IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

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

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003186

A Lightweight Secure Auditing Scheme for Shared Date in Cloud Storage

Dr.S.Soundararajan[1], Harini K M [2], Lakshmipurapu Seemaa Sumana Sree[3], Thummagunta Likhitha[4]

Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1]

U.G. Students, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2,3,4]

ABSTRACT: With the fame of distributed computing, cell phones can store/recover individual information from anyplace whenever. Thusly, the information security issue in versatile cloud turns out to be increasingly extreme and avoids advance improvement of portable cloud. There are considerable investigations that have been led to enhance the cloud security. Be that as it may, the vast majority of them are not pertinent for portable cloud since cell phones just have restricted figuring assets and power. Arrangements with low computational overhead are in incredible requirement for versatile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for portable distributed computing. It receives CP-ABE, an entrance control innovation utilized in typical cloud condition, however changes the structure of access control tree to make it appropriate for versatile cloud situations. LDSS moves a huge bit of the computational escalated get to control tree change in CP-ABE from cell phones to outside intermediary servers. Besides, to diminish the client repudiation cost, it acquaints property depiction fields with actualize sluggish denial, which is a prickly issue in program based CP-ABE frameworks. The test results demonstrate that LDSS can adequately decrease the overhead on the cell phone side when clients are sharing information in portable cloud conditions.

KEYWORDS:LDSS, CP-ABE, Cloud

I. INTRODUCTION

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. If the connection to the user is relatively close, it may be designated an edge server. Clouds may be limited to single organization (enterprise clouds), or be available to multiple organizations (public cloud).Cloud computing relies on sharing of resources to achieve coherence and economies of scale.

Advocates of public and hybrid clouds note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand, providing the **burst computing** capability: certain periods of peak demand.

II. RELATED WORKS

A. In 2015, Kan Yang; XiaohuaJia; KuiRen; Bo Zhang published a paper about "Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage System". It proposes a multi-authority ciphertext-policy attribute-based encryption-based data access control for cloud storage, in which the authors claimed that the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Unfortunately, our further analysis and investigation show that their work adopts a bidirectional re-encryption method in ciphertext updating, so a security vulnerability appears. Our proposed attack method demonstrates that a revoked user can still decrypt new ciphertexts that are claimed to require the new-version secret keys to decrypt.

B. In 2013, Piotr K; Tysowski.;M. Anwarulpublished a paper about "Hybrid Attribute- and Re-Encryption-Based

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003186

Key Management for Secure and Scalable Mobile Applications in Clouds". It proposes aOutsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honestbut-curious

C. In 2014, BoyangWang;Baochun Lipublished a paper about "A secure data self-destructing scheme in cloud computing ". It proposes a system with the rapid development of versatile cloud services, it becomes increasingly susceptible to use cloud services to share data in a friend circle in the cloud computing environment.

D. In 2014, JinboXiong;XimengLiu;ZhiqiangYao;JianfengMa;QiLi;KuiGengpublished a paper about "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud ". It proposes a system With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors.

