Secure Data Storage And Retrieval In The Cloud

T Kishore Babu[#1],T Paul Kiran[*2], T Ganesh[#3], N Vinay Teja[#4]

[#]*Assistant Professor, CSE,Andhra Loyola Institute of Engineering and Technology,Vijayawada,India#*

[2,3,4]*Student, CSE,Andhra Loyola Institute of Engineering and Technology,Vijayawada,India*

Abstract*—In Cloud computing, user can remotely store and fetch their data based on-demand service, without the burden of local data storage and preservation. However, the protection of the private data processed and generated during the computation is becoming the major security concern. The main objective of cloud computing enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. The main concern of this paper is optimal storing, retrieval of data with effective security in cloud computing. The proposed methodology suggests the encryption of the files to be uploaded on the cloud. The integrity and confidentiality of the data uploaded by the user is gaurd doubly by not only encrypting it but also providing access to the data only on successful authentication. The proposed system takes care of data security while it is in transit and also has mechanisms to support confirmation of data for correctness.*

Keywords-Cloud Computing; Cloud security; Fully Homomorphic Encryption [FHE]; Resource outsourcing; Advanced Encryption Standard [AES]

I. INTRODUCTION

Cloud consists of a large pool of easily usable and attainable virtualized resources. The users can access these resources based on their needs. Cloud computing has three service models such as Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service. Cloud deployment models are Public Cloud, Private Cloud, and Hybrid Cloud. The cloud has many advantages such as Pay-As-You-Use, Rapid Elasticity, Multi tenancy, Resource Pooling, reduced maintenance and capital investments etc. These features have made cloud computing more profitable. The rapid usage of cloud has led to many security questions.

Cloud security is the biggest drawback for its selection. The various security issues include Data loss, DDOS attacks, multenancy issues, availability etc. Users are more anxious about their data stored into cloud and retrieval of the data from the cloud. Thus, productive measures need to be taken to secure the users data. For this purpose, the paper offers an Effective Secure Storage and Retrieve system which guarantee the secure managing of the user's stored data and its retrieval. The proposed system adopts the encryption algorithms such as AES and FHE to secure users data. The locking mechanism is employed to allow only the authorized users to access the data.

The rest of this paper is classified as follows: The second section discusses related work. The third section sets out the research framework for our suggested work. The forth section discusses a potential implementation for upload and download of data in cloud computing. The fifth section depicts the snapshot of proposed work. Finally in the sixth section, the paper draws some conclusion and future work.

II. LITERATURESURVEY

Cloud computing offers a striking service for data storage known as cloud storage. Internet-based online services do provide huge amounts of storage space and customized computing resources, this computing platform shift, however, is removing the responsibility of local machines for data maintenance at the same time. As a result, users are at the elegance of their cloud service providers for the availability and fairness of their data Cong Wang et. al. [3]. The "provable data possession" (PDP) model for ensuring security of file on untrusted storages was defined by Ateniese et. al. [4]. Their scheme made use of public key based homomorphic tags for inspecting the data file, thus providing public empirical. Based on Gentry's et. al. [6] break through work on fully homomorphic encryption (FHE) scheme, a general result of secure computation outsourcing has been shown feasible in theory, where the computation is represented by an encrypted combinational Boolean circuit that allows to be assess with encrypted private inputs. However, applying this general mechanism to our daily calculation would be far from practical, due to the extremely high intricacy of FHE operation as well as the gloomy circuit sizes that cannot be handled in practice when constructing original and encrypted circuits. A method that allows

user to store and access the data securely from the cloud storage. Cloud storage identifies the storage on cloud with almost economic storage and backup option for small enterprise. The actual storage location may be on single storage environment or copy to multiple server storage based on importance ofdata.

Ming Li et. al. [9] established an Authorized Private Keyword Search (APKS) framework over encrypted cloud data and proposed two paperback solutions for APKS based on Hierarchical Predicate Encryption (HPE). This paper authorize systematic keyword searches with range query and the query privacy. Wang et. al. [10] gives the first study of secure outsourcing of linear programming in cloud computing. Their solution is based on the problem alteration and has the advantage of bringing customer savings without introducing significant overhead on cloud. However, those techniques involve cubic time computational burden matrix-matrix operations, which the weak customer in our case is not compulsory able to handle for large-scale problems. Design the independent inspecting service to check the data integrity in the cloud. It supports the data dynamic operation in cloud, which is efficient and secure model. Further extend inspecting protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. Describes data security and privacy protection issues in cloud. Here discusses data security and privacy protection issues related with cloud computing across all stages of data lifecycle.

