International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST12182111

A Privacy-Preserving Outsourcing Data Storage Scheme with Oruta Data Auditing

Mrs. A. Kalaiyarasi, Dr. E. Punarselvam, B. Lavanya, A. Nivetha, A. Salai Amirtha Lakshmi, S. Kowsalya
Department of Information Technology Muthayammal Engineering College (Autonomous), Tamilnadu, India

Article Info
Volume 8, Issue 2
Page Number : 620-625

Publication Issue
March-April-2021

Article History
Accepted : 25 April 2021
Published : 30 April 2021

ABSTRACT

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. With cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost. With cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. In this project, we propose Oruta, a privacy-preserving auditing scheme for shared data with large groups in the cloud. We utilize ring signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity of the signer on each block. We can implement the batch auditing scheme to perform efficient public auditing to protect both identity and data privacy in cloud environments.

Keywords : Cloud Computing, IT services, Storage, Privacy-Preserving Auditing Scheme.

I. INTRODUCTION

Cloud computing is the long-dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third-party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third-party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, here utilize and uniquely combine the public key-based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, here further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

II. PROPOSED SYSTEM

We propose a privacy-preserving and auditing-supporting outsourcing data storage scheme by using encryption and digital watermarking. Logistic map-based chaotic cryptography algorithm is used to preserve the privacy of outsourcing data, which has a fast operation speed and a good effect of encryption. Local histogram shifting digital watermark algorithm is used to protect the data integrity which has high payload and makes the original image restored listlessly if the data is verified to be integrated. Experiments show that our scheme is secure and feasible. We propose an outsourcing data storage scheme supporting privacy-preserving and auditing service.

III. MODULES DESCRIPTION

A. Cloud resource allocation

Cloud data storage service three different entities such as the cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources; the third-party auditor, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. To provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner.

B. HARS scheme

HARS contains three algorithms: KeyGen, RingSignandRingVerify. In KeyGen, each user in the group generates his/her public key and private key. In RingSign,a user in the group is able to generate a signature on a block and its block identifier with his/her private key and all the group members' public keys. Block identifiers a string that can distinguish the corresponding block from others. A verifier is able to check whether a given block is signed by a group member in Ring Verify.

C. Data integrity analysis

TPA checks the correctness of data storage to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact to ensure that the TPA cannot derive users' data content from the information collected during the auditing process. And implement the batch auditing scheme to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

D. Batch auditing

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. In this module, to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

E. Evaluation criteria

Evaluating the performance and this project enables to support scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner and to perform the duplicate check upon receiving the duplicate request from users.

IV. IMPLEMETATION

To achieve privacy-preserving public auditing, we propose to uniquely integrate the Homomorphic linear authenticator with random masking technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server. With the establishment of privacy-preserving public auditing, the TPA may concurrently handle multiple auditing upon different users' delegation. The individual auditing of these tasks for the TPA can be tedious and very inefficient.

