IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

Identity-Based Public Integrity Auditing of Shared Data with LWE Enhanced file Protection

Prachi Apale, Sharavari Deshpande, Sudha Lokhande, Rushikesh Fulare, Prof. Nilima Dandge

Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research,

Badnera, India

ABSTRACT*:* When private data is shared among various users supported on cloud storage, it's critical to preserve the anonymity of the information/data uploader against the auditor. That is, the auditor shouldn't get data uploader's identity through the information audition. To address this problem, many PDP(Provable Data Possession) schemes with user identity privacy-persevering are proposed. However, most proposed schemes are designed with supported PKI technique which suffers from big burden of certificate management. Moreover, the auditors in most of such schemes bear heavy computation cost which results to the reduced efficiency.Also. the leakage of sensitive data is increased while outsourcing. To deal with this, the framework for a new light weight encryption (LWE) to outsource the coded data to the cloud without interjecting the sensitive information on the cloud server and maintaining the integrity, is designed. It also maintains the balance between security and computational outflow in user system to enhance integrity.

KEYWORDS*:* Cloud secure storage, identity-based cryptography, group data integrity checking, user privacy preserving, efficiency and security.

I. INTRODUCTION

Data Privacy is nothing but the privacy of personal data such as personal information, financial records, medical records, private images etc. Whereas cloud computing could be described as the storing, implementation and retrieval of the data that is stored on the cloud. There exists many common social networking applications such as Facebook, LinkedIn, Twitter etc. In today's world, social networking and cloud computing work hand in hand in various aspects. In case of the social cloud systems, the applications provides features such as authentication and user management. In order to provide these features, most organizations make use of cloud computing. With increasing growth of data, the organizations face challenges with respect to providing privacy to its users. The most common issues pertaining to cloud computing include security, integrity and availability. Various criticisms are made regarding the security and data modification. Thus, even though cloud computing is very commendable, there are certain issues with respect to the practices and policies that presently remain weak.

When any user uploads data over the cloud, it should be encrypted in such a way that other people with malicious intentions should not be able to decipher it. In case the data gets accessed by unauthorized people, they may modify the data and such tempered data could be harmful to both the sender as well the receiver. The user must then have a way to make sure that the integrity of the document, that is either sent or received is intact. To address this issue, the concept of data auditing is used with the help of a third party auditor which could also be a separate server. The auditing of the data integrity ensures that only the proper, untampered file is received by the end user.

II. RELATED WORK

Ateniese etal. (1) originally considered to check data integrity by PDP model and proposed two concrete schemes rested on RSA algorithm. Analogous to PDP, PoR model proposed by Juel and Kaliski etal. (2) has the function of ever check data integrity too. To upgrade scheme effectiveness, Shacham and Waters (2) developed a compact PoR scheme with shorter authentication label. To support dynamic operations, Ateniese etal. (3) based on symmetric key encryption designed a more flexible PDP scheme, where data blocks can be adjoined, updated and deleted. Erway etal. (4) proposed a PDP protocol with full data block dynamic operations including data insertion. To enhance dynamic operation effectiveness, Yanetal. (5) realized a PDP scheme with the new data structure. Also, Shen etal. (6) designed

