IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 4 ISSUE : 11 Print / Issue Publication Date: 10-May-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2020.v04i11.019

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 98-104
Published Online March 2020 in IJEAST (http://www.ijeast.com)

A FRAMEWORK FOR MODIFIED LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR CLOUD COMPUTING

Konika Mallik[1], Dr. G. Ramu[1], P. Nagaveni[2], N. Geetha[2].
[1, 2, 2] UG Student, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Telangana, INDIA.
[1]Associate Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Telangana, INDIA.

***Abstract* — Cloud computing has become one of the most commonly used technological service used in these days. As cloud computing is being developed rapidly, it has given its users "A technological future". In parallel to it, usage of mobile and its equivalent devices has also reached their substantially highest level. Due to the popularity and services provided by mobile cloud computing, web, mobile and other devices can store, process and retrieve a very vast amount of data. However, in that process, data security has become the major concern. Although, substantial studies have been conducted towards this issue, it cannot easily be made null as long as hackers and intruders exist with the common people. Here, we propose a "Modified Light Weight data sharing scheme for Cloud computing", an access control technology that adopt R-RABE (Revocable and Re-used ABE). MLDSS uses a novel algorithm to provide data security when it is uploaded on to the server. Further, it re-uses the secret keys created in the process to reduce cloud burden. With this application, owners and users of data can effectively share and retrieve information with diminished security issues.**

Keywords — **Lightweight data sharing, Revocable ABE, data security, cloud computing, secret keys, cloud burden.**

I. INTRODUCTION

As the importance of Cloud computing is rapidly being increased in this fast-growing generation, it has empowered its users with an "enriching and everlasting future". Parallel to its way, usage of mobiles and their services also have been increased. People get crucial information in just couple of seconds even through their personal mobile phones. Moreover, they can store, process and access sensitive information in their own devices with personal perspective and attention so that they cannot be accessed by unauthorized users or the people with negative intention of manipulating and destroying one's information. Although, rapid inclusions and studies have been made with respect to this strategy, data and file security is still the major concern. The issue cannot be easily solved as far as false people (hackers and intruders) exists in this world. But, being intelligent machines and responsible citizens, we can always put a step forward in trying to improve the current scenarios and protecting crucial data and information.

One of the steps taken by the authors of "Light Weight Data Sharing Scheme for Mobile Cloud Computing" [1] has opened a door for mobile users for reducing cloud overburden by using external servers for encryption and decryption processes. It seems to be simple but it proposes a novel strategy which greatly reduces burden on client-side devices by slightly increasing the same on server side. In the process of developing our work towards data security, as we have taken major references from the work of these authors, we take a privilege in discussing some of the major steps of this algorithm (LDSS).

(1) It designs an algorithm called LDSS-CP-ABE which uses CP-ABE (Ciphertext-policy ABE) to provide access control policies to LDSS users.

(2) The algorithm is named "Light Weight" with the view that it uses proxy servers for encryption and decryption processes i.e. computationally intensive operations are done on server side (in proxy servers), thereby, reducing client-side burden.

(3) It reduces user revocation problem.

(4) It finally develops a beneficial framework which substantially reduces client-side overburden by just introducing slight burden on server side.

Further to the discussion, LDSS provided various apparent results which undoubtedly proved beneficial to the society where people simultaneously receive and transfer information. In this application, people can upload their photos, videos and documents safe and secure from unauthorized users.

Along with the safe and secure mechanism provided by LDSS, we further propose an algorithm named R-RABE (Revocable and Re-used ABE), an ABE technology which majorly forces on re-using the existing secret keys, thereby, further reducing computational work on cloud. We named this approach as

"Modified Light Weight Data Sharing Scheme for Cloud Computing".

We are majorly concerned about two people in this scenario, first is the Data Owner and second is the Data User. Data Owner uploads his or her data which can be in the form of file, document, audio, video, etc., with the belief that the data will be stored securely and he/she can access them at anytime and anywhere. Also, with the second belief that no one can misuse the data and can only be viewed by the users he/she wants. On the other hand, Data User is the person who consumes data access permissions for accessing files uploaded by the Data Owner.