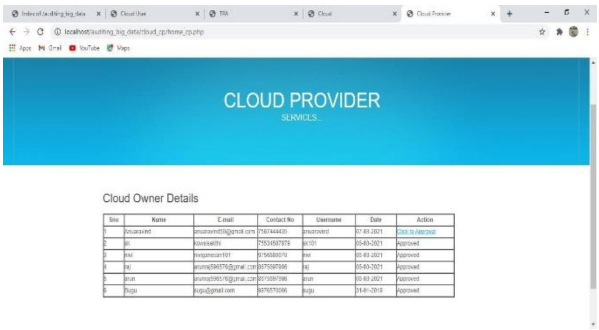

FIG 1: USER APPROVAL

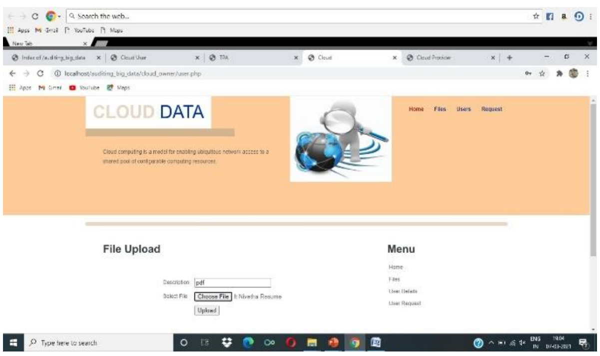

FIG 2: USER FILE UPLOAD

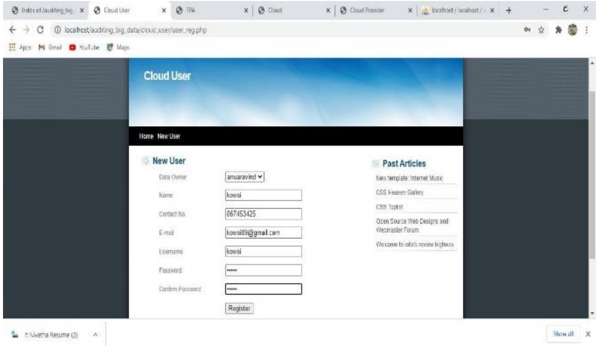

FIG 3: NEW USER REQUEST

FIG 4: DATA OWNER APPROVES USER REQUEST

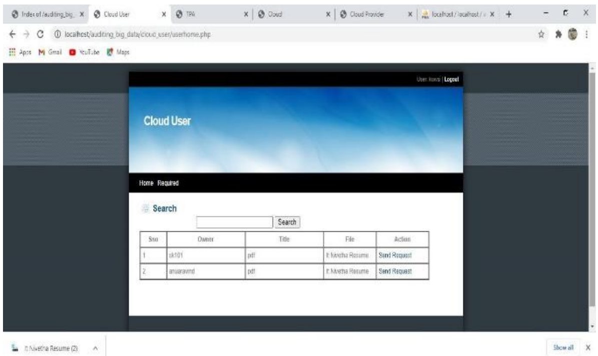

FIG 5: REQUESTING FILE TO DATA OWNER

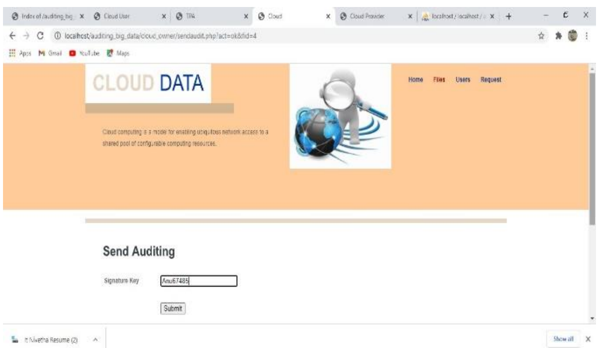

FIG 6: DATA OWNER SEND FILE FOR AUDITING

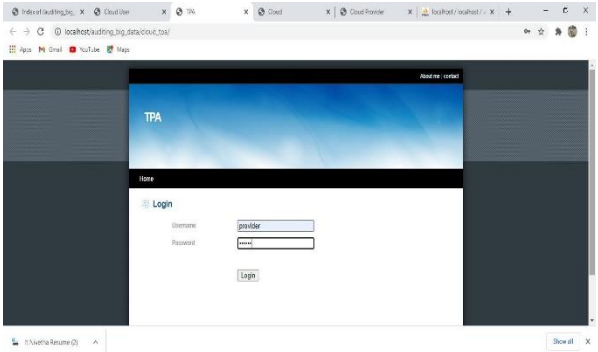

FIG 7: THIRD PARTY AUDITOR LOGIN

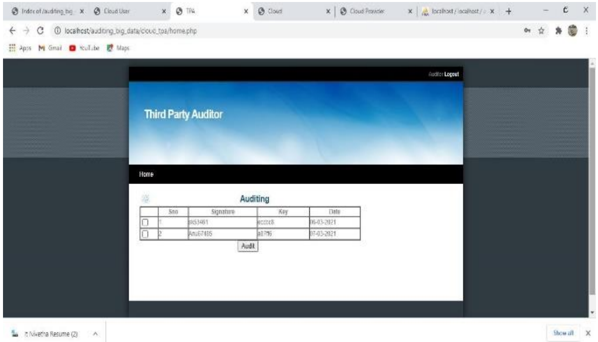

FIG 8: AUDITOR APPROVES THE FILE

V. CONCLUSION

Cloud Computing is gaining popularity and advancement day-by-day. But still the security threat hinders the success of Cloud Computing. In this paper, some of the privacy threats are addressed and the techniques to overcome them are surveyed. While some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy. Also, approaches to preserve privacy at the time of public auditing are also discussed. Thus, to conclude it is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time. Data freshness is essential to protect against misconfiguration errors or rollbacks caused intentionally. We can develop an authenticated file system that supports the migration of an enterprise-class distributed file system into the cloud efficiently, transparently and in a scalable manner.

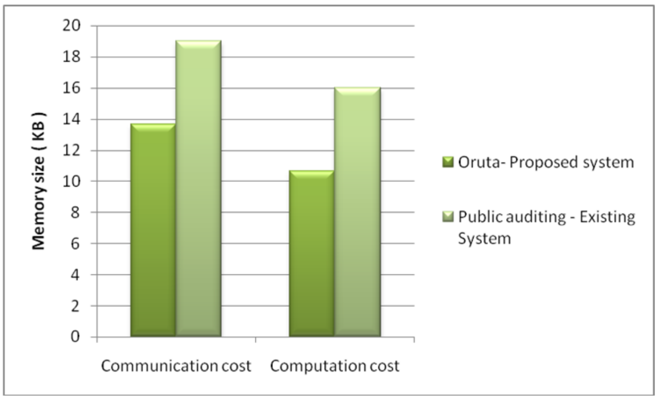

FIG 9: RESULT

VI. FUTURE ENHANCEMENTS

In the future authenticated in the sense that enables an enterprise tenant to verify the freshness of retrieved data while performing the file system operations. The user must be given complete access control over the published data. Also, powerful security mechanisms must always supplement every cloud application. Attaining all these would end up in achieving the long-dreamt vision of secured Cloud Computing in the nearest future. In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

VII. REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610.

[3]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data

Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[4]. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2001, pp. 552–565.