III. PROPOSED METHODOLOGY

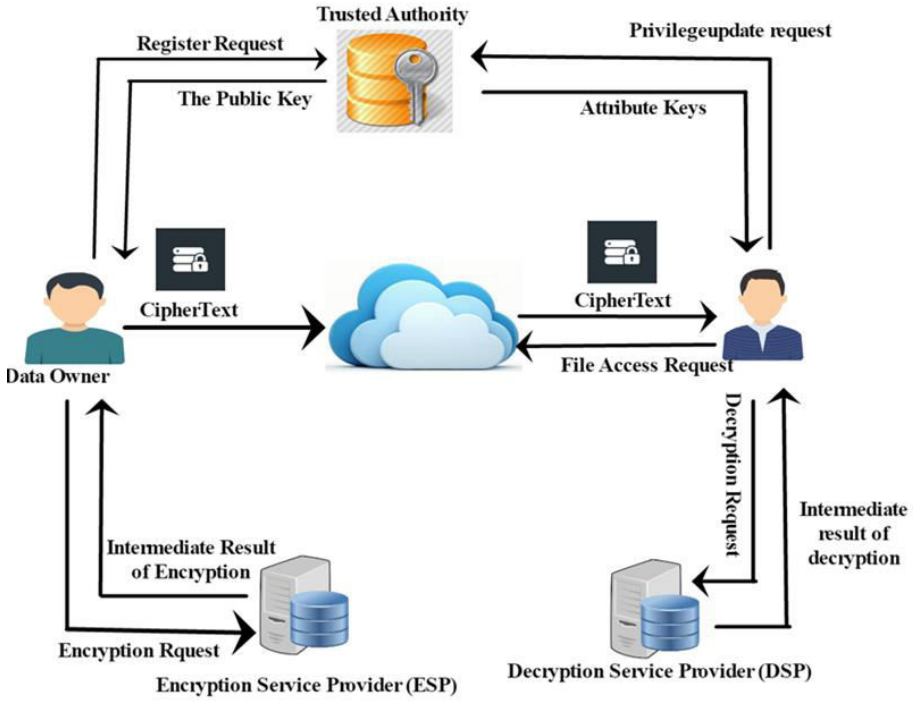

Figure 1: **Architecture of the proposed system**

We propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

Data Owner Module:

Data owner can provide data or files that contain some sensitive information, which are used for sharing with his/her friends. All these shared data are outsourced to the cloud servers to store. And generate the three attribute key for the data user. This attribute key is using for security. Ans additionally data owner allocate the file access time interval for when data user will access the file in that particular time interval only data owner only a decryption the file and upload the file into a cloud sever

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003186

Data User Module:

The data users are having a registered users only when data user want to file from the cloud server that time send file request to the data owner. the data owner file upload for the that data user here security keys are generate from the data user mail and mobile number. that is unique to every users. and time interval also allocate from the data owner. that time interval only user can access the file from the cloud server

Admin Module:

In here admin have a monitoring the all work flow from the file owner and file user activity and also all the private keys, and attribute keys are generate from the file owner and admin side that for security of the files. Admin has only send the key generation for file uploading for data owner and generate the key for file download from the data user its used for the unauthorized user not access the file from the cloud server without key.

Time Server Module:

The time server module is a most important module of in this project. Here file owner allocate the time interval in this module. When file owner upload the file into the cloud server that time owner allocate the file download interval time. This is used for the other user can't access the file from the cloud server. Current system time will cross the allocate the ending time while that file will be deleted from the cloud.

Cloud Server Module:

The cloud server module is when user and file owner registered that information and file owner upload the files details that type of all information are stored in this cloud server. Here data owner /user / admin data bases are stored in cloud sever and file upload to cloud sever and file retrieve from the cloud sever only. This is main part of our project. when unauthorized used cant access the file without authentication in cloud sever

Secure Self-Destruction Scheme Module:

Here we are using the generating the attribute from the users information. For ex mail and mobile number are taken and generate the key. That key are generate from the file owner when file owner upload to the cloud server that time this operation will performed. This attributes are mostly used for the security for the files in cloud.