One of the major advantages in using this application for storing data and files instead of directly storing them in hardware like personal systems or mobile phones is that system or mobile storage will greatly be reduced along with the reduction of data security issues. Before uploading personal data, which is sensitive to his or her concern for data owner, the data must be encrypted and it must be decrypted back when an authorized data user wants to access it. However, some of the old mechanisms, although, performs well in decryption and encryption and other operations, imparts hectic task on the users as the data owner need to share password to each and every user with whom he or she wants to share data. Further to this issue, some other mechanisms tried to simplify this privilege policy in which data owner can segregate the intended data users into particular sets and provide password to each group. However, we cannot surpass the fact that password and user management is a major task.

Therefore, in this proposed system, the data owner need not worry about sending password to data user. File attributes would be set automatically once the owner of the file uploads it onto the application. When a particular data user requests for a file, the user attributes and file attributes are matched for validation. If they match successfully, undoubtedly, the user can access that file, else, he or she cannot. A secret key is generated once the user is proved valid, and after time lapses, all the access permissions are revoked. This system also proposes an algorithm called R-RABE (as previously mentioned) which re-use the existing secret keys for different file transfers, idle at current time.

The next section shows the detailed Literature Survey on this paper.

II. LITERATURE SURVEY

(2014) An approach towards migrating key-creation burden to external servers from client machines for effective and secure data and information sharing [1]:

Authors related to this paper have proposed and designed a scheme and method called LDSS (Lightweight Secure Data and Information Sharing Scheme). The scheme uses CP-ABE (Ciphertext policy ABE), basically an access control phenomenon and technology technically used for general cloud environment and Infrastructure, but additionally modifies the design of access control tree to further make it clearly and efficiently more suitable for web and mobile (world-wide) cloud storage and environments. To lessen the burden on client side, it transfers the major portion of computationally intensive operations to the external servers. Also, to decrease user revocation problem, it uses Lazy re-encryption technique, one of the major issues in CP-ABE methods. All technical and experimental results showed clearly that this scheme has an ability to securely and effectively reduce overburden on client side whenever users want to share data via internet.

(2016) An algorithm designed for Ciphertext Search based on keywords [2]:

The authors of this paper are Ren Xunyi and Yan Shiyang. They majorly focused on data leakage problem. They illustrated that cloud storage have the advantage of high reliability, scalability, inexpensive, easy to manage and without access limit. In this context, when users intend to upload files, keywords are extracted from it. It follows two steps, both of which are done basically on the client side. Both encrypted indexes and Ciphertext are stored efficiently on cloud i.e., on the server side. Whenever, a particular user requests for a file, client systems basically uses the designed search algorithm developed to process and analyse the definite keyword to a corresponding query and processing pointer and give the final result to the external server, which is in turn used by the server to retrieve the user's definite encrypted index of search. That server uses that index to search and find out the corresponding ciphertext and submits the final result to the client and then client attempts to use his or her private key to decrypt the stored ciphertext.

(2012) Secret Key Cryptographic Algorithm [3]:

Authors of this paper discussed about the public key cryptographic technique and its applications such as Data Encryption Techniques and Key Agreement and developed a new secret key algorithm. If a user wants to encrypt data and information, he or she must provide the public key of the user to whom he wants to share the data along with the message to be encrypted.

(2011) An approach towards Data leakage solution for access control in cloud [4]:

The authors of this paper are Qihua Wang and Hongxia Jin. In this paper, they proposed a system to reduce the data leakage issue in collaboration systems of SaaS efficiently by decreasing human bugs and errors. They designed and proposed a series of systems and mechanisms for providing defence surpassing the problem of information leakage. They implemented a prototype of this solution.

(2013) Design of Access control phenomenon for efficient and easy revocation [5]:

The authors of this paper are Kan Yang, Kui Ren and Xiaohua Jia. They proposed an access control design framework in public and private cloud storage and develop a fine-grained access control method and scheme based on CP-ABE

(Ciphertext-Policy based 887ABE) and also propose a reliable and efficient attribute revocation method for such systems.