III. PROPOSED SYSTEMARCHITECTURE

The Proposed System works the highly secured encryption mechanism to secure the data storage and retrieval as represented in Figure 1. The file present on the appliance will be encrypted using AES algorithm. The user can also download any of the uploaded compression files and read it on the system. It works on fully holomorphic encryption (FHE) scheme where the calculation is represented by an encrypted combinative Boolean circuit that allows to be evaluated with encrypted private inputs. Every data is locked for security motive and only authorized users can access the data by using authenticated name and mailid.

Cloud is data storage system in the cloud which allows the users to store their data in to the cloud and do not have the data regionally. Therefore, the security and handiness of the data files which are stored on to the distributed cloud servers need to be protected. As decorated in Figure 1, after successful registration of the user, the user can upload the crave data in cipher text form. User will be provided with options for file, text or image upload in reliablemanner.

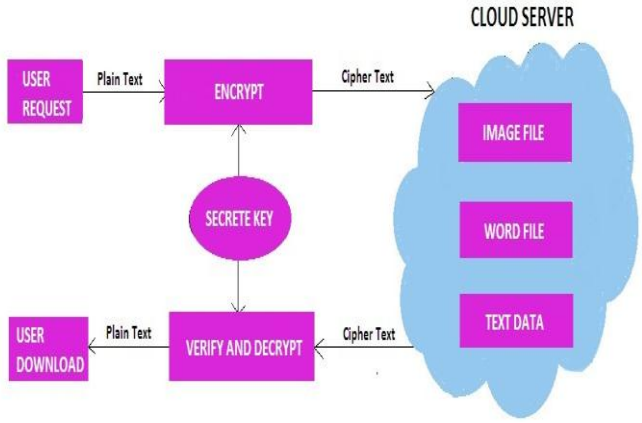

Figure 1. Architecture of Effective Secure Storage and Retrieve in Cloud Computing.

After secure storage, user can reclaim by downloading the data from the cloud server. The authenticated user can download the file safely which is being uploaded. The user can also get the decryption and encryption details.

IV. IMPLEMENTATION

The proposed system is executed using Java, MySQL and public cloud Open shift. JSP is used for create front end and server side script. Apache Tomcat 5.0/6X/7X is used as application server in our job. This section report the module implementation.

A. DataUpload

The data upload module makes the user to upload the data such as file, image and text can be uploaded to the cloud server. To upload the crave files, user must give his details such as user name and password. The valid authenticated user can connect to the cloud and upload the data by providing its information such as data name and email. The secret key is produced using AES algorithm. After affluent uploading of the data, the connection can be disconnected. The data uploading process takes placeconsecutively as in algorithm.

B. DataDownload

The data download module makes the authenticated users to download the requested data. The authenticated user create the connection with cloud and can request the wanted data. The user must provide facts such as data name and email id to decrypt the key using AES. If the data name and email is true, then the user can download the data from the cloud. After

1. Obtain user name and password from theuser
   - If user is authenticated, start connection with the cloud
   - Else, show error
2. Ask user to collect data to be uploaded onto thecloud
3. Ask the user to input data name and email for the encryptionprocess
4. Save this data name and email then produce akey
5. Deploy the encryptionalgorithm
6. Upload the given data on to thecloud
7. Disconnect connection from thecloud

Figure 2. Data Uploading Algorithm

successful download, the user can break the connection from cloud. The data downloading process takes place step by step as in algorithm.

1. Obtain user name and password from theuser
   - If user is authenticated, start connection with thecloud
   - Else, show error
2. Ask user to select the rank (Files, Images orText)
3. Ask user to search your required files to bedownloaded
4. Ask the user to input the data name and Email-id for the decryptionprocess
5. Check the name andEmail-id
   - If the input data is valid, generate akey
   - Else show an error and rejectpassword
6. Apply decryptionalgorithm
7. Download the required data from thecloud

Figure 3. Data Downloading Algorithm

V. EXPERIMENTS ANDRESULTS

Home page

The snapshot below shows the home page of the proposed system. The home page is made using html language. It has links to user registration, user login and user upload pages. This page contains only connections to other pages and does not have any particular activity or computations being done here.

