRQ) supporting searching and data access control over encrypted spatial data. They employed secure KNN computation, polynomial fitting technique, and order-preserving encryption to achieve secure, efficient, and accurate geometric range query over cloud data [5]. Few papers proposed a privacy-

preserving Attribute-Keyword based data Publish-Subscribe (AKPS) scheme for cloud platforms. Specifically, in order to protect the privacy of the published data against the cloud server and other none-subscribers, they employed the attribute-based encryption with decryption outsourcing to encrypt the published data, such that the publishers can control the data access by themselves and the major decryption overhead can be shift from the subscribers' devices to the cloud server [6]. Few papers dealt with the encryption where the encryption key is associated with the content itself and the private decryption keys are distributed to the authorized consumers. To deal with the security requirements for content-based encryption, we define a security model that captures existential unforgeability and semantic security [7].

III. Problem Statement

In the existing system, the user is the data owner, who outsources her/his data to the cloud server and accesses the outsourced data as needed. After data outsourcing, the user employs a TPA, agrees a verification period with TPA, and let TPA periodically verify the data integrity. The cloud server is subject to the cloud service provider, and provides cloud storage services. It has not only significant storage space, but also a massive amount of computing power. TPA works for the user. It feeds back the verification results to the user and the cloud server, and detects the data corruption as soon as possible. The communication between TPA and other entities is authenticated. The KGC is controlled by an authority. It generates a partial private key for the user by using the user's identity.

IV. Proposed Method

In the proposed system, we explain, How to resist the procrastinating TPA without introducing any trusted participant. Existing public schemes assume that TPA would perform the data integrity verification at the prescribed time. However, the procrastinating auditor would not detect the data corruption as soon as possible, and it might be too late to recover the data loss or damage. Such procrastination is hardly to be detected by the user without a trusted participant's help.

This paper also explains how to avoid the certificate management. As discussed before, certificate management is cumbersome and costly in practice. Enabling TPA to verify the data integrity without managing users' certificates could be economic and favorable in practice. To enable secure verification of outsourced data integrity in cloud storage under the aforementioned model, the following objects should be achieved.

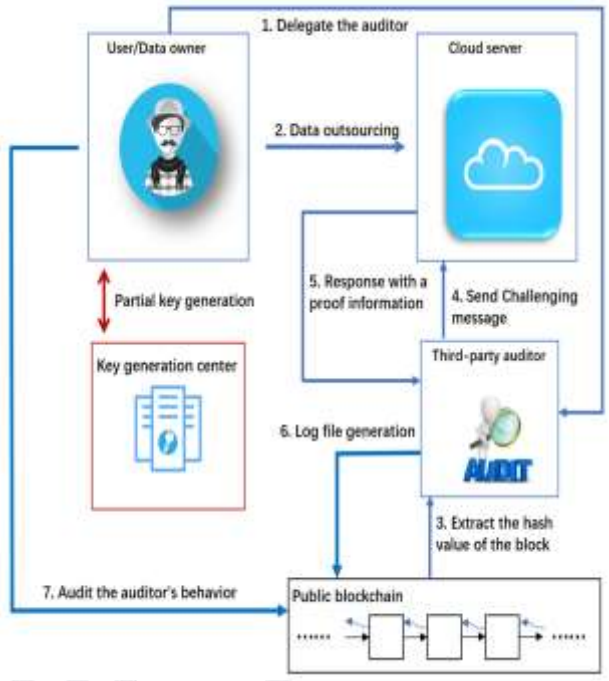

Fig. 1 Architecture.

The communication and computation overhead should be as efficient as possible; TPA is able to verify the data integrity without managing the users' certificates and bearing a priori bound on the number of verification interactions; TPA should be stateless, and is not required to maintain and update state during verification.

When a cloud server passes the TPA's verification, it must possess the specified data intact; a malicious TPA and a procrastinating TPA cannot deceive the user; Collusion between any two participants cannot break the security of the proposed scheme.

V. IMPLEMENTATION

A. *Modules*

1) Data Owner: The Data Owner is accountable for the data within a specific Data Domain. They are responsible to ensure that information within their Domain is governed across systems and lines of business. Data Owners usually are part of the Steering Committee, either as voting or non-voting members.