(2018) Efficient and Secure Attribute-Based Encryption (ABE) enabling Keyword search [6]:
The authors of this paper are Zhenfu Cao, Xiaolei Dong, Haijiang Wang, and Dongmei Li. The authors design a system called Attribute-based encryption (ABE) enabling Keyword Search. It is such a system that facilitates Keyword search and access control methodologies and strategies. Due to the aggregation technique proposed in this system, this search method need only three pairings, which is greatly useful when compared to other previous schemes.

(2014) Completely secure Attribute based encryption with key policy and faster decryption [7]:
The authors of this paper are Junzuo Lai, Robert H. Deng, Yingjiu Li and Jian Weng. In this process, they proposed a new phenomenon on KP-ABE (Keyword-Policy ABE). It has basically four features: expressive, completely secure, constant(non-varying) size ciphertexts and simultaneous decryption.

(2007) An algorithm to enable to use a key in order to generate ciphertext for network security [8]:
The authors of this paper are Homer Wu, Tsang-Yean Lee, Chong-Yen Lee and Wuu-Yee Chen. They divided normal text (plaintext) into two parts, One is the fixed length part and other is the variable length part. They proposed and encryption strategy and algorithm which is used to encrypt the first part of the encrypted text (ciphertext) and also key of the ciphertext part.

(2017) Access control method (CP_ABE) with abstract policies [9]:
The authors of this paper are Nurmamat Helli and Kaysar Rahman. They propsed a CP-ABE (Ciphertext-Policy Attribute Based Encryption technique) access controlled technique with abstract properties and attributes.

(2017) Enabling encryption based on cryptography and design of compression techniques [10]:
The author of this paper is Sarita Kumari. The author discusses about AES algorithm (one of the most powerful techniques among encryption algorithms).

III. IMPLEMENTATION METHODOLOGY

To implement the proposed algorithm i.e., R-RABE (Revocable and Re-used ABE), we must know clearly about its parent algorithm i.e., ABE (an Attribute based encryption technique). It is basically a method and phenomenon of public key encryption technique and methodology where the secret key of a user and the ciphertext (usually encrypted plaintext) depends upon attributes such as country, state, age, name, etc. In this technique, decryption of ciphertext is allowed only if the attributes of user match with the attributes of the ciphertext. This technique was initially introduced by Brent waters and Amit Sahai and slowly developed by Vipul Goyal and Omkant Pandey. Several other researchers have further come forward to develop ABE.
As discussed earlier, method of re-using of secret keys will be mentioned further.
Re-using of secret key have the following advantages:

- It reduces storage requirements of keys.
- Reduces key verification cost.
- Net key verification and validation time.
- Can use same secret key for different file transfers.

Further steps demonstrate the algorithm for secret key collection and re-use:
The algorithm consists of the following steps:
Secret key collection algorithm (R-RABE) is represented by "S" on the overall basis as follows

S = [Begin, GenPK, EncryptF, STokenGen, DecryptF, UpdateCT, PPKUpdate, Revoke]

Begin: This is the first step in the algorithm in which initially the key authority invokes R-RABE. The inputs to this step are a security attribute A, maximal number of file requests at a particular instant of time t (N) and status list SL and it outputs a pair of master keys (mpk-private key and msk-secret key), updated status list USL, updating the status of all revoked users and public parameter P.

Begin (A, N, SL) → (mpk, msk, USL, P)

GenPK: Next step is to generate private key to a corresponding user. It takes the master secret key (msk), master public key (mpk), attribute A and public parameter P concerned with a particular user from the begin phase and outputs private key ppk and updated status list USL as output.

GenPK (msk, mpk, A, P) → (ppk, USL)

Both the above steps are performed by trusted key authority.

EncryptF: This step is concerned with the data owner. It takes the public parameter P, message m, time period T (the time up to which the user will have access control on the particular file and attribute A and produces ciphertext (encrypted file) CT as output.