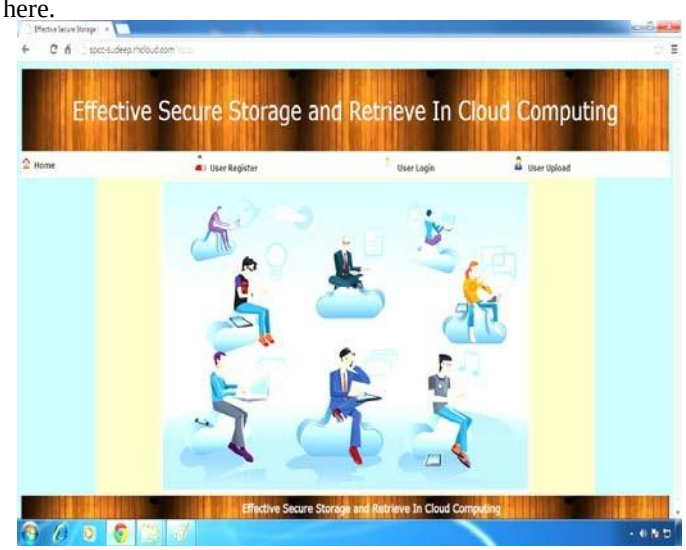

Figure 4. Home Page

User Login Page

The snapshot fig below shows the user login page. In this page after successful registration, the user will be given with login for the file, text or image upload and download. Here only valid user can sign in to the cloud through valid Email and password forauthentication.

Figure 5. User Login Page

User Upload Page

The snapshot fig below shows the user upload page. In this page the user will be given with options for file, text or image upload. Here we also have two more options for user to logout and redirecting to home page.

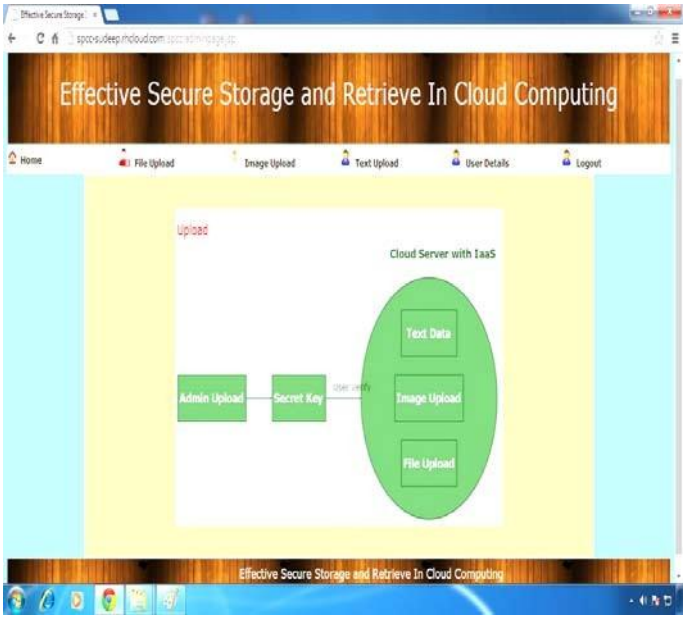

Figure 6. User Upload Page

File Upload Page

The snapshot below shows the file upload page. In the file upload first we have to check whether the database connection is set up or not, if the connection is ensured it continues with the execution else it displays error message. Once database is connected the file is uploaded to theserver.

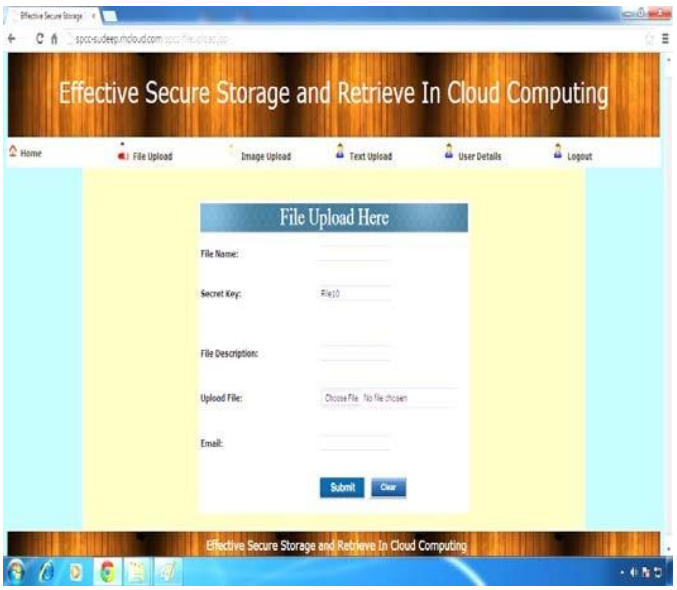

Figure 7. File Upload Page

User Download Page

The below snapshot shows how the user can download from the server database. In this page the user will be given with options for file, text or image download. Here we also have two options for user to logout and redirecting to home page.