[5]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. In- ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[6]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2008, pp. 90–107.

[7]. Y. Zhu, H.Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[8]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 534–542.

[9]. D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 514–532.

[10]. D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2011, pp. 149–168.

[11]. A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical Short Signature Batch Verification," in Proc. RSA Conference, the Cryptographers' Track (CT-RSA). Springer-Verlag, 2009 pp. 309–324.

[12]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proc. ACM Conference on Computer and Communications Security (CCS), 2006, pp. 89–98.

[13]. A. Juels and B. S. Kaliski, "PORs: Proofs pfRetrievability for Large Files," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 584–597.

[14]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. International Conference on Security and Privacy in Communication Networks (SecureComm), 2008.

[15]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in Proc. ACM Conference on Computer and Communications Security (CCS), 2009, pp. 213–222.

[16]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS), 2009, pp. 1–9.

[17]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp. 31–42.

[18]. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codesbased Secure and Reliable Cloud Storage Service," in Proc. IEEE International

Conference on Computer Communications (INFOCOM), 2012.

[19]. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," in Proc. ACM Conference on Computer and Communications Security (CCS), 2011, pp. 491–500.

[20]. Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012.

Cite this article as :

Mrs. A. Kalaiyarasi, Dr. E. Punarselvam, B. Lavanya, A. Nivetha, A. Salai Amirtha Lakshmi, S. Kowsalya, "A Privacy-Preserving Outsourcing Data Storage Scheme with Oruta Data Auditing", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 620-625, March-April 2021. Available at
doi : https://doi.org/10.32628/IJSRST12182111
Journal URL : https://ijsrst.com/IJSRST12182111