EncryptF (P, m, T, A) → (CT)

STokenGen: It is performed on the side of data user. Data user performs and executes this step to generate and produce tokens of search operation for his or her requests. It considers the private key ppk and also a keyword k as inputs and outputs search token stk.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 98-104
Published Online March 2020 in IJEAST (http://www.ijeast.com)

STokenGen (ppk, k) → (stk)

DecryptF: It considers ciphertext (an encrypted plaintext) CT and a decryption private key ppk as inputs and then display the actual message 'm' uploaded by the data owner m as output.

DecryptF (CT, ppk) → (m)

UpdateCT: This update algorithm is performed by cloud server. It considers the public parameter P, older encrypted text (ciphertext) CT, old time period T, new time T' as inputs and then output the updated Ciphertext UCT.

UpdateCT (P, T, CT, T') → (UCT)

PPKUpdate: This key update algorithm is performed by the key generation authority. It considers the private key ppk and an update operator v as inputs and then generates a new and updated private key (specifically for the user) ppk' as output.

PPKUpdate (ppk, v) → (ppk')

Revoke: This step takes public parameter P, attribute A to be revoked, status list SL, time period T as input and produces revoked list LR as output.

Revoke (P, A, SL, T) → (LR)

Main objectives of this project are

- To implement a lightweight data sharing strategy with a software application available for any type of user, which enables the user to keep his or her data or files secure and safe from intruders and unauthorized users.
- To minimize the overburden of re-creation of secret keys by utilizing the existing keys and enable a modified attribute-based encryption named as R-RABE (Revocable and re-used ABE).

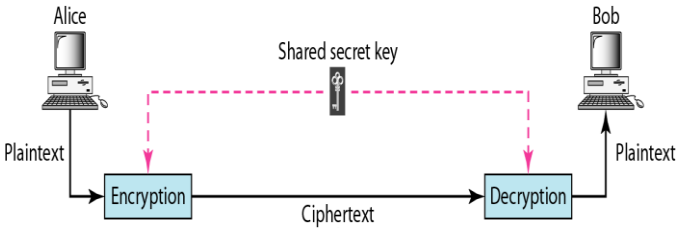

Fig 1: Common Process of Encryption and Decryption

Involvement of each person and corresponding operations are mentioned below

- Data Owner (DO) starts the process of this application by uploading data or file in the cloud and share it with data users and friends. He or she is the one who determines and sets the access control policies i.e. he or she is the one who is responsible for deciding the viewers of a particular file or data.
- Data User (DU) then in further steps retrieves data from the cloud i.e. who meets and satisfies the access control policies.
- Trust Authority (TA) is involved in the responsibility of generating and distributing attribute keys to its users.
- Encryption Service Provider (ESP) converts plain data uploaded by Data Owner to encrypted text for security
- Decryption Service Provider (DSP) converts back the encrypted into user understandable plain text for Data User.
- Cloud Service Provider (CSP) takes and stores the encrypted data uploaded by Data Owner and does the tasks requested by Data Owner.
- SKC is collects and stores secret keys before and after they have been revoked, thereby, to use them again. Expected outcomes from this project are as follows
- Initially Data Owner sends (uploads) data or file in the cloud. But data to be stored by the data owner must be encrypted (converted to ciphertext) before it is uploaded on to the cloud.
- A well-designed policy of access control on data files is set in which certain attributes must be defined if the data owner wants to make his or her data secured in the cloud.
- Encrypted symmetric secret keys are produced by R-RABE (Revocable and Re-used ABE).
- Then, only a data user who gets attribute keys definite to a file can access the file uploaded by the data owner.