2) Cloud Server: The cloud is commonly used to refer to several servers connected to the internet that can be leased as part of a software or application service. Cloud-based services can include web hosting, data hosting and sharing, and software or application use.

'The cloud' can also refer to cloud computing, where several servers are linked together to share the load. This means that instead of using one single powerful machine, complex processes can be distributed across multiple smaller computers.

3) Key Generation Center: The class of centralized group key management protocols is the most widely used group key management protocols. Harney et al. Proposed a group key management protocol that requires O(n), where n is the size of group, encryptions to update a group key when a user is evicted or added if backward and forward secrecy are

required. A set of scalable hierarchical structure-based group key protocols have been proposed..

4) Third Party Auditor: A third-party audit occurs when a company has decided that they want to create a quality management system (QMS) that conforms to a standard set of requirements, such as ISO 9001, and hire an independent company to perform an audit to verify that the company has succeeded in this endeavor. These independent companies are called certification bodies or registrars, and they are in the business of conducting audits to compare and verify that the QMS meets all the requirements of the chosen standard, and continues to meet the requirements on an ongoing basis. They then provide certification to companies that they approve. This can be used to give customers of the certified company confidence that the QMS meets the requirements of the chosen standard.

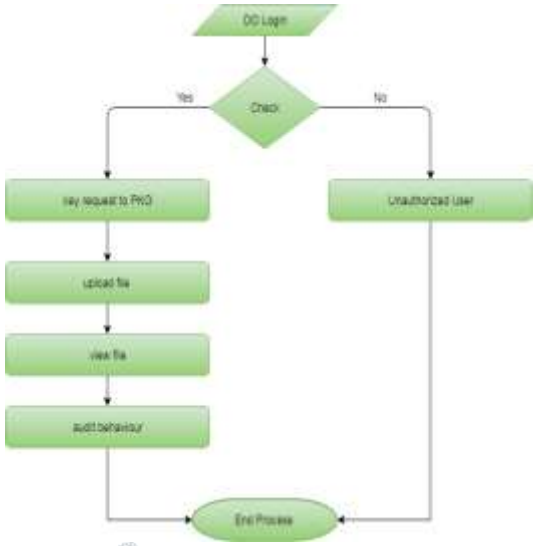

Fig. 2 Data Owner.

B. Algorithm

SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the strongest hash functions available. SHA-256 is not much more complex to code than SHA-1, and has not yet been compromised in any way. The 256-bit key makes it a good partner-function for AES. It is defined in the NIST (National Institute of Standards and Technology) standard 'FIPS 180-4'. NIST also provide a number of test vectors to verify correctness of implementation. SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash. The Sha-256 algorithm is based on the Merkle-Damgard construction method, according to which the initial index is divided into blocks immediately after the change is made, and those, in turn, into 16 words. Mining uses SHA-256 as the proof-of-work algorithm. SHA-256 is used in the creation of bit coin addresses to improve security and privacy.

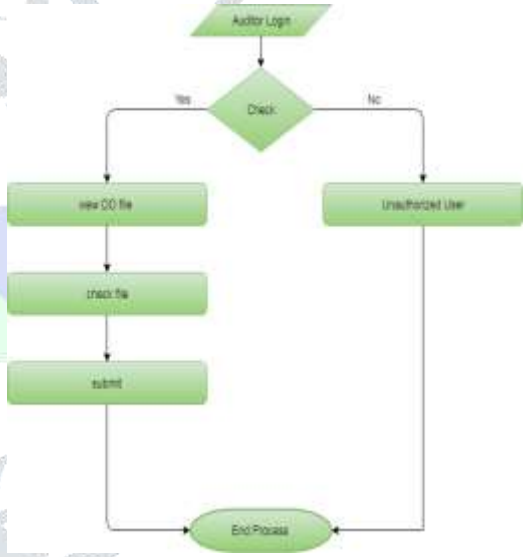

Fig. 3 Auditor.