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

another new data structure to realize data operations of their PDP scheme. To increase data continuity, Liu etal. (7) proposed amulti-replicas data integrity checking protocol, which supported completely dynamic data updates. Wang (8) developed an integrity checking protocol for data on multi cloud servers. Li etal. (9) further considered a more complex medium thatmulti-copies stored in multi CSP s and constructed a concrete scheme to check the integrity of all duplicates for one time. To support delegation of data checking, Wang (10) proposed a representative PDP scheme in which a commitment was used to authenticate the validity of adjudicator. Further, Yan etal. (11) strengthened the restriction of the verifier and proposed a verifier- designated PDP scheme. To maintain the data isolation, Wang etal. (12) proposed a notion of data sequestration protection and designed a public auditable PDP scheme. To get relieve of instrument operation problem, Yu etal. (13) grounded on identity- based crypto presented a PDP scheme with data sequestration protection. Shen etal. (14) proposed a PDP protocol to guarantee the sequestration of authenticators. Wang etal. (15) proposed the first PDP model for data shared in group which employed ring signature approach to create labels so as to support public auditing and user privacy conserving. Wang etal. (16) proposed a new PDP scheme for shared data with user sequestration conserving. Likewise, the scheme in (16) also supported dynamic group which allowed user to join or leave the group at any time. Liu etal. (18) designed a PDP scheme grounded on broadcast encryption (17) supporting dynamic group. Wang etal. (19) accounted the user revocation issue and proposed a PDP scheme which outsourced user cancellation to CSP by proxy resignature fashion. Yang etal. (20) designed a PDP protocol for group data with user identity sequestration and traceability. Also, Yang etal. (23) presented a scheme of shared data grounded on certificateless cryptography too. Although the scheme claimed that it was suitable to guarantee user identity, unfortunately, TPA can get the relationship of data and the public keys in the verification phase. Therefore, it didn't really realize user sequestration conserving. Wu etal. (24) presented a new PDP scheme with user privacy protection, but the communication and computation charges of the scheme were too heavy especially in the challenge phase

III. PROPOSED WORK

In this paper, the identity based public integrity auditing of shared data and LWE enhanced file protection scheme for document security is proposed. The user is worried about the authenticity of data stored in the cloud as modifications could be made by attackers. Therefore, the concept of public integrity auditing with the help of a Third Party Auditor is suggested.

In our case, we proposed an automatic auditing verification process without interference of any human being. We proposed a separate automatic TPA server which will receive integrity verification request along with the document. The TPA server will find out the hash value of requested document and send request to get the hash value of same document to the cloud server. The cloud server will send requested hash value after identity verification and the integrity of the document will be checked on TPA server. The result will be visible and accessible to the users.

Following are the three major objectives suggested in this paper.

1] To develop an online cloud based social networking system: An online based social networking system is developed where the users would be able to share documents, create groups and have effective communication.

2] To provide security using the LWE enhanced protection scheme**:**In order to ensure the security and privacy of the data that is shared by the users, it is essential to provide certain form of encryption. In this case, an LWE i.e. Light Weight Encryption enhanced file protection scheme is implemented.

3] To implement Identity-based public integrity auditing of shared data:The users would be able to send auditing request for any document they wish to check the integrity of. This auditing of the data would take place in such a way that the user's privacy would be protected.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

Flowchart of the proposed scheme:

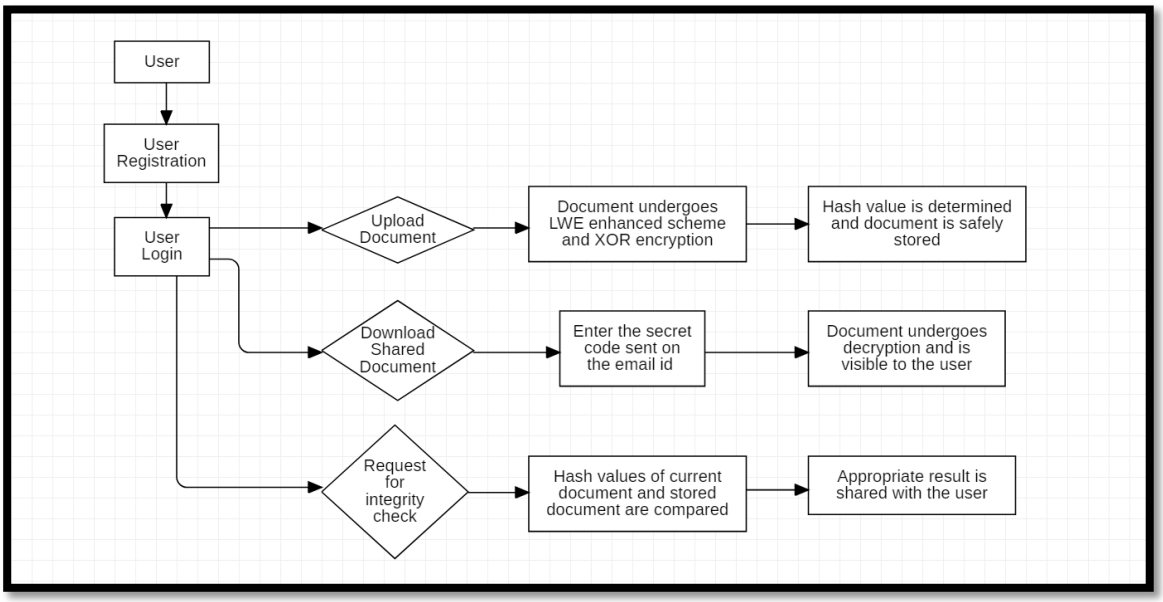

Figure 1: Flow chart – Proposed work

IV. IMPLEMENTATION

LWE Scheme:

Three entities play a significant role in this method. These entities include the file owner, the cloud server and the file receiver. The file owner i.e. the sendershares the sensitive information which includes the metadata, key etc. This is done in order to facilitate the access of the file from cloud storage. On the basis of the verification, the file users or the receivers are able to access the encrypted file from the cloud server. Some private but important information such as the user authentication details, key, metadata and index are collected from the sender or the file owner.

Steps followed in the suggested LWE enhanced file protection:

• Upload document
• Convert document into byte array
• Convert the byte array into n no of chunks
• Encrypt every chunk using XOR Algorithm and secrete key k
• Convert the chunks into base64 format
• Shuffle the chunks
• Combine the chunks and store in single file
• Create meta-data file containing chunks sequence, size of file, secrete key etc
• Encrypt meta-data using XOR Algorithm
• Store the file on cloud

XOR Encryption:

The XOR algorithm mentioned in the above mentioned scheme consists of the follows steps:

- Take path of image as an input
- Take encryption key as input
- Open file for reading
- Convert file into a byte array to perform encryption easily on numeric data
- Perform XOR operation on each value in byte array

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

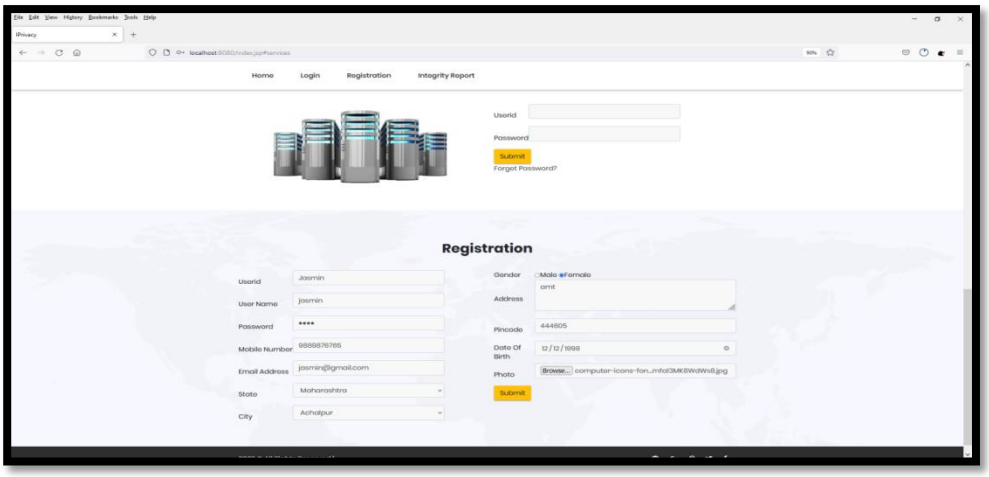

Figure 2: User Login and Registration

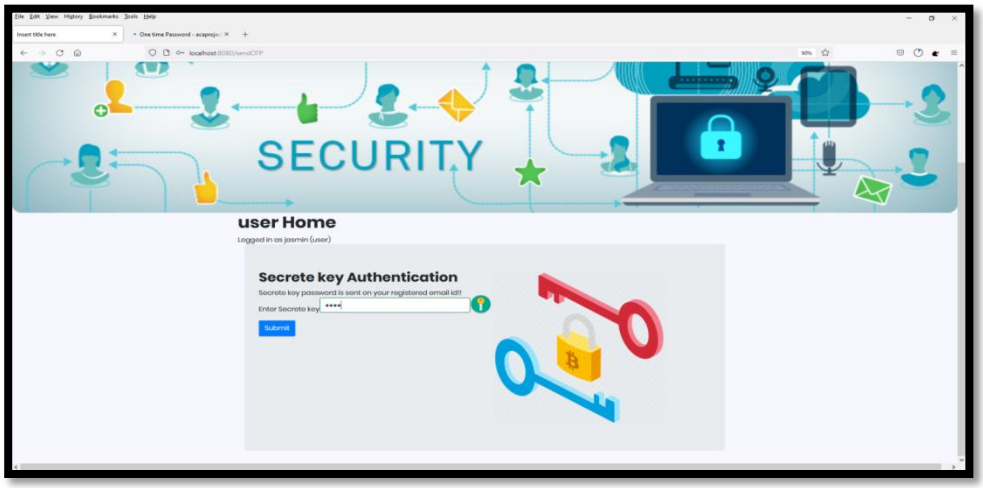

Figure 3: Accessing shared documents using the Secret Key

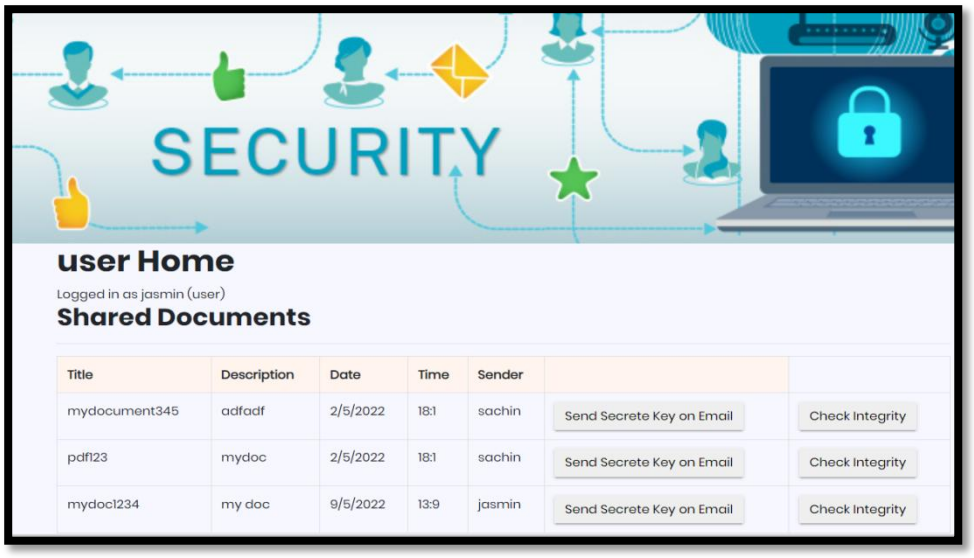

Figure 4: Requesting for Integrity Auditing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

Figure 5: The Integrity Report as visible to the users

V. CONCLUSION

In cloud computing and various associated services, along with storing the data, it is also shared to multiple users. The LWE scheme that is proposed and mentioned, ensures the privacy of the user in the system of the file uploader. It assures confidentiality due to encryption and integrity due to two time encryption that is included in the client system (file owner) and the cloud server.

Hence, the auditing scheme that is used,performs efficient public auditing to protect both identity and data privacy in cloud environment and works to implement double encryption approach to provide additional security in cloud storage environments.