IV. MODULES

Let us see the modules and the people involved in this application:
It has the following seven components mentioned below:
(1) Data Owner (DO): Basically, Data Owner is the person who uploads required data or file onto web or mobile cloud and has the right to share it with his or her people. He is the one who owns all the access (to view and manage) control policies.
(2) Data User (DU): Data User is the person who retrieves or accesses data from web or mobile cloud uploaded by data owner.
He or she can do that if access control permission is provided.
(3) Trust Authority (TA): Trust authority generates and distributes attribute keys to its users.
(4) Encryption Service Provider (ESP): The Data Encryption processes and operations required for Data Owner are done by ESP by providing Data encryption keys.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 98-104
Published Online March 2020 in IJEAST (http://www.ijeast.com)

(5) Decryption Service Provider (DSP): The Data Decryption processes and operations required for Data User are done by DSP by providing data decryption keys.
(6) Cloud Service Provider (CSP): It basically stores the data uploaded by data owner and does the operations asked by Data Owner and stores his or her data.
(7) Secret Key Collector (SKC): SKC is responsible for collecting and storing secret keys before and after they have been revoked, thereby, to use them again.

V. PERFORMANCE ANALYSIS AND RESULTS

The whole process revolves around seven major participants in this application: Data Owner (uploads data), Data User, Cloud Service Provider (stores data), Encryption Service Provider, Decryption Service Provider, Trust Authority and Secret Keys Collector.
The major steps involved here are mentioned below

- Initially, the person involved is the Data Owner who wants to make his file secured, therefore, believes the cloud service Provider and uploads his file on to the cloud. For doing that, he or she need to register with certain details which would late help in generating attribute and symmetric keys.
- Once the data owner uploads his file, he can access the file anytime and anywhere because it is his own file. Moreover, he or she do not need to worry about the hackers as the data is protected with a better algorithm and also about the storage as the data and its secret keys are completely stored on the proxy server but not in his own device.
- Now a data owner with certain access control permissions can access the file uploaded by the data owner. To do that, DU first need to register, same as a DO, the only thing DU should mention additionally is a File access attribute. If the file attribute and user attribute match successfully, a secret key would be sent to the mail ID of DU, with which DU can easily view and access the particular file.
- After an instant of time, all the access permissions of DU are revoked and its status is thus sent to the revoked list, so that, the same secret key idle at that particular time can be used for other file transfer and share.

Analyzed results are shown next

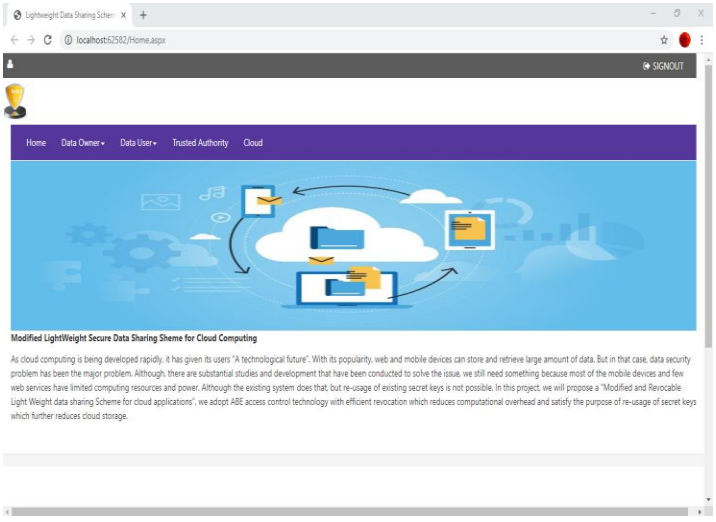

Fig 2: Home Page

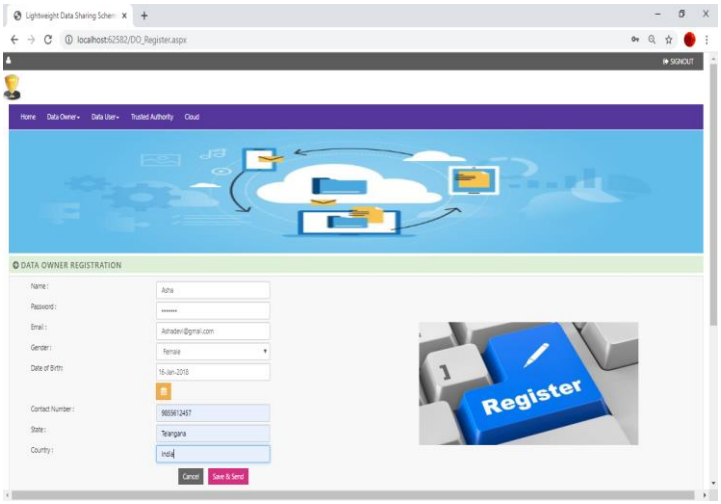

Fig 3: Registration of Data Owner (First step)