VI. RESULTS

Upon running the programs, a home page with the admin, data owner, KGC and auditors get displayed. Initially the data owner needs to get registered with the credentials. Then with these details, the data owner gets sign in. For uploading the file, user i.e., the data owner requires a key. So the user needs to put a request to the KGC for the key. For requesting the key from the cloud service provider, the user need to enter name, e-mail id and provide a message for reference. Then submit all the details. If we check the cloud service response, the status will be pending. In the auditor behaviour, we can observe the blocks connected with the hash code of previous and present blocks. Next, login into the KGC with the necessary credentials. A page gets displayed. Now click on send key (message, what you have provided in the cloud service request). Finally, click on submit. Now the user gets a public

key to his/her mail. Then to upload the file, the user needs to enter the public key and secret key. The user can finally upload the required file. Then click on submit, after uploading. Now, it's the work of the auditor to check whether the uploaded file is true or fake or corrupted. For this, the auditor logins with the credentials and verify the file. If it is correct, he sends true. Else, he sends false. The data owner can check the file status. Finally, the admin can maintain the list of data owners, auditors and the uploaded contents.

The following are the various screenshots obtained in the execution and performance evaluation.

Fig. 4 Column chart

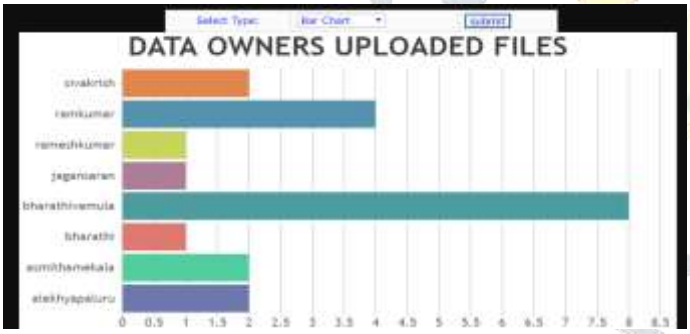

Fig. 5 Bar chart

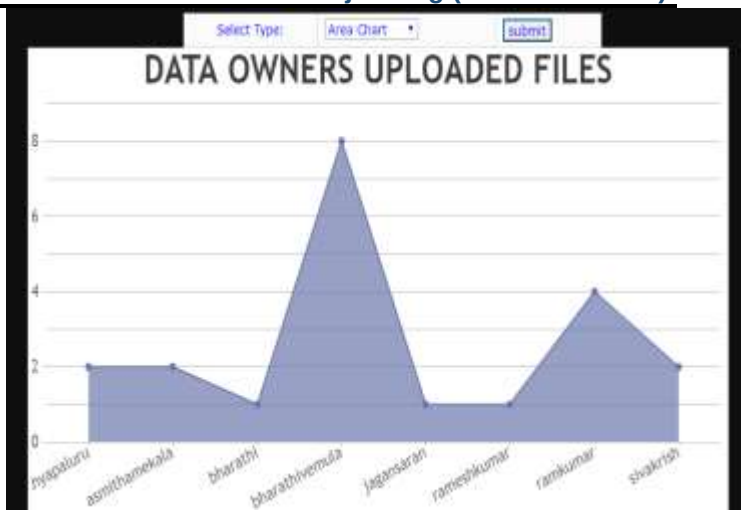

Fig. 6 Area chart

Fig. 7 Spline chart

Fig. 8 Line chart

VII. CONCLUSION

In this paper, we have proposed a certificate less public verification scheme against the irresponsible auditor. This paper utilizes the on-chain currencies, where each verification performed by the auditor is combined into a transaction on the block chain. Additionally, CPVPA is free from the problem of

certificate management. The security analysis demonstrates that CPVPA provides the strongest security guarantee. We have also performed a comprehensive performance analysis, which explains that CPVPA is constant and efficient in terms of communication overhead.

VIII. Future Scope

As the outsourced data processing (e.g., outsourced computation and searching over encrypted data) has also played an important role in current information age, we will explore the integration of block chain into existing schemes which should have a deep impact on outsourced data processing.

References

[1] 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, 2018.

[2] 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, 2018.

[3] 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.

[4] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on block chain," Future Generation Computer Systems, 2019.

[5] 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, 2019.

[6] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacy preserving attribute-keyword based data publish-subscribe service on cloud platforms," Information Sciences, 2017.

[7] H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing content-centric networks with content-based encryption," Journal of Network and Computer Applications, 2019.