IV. RESULTS

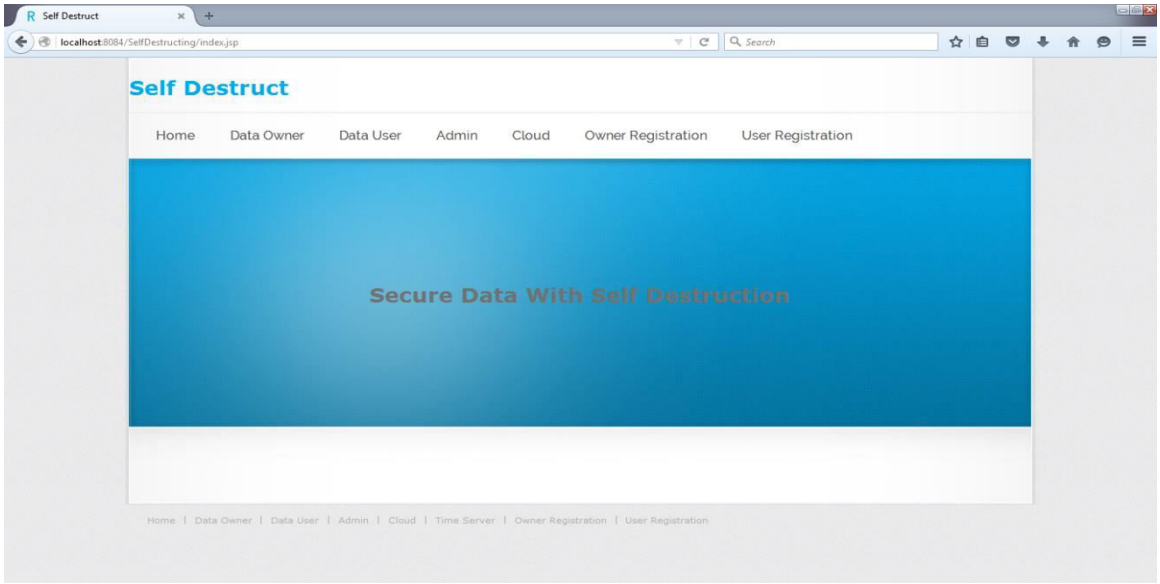

Figure 2: HOMEPAGE

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003186

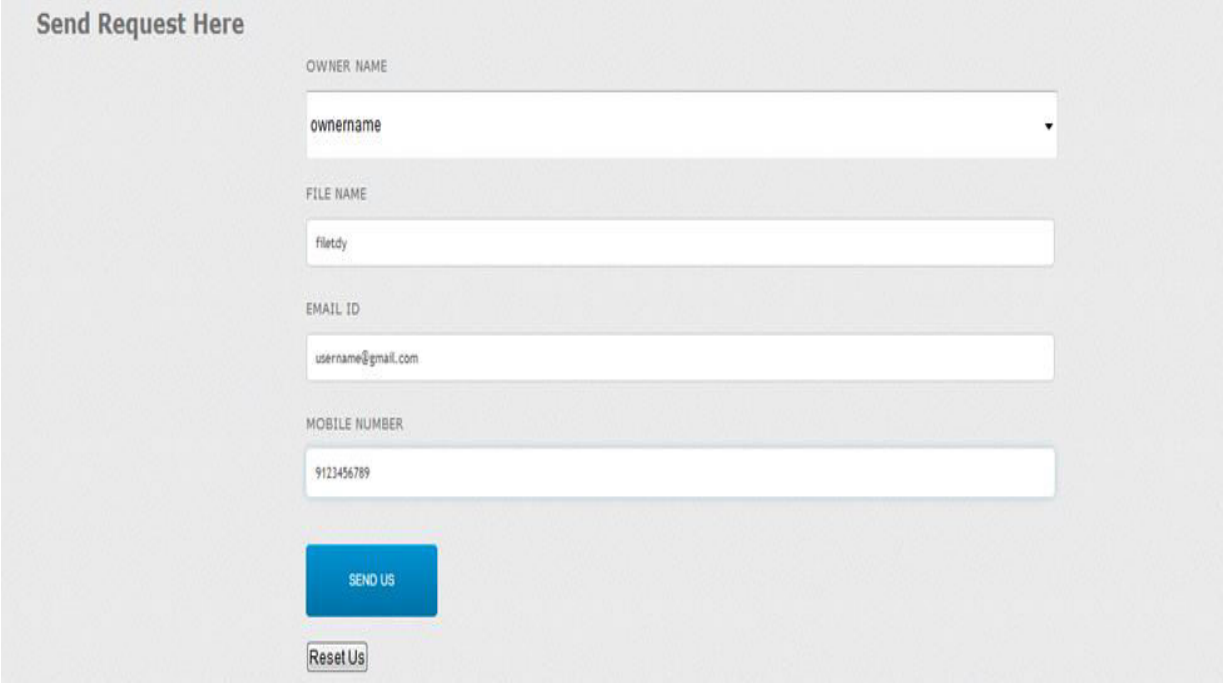

Figure3: USER REQUEST

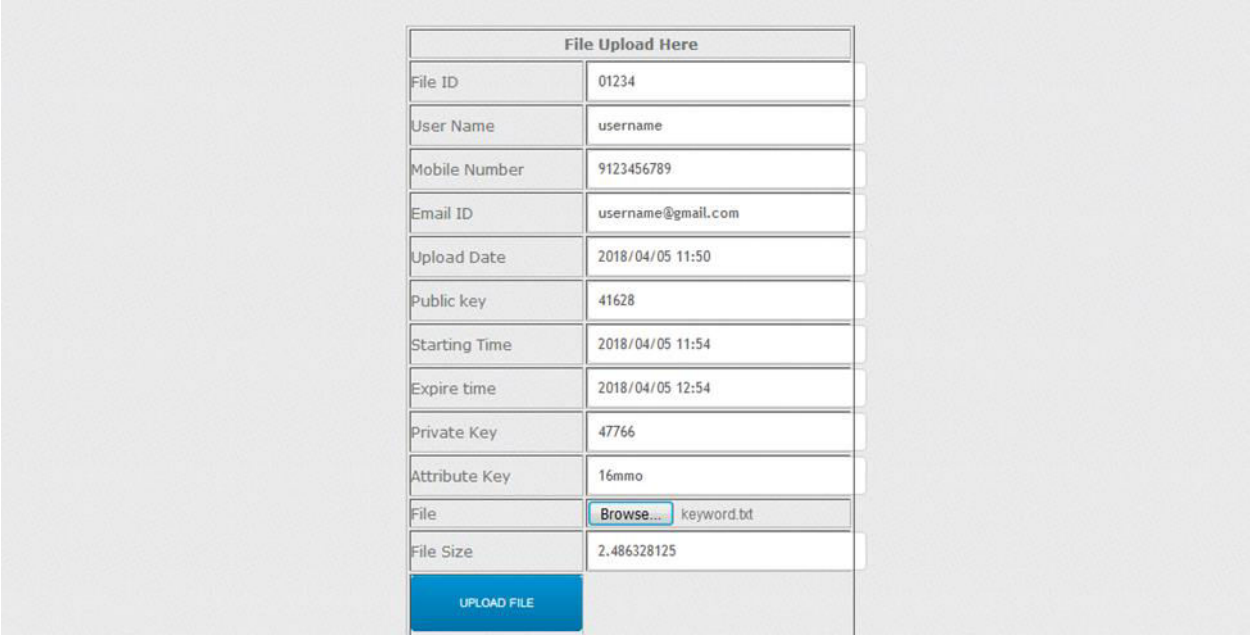

Figure 4: OWNER FILE UPLOAD

V. CONCLUSION

In this paper, we propose a privacy preserving multi-keyword search scheme with lightweight fine-grained access control (MRSF). Contrasted and past schemes, other than acknowledging access control, MRSF accomplishes a superior search execution and higher security level. All together to improve the practicability and security of MRSF, we join the TF-IDF rule with the ordinary arrange coordinating technique and incorporate the access control procedure with the improved secure kNN scheme. Formal security definitions and comparing investigation show that MRSF is

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003186

IND-CLS-CPA secure, we additionally demonstrate that MRSF is safe to the agent KPAs. At last, broad assessments show the compelling variables for search exactness and effectiveness of MRSF.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in IEEE International Conference on Distributed Computing Systems, 2010.
[2] L. Zhang, Y. Zhang, and H. Ma, "Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data," IEEE Access, vol. 6, pp. 34 214–34 225, 2018.
[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, Jan 2014.
[4]D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, May 2000, pp. 44–55.
[5] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 442–455.
[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.
[7] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited:consistency properties, relation to anonymous ibe, and extensions," in Advances in Cryptology – CRYPTO 2005.
[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in 2010 Proceedings IEEE INFOCOM, March 2010, pp. 1–9.
[9] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, and S. Mitra, "Zerber: r-confidential indexing for distributed documents," in Proceedings of the 11th international conference on Extending database technology: Advances in database technology. ACM, 2008, pp. 287–298.
[10] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+r:Top-k retrieval from a confidential index," in Proceedings of the 12th International Conference on Extending Database Technology:Advances in Database Technology, ser. EDBT '09. New York, NY, USA: ACM, 2009, pp. 439–449.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details