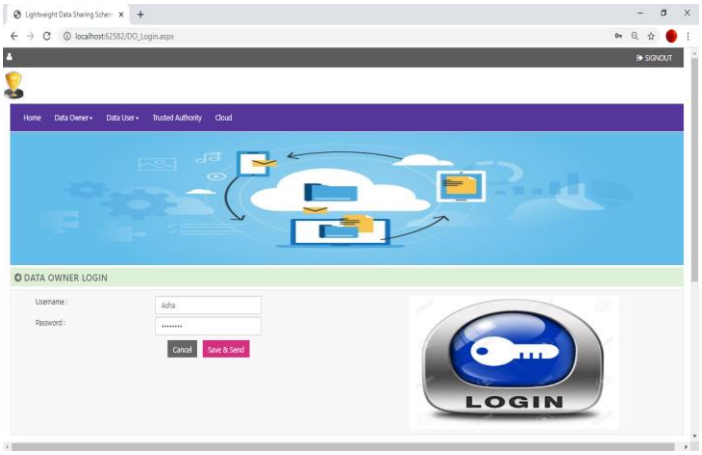

Fig 4: Data Owner Login Page

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 11, ISSN No. 2455-2143, Pages 98-104
Published Online March 2020 in IJEAST (http://www.ijeast.com)