REFERENCES

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, andD.Song,‘‘Provabledatapossessionatuntrustedstores,’’inProc.14th ACMConf.Comput.Commun.Secur.(CCS),Alexandria,VA,USA,2007, pp. 598–609.
2. A. Juels and B. S. Kaliski, ‘‘PORs: Proofs of retrievability for large files,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584–597.
3. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ‘‘Scalable and efficient provable data possession,’’ in Proc. 4th Int. Conf. Secur. Privacy Commun. Netowrks (SecureComm), 2008, pp. 1–10.
4. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ‘‘Dynamic provable data possession,’’ in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), 2009, pp. 26–222.
5. H. Yan, J. Li, J. Han, and Y. Zhang, ‘‘A novel efficient remote data possession checking protocol in cloud storage,’’IEEETrans.Inf.Forensics Security, vol. 5, no. 1, pp. 78–88, Jan. 2017.
6. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ‘‘An efficient public auditing protocol with novel dynamic structure for cloud data,’’ IEEE Trans. Inf. Forensics Security, vol. 5, no. 10, pp. 2402–2415, Oct. 2017.
7. C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, ‘‘MuRDPA: Top-down leveled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud,’’ IEEE Trans. Computer., vol. 64, no. 9, pp. 2609–2622, Sep. 2015.
8. H. Wang, ‘‘Identity-based distributed provable data possession in multi cloud storage,’’ IEEE Trans. Services Computer., vol. 8, no. 2, pp. 328–340, Mar. 2015.
9. J.Li,H.Yan, and Y.Zhang,‘‘Efficient identity-based provable multi-copy data possession in multi-cloudstorage,’’IEEETrans.CloudComput.,early access, Jul. 16, 2019, doi: 10.1109/TCC.2019.2929045.
10. H.Wang,‘‘Proxy provable data possession in public clouds,’’IEEE Trans. Services Computer, vol. 6, no. 4, pp. 551–559, Oct. 206.
11. [11] H. Yan, J. Li, and Y. Zhang, ‘‘Remote data checking with a designated verifier in cloud storage,’’ IEEE Syst. J., vol. 14, no. 2, pp. 1788–1797, Jun. 2020.
12. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy preserving public auditing for secure cloud storage, ’’IEEE Trans. Computer., vol. 62, no. 2, pp. 362–375, Feb. 206.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004138|

13. Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, ‘‘Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage, ’’IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 767–778, Apr. 2017.
14. W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, ‘‘Remote data possession checking with privacy-preserving authenticators for cloud storage,’’ Future Gener. Comput. Syst., vol. 76, pp. 66–145, Nov. 2017.
15. B. Wang, B. Li, and H. Li, ‘‘Knox: Privacy-preserving auditing for shared datawithlargegroupsinthecloud,’’inProc.10thInt.Conf.Appl.Cryptogr. Netw. Secur. (ACNS), 205, pp. 507–525.
16. [16] B.Wang,H.Li,andM.Li,‘‘Privacy-preserving public auditing for shared cloud data supporting group dynamics,’’ in Proc.IEEE Int.Conf.Commun. (ICC), Jun. 206, pp. 1946–1950.
17. [17] L. Chen, J. Li, and Y. Zhang, ‘‘Anonymous certificate-based broadcast encryptionwithpersonalizedmessages,’’IEEETrans.Broadcast.,vol.66, no. 4, pp. 867–881, Dec. 2020, doi: 10.1109/TBC.2020.2984974. [18] X. Liu, Y. Zhang, B. Wang, and J. Yan, ‘‘Mona: Secure multi-owner data sharing for dynamic groups in the cloud,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 206.
18. [19] B. Wang, B. Li, and H. Li, ‘‘Panda: Public auditing for shared data with efficient user revocation in the cloud,’’ IEEE Trans. Services Computer., vol. 8, no. 1, pp. 92–106, Jan. 2015.
19. [20] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ‘‘Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,’’ J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016.
20. H. Yan and W. Gui, "Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving," in IEEE Access, vol. 9, pp. 45822-45831, 2021, doi: 10.1109/ACCESS.2021.3066497.
21. M. Sankari, P. Ranjana and D.Venkata Subramanian “iPrivacy: LWE Enhanced image protection over cloud storage” in IEEE I-SMAC Dec 2019, DOI:10.1109/I-SMAC47947.2019.9032452
22. Amit Agnihotri, E. Anupriya, Sachin Soni, Saurabh Babelay, “ Encryption using XOR based Extended Key for Information Security”,International Journal on Computer Science and Engineering, January 2011.
preserving authenticators for cloud storage,’’
23. H. Yang, S. Jiang, W. Shen, and Z. Lei, ‘‘Certificateless provable group shared data possession with comprehensive privacy preservation for cloud storage,’’ Future Internet, vol. 10, no. 6, p. 49, Jun. 2018.
24. G. Wu, Y. Mu, W. Susilo, F. Guo, and F. Zhang, ‘‘Privacy-preserving certificateless cloud auditing with multiple users,’’ Wireless Pers. Commun., vol. 106, no. 3, pp. 1161–1182, Jun. 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details