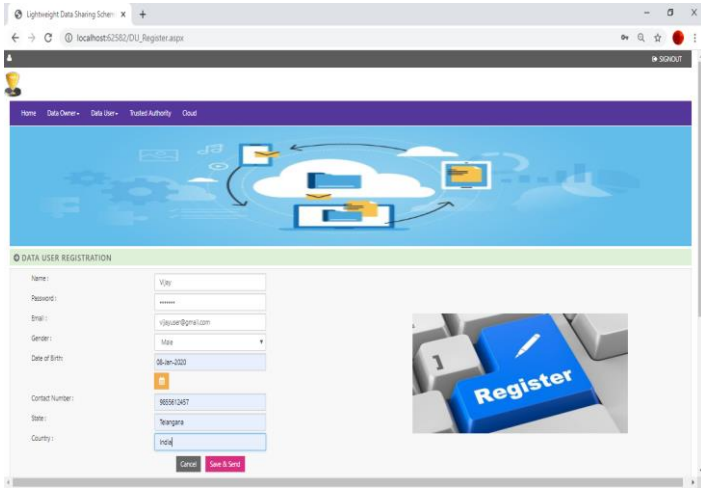

Fig 5: Registration of Data User

Fig 6: Data User Login

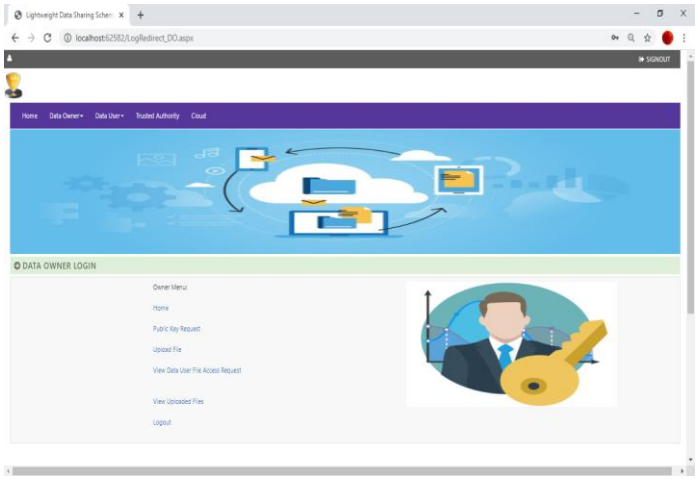

Fig 7: Data Owner Dashboard

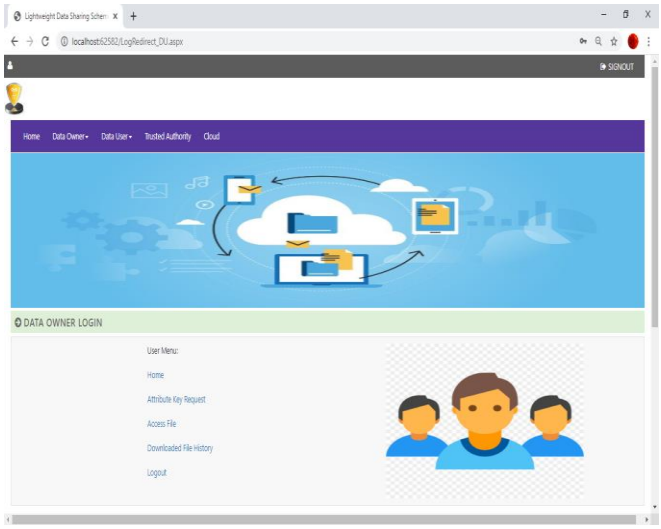

Fig 8: Data User Dashboard

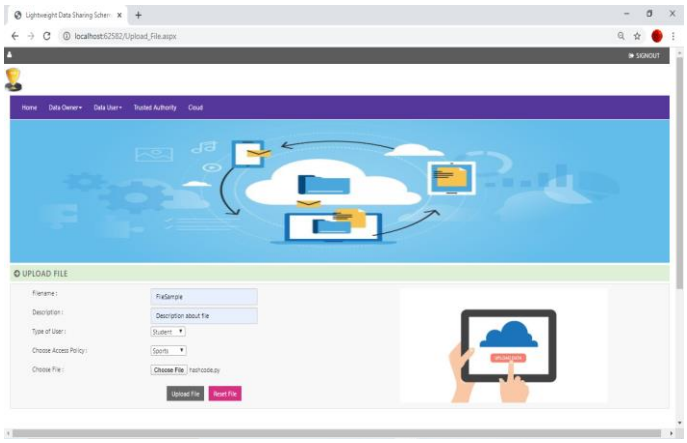

Fig 9: Upload file to be encrypted

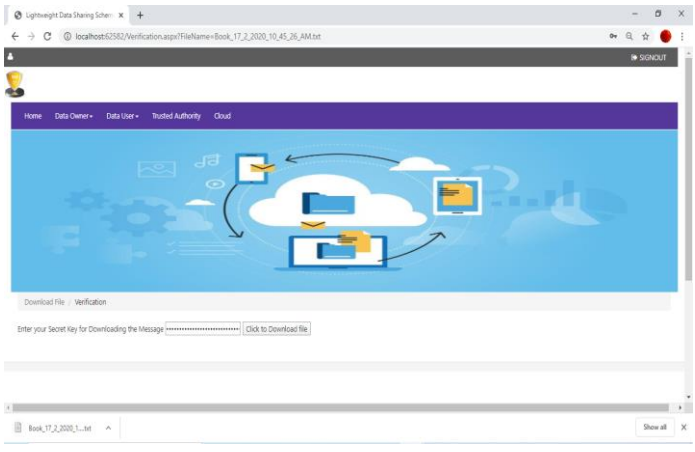

Fig 10: Download File

VI. CONCLUSION

Various theories and studies have been conducted on access control techniques and strategies based on different types of encryption algorithms, However, not every encryption algorithm is suitable for all types of devices such as some web and mobile devices because even we get control over security measures, we still need computationally less intensive and less storage resources to provide better services to the users. Here i.e., in this paper, basically, we develop and propose MLDSS (Modified Lightweight Secure Data Sharing Scheme for Cloud Computing) to provide data security to both the owners and users of data when it is uploaded on to the server and also develop an algorithm named R-RABE (Revocable and Re-used ABE) which not only reduces user revocation problem but also facilitates the purpose of reusing the existing secret keys for different file transfers to further reduce cloud overhead and storage. It introduces a periodic MLDSS-R-RABE algorithm to shift major computation storage and overhead from web, mobile and other devices to external servers, therefore, solving secure data sharing problem in the cloud. In the future work and enhancement, we will look to design new approaches and methodologies to further reduce cloud storage and also develop voice-based application for the similar type.

VII. REFERENCES

[1] Zhiyong Xu, Ruixuan Li, Cheng-Zhong Xu, Chenglin Shen and Heng He (2014) - "Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing", IEEE (Institute of Electrical and Electronics Engineers) Transactions on Cloud Computing.

[2] Ren Xunyi and Yan Shiyang (2016) - "Keyword-based Ciphertext Search Algorithm under Cloud Storage", MATEC (Midwest AIDS Training and Education Center) Web of Conferences, 61, 03002, APOP2016.

[3] G. Naga Satish, Dr. Ch. V. Raghavendran, P. T. K Mehar and Dr. P. Suresh Varma (2012) - "Secret Key Cryptographic Algorithm", International Journal of Computer Science, Information Technology and Management, Vol. 1, No. 1-2, (January-December, 2012).

[4] Hongxia Jin and Qihua Wang (2011)- "Data leakage mitigation for discretionary access control in collaboration clouds", Proceedings of the 16th symposium of ACM on Access control models,methods and technologies, pp. 103-112, June 2011.

[5] XIaohua Jia, Kan Yang and Kui Ren (2013) - "Attribute-based fine-grained access control with efficient revocation in Cloud Storage Systems, Information, computer and communications security, Proceedings of the 8th ACM SIGSAC symposium, May 2013, pp. 523-528.

[6] Haijiang Wang, Zhenfu Cao, Dongmei Li and Xiaolei Dong (2018) - "Secure and Efficient Attribute-Based Encryption with Keyword Search", The Computer Journal, Volume 61, Issue 8, August 2018, pp. 1133-1142, 18 April.

[7] Yingjiu Li, Robert H. Deng, Junzuo Lai and Jian Weng (2014) - "Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption", ASIA CCS '14, Information, Computer and Communications Security, Proceedings of the 9th ACM symposium, June, pp. 239-248.

[8]Homer Wu, Chong-Yen Lee, Tsang-Yean Lee and Wuu-Yee Chen (2007) - "Algorithm of cipher text containing key to produce cipher text transmitted in network security", AIKED '07, Knowledge Engineering and Data Bases, Artificial Intelligence, Proceedings of the 6th Conference on 6th WSEAS International Conference, Volume 6, February 2007, pp. 201-205.

[9] Kaysar Rahman and Nurmamat Helli (2017) - "CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy", Security and Communication Networks, Article ID 2713595, Volume 2017.

[10] Mrs. Sarita Kumari (2017) - "A research Paper on Cryptography Encryption and Compression Techniques", ISSN:2319-7242, Volume 6, International Journal of Engineering and Computer Science, Issue 4, pp. 20915-20919.

[11] Liang Xiaohui, Cao Zhenfu, Lin Huang (2009), et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286.

[12] Pirretti M, Traynor P, McDaniel P (2006), et al. Secure attribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112.

[13] Yu S., Wang C., Ren K. (2010), et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270.

ACKNOWLEDGEMENT

1. **Konika Mallik** is pursuing B. Tech in the stream of Computer Science and Engineering in Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India.
2. **Dr. G. Ramu** is an Assistant Professor in the Department of Computer Science in Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India.
3. **P. Nagaveni** is pursuing B. Tech in the stream of Computer Science and Engineering in Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India.
4. **N. Geetha** is pursuing B. Tech in the stream of Computer Science and Engineering in Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143