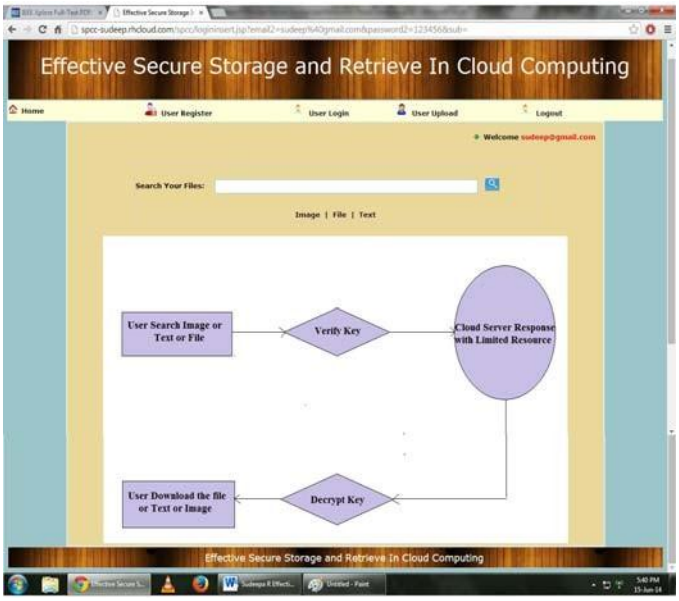

Figure 8. User Download Page

File Download with Key Verification

This page is put to show how the user can download after key verification. Once the file is uploaded from the client(user) computer, we should be able to download from the server computer, for this first we have to establish a database connection where it generates the file in the decrypted arrangement. After authentication of the user, the file would be used fordownload.

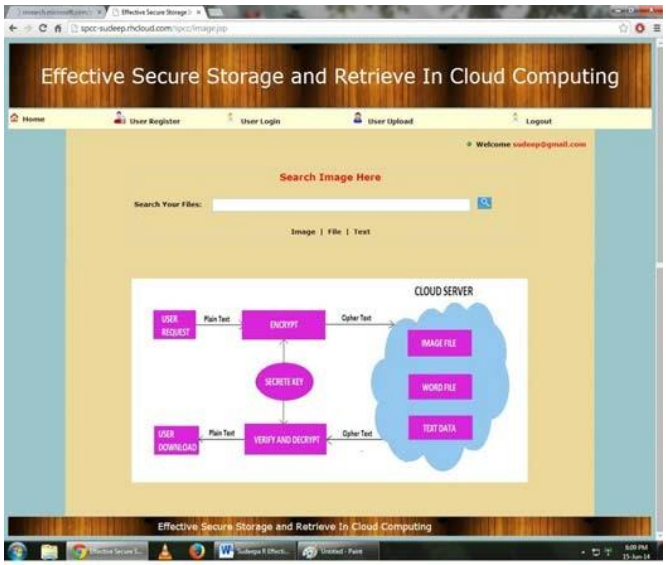

Figure 9. File Download with Verification Key

Unlocked Files and Download

This page is made to show files which are unlocked for view and download. The file unlock is done on the server side of the computer to download the contents uploaded from the client(user) side.

Once the file is uploaded from the client(user) computer, we would be able to download from the server computer, for this first we have to establish a database connection where it makes the file in the decrypted format. Once the database is connected, the file can be downloaded by the user.

Figure 10. Unlocked Files and Download

Locked Files

This page is made to show files which are locked for view and download. The file lock is done on the server side of the computer to limit download of the contents uploaded from the client side.

Figure 11. Locked Files

Encryption/Decryption

This page is made to show the encrypted and decrypted value of file key. It would also display the files uploaded to cloud server. This is a proof generating technique which can be used for establishing the truth.

Figure 12. Encryption/Decryption

VI. CONCLUSION AND FUTURE ENHANCEMENT

The proposed system effectively gives secure data uploading and retrieval by employing AES and FHE. AES provides more security to the system as it is not vulnerable to any known pounce. The proposed system also increases the accuracy and availability of user data in the cloud. Proposed mechanism provides such a practical mechanism design which attains input/output privacy, cheating flexibility, and efficiency in the cloud.

The current project can be extended to following future improvement.

- The algorithm can also be magnified to not only encrypt data i.e., file, image and text but also audio and videofiles.
- Devise robust algorithms to achieve numerical firmness.

ACKNOWLEDGMENT

The authors would like to acknowledge and thank Technical Education Andhra LoyolaEngineering College (ALIET),JNTUK, Andhra Pradesh for supporting the research work.

REFERENCES

[1] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," 2009, online at https://www.sun.com/offers/ details/sun transparency.xml.

[2] Removing S, Elf M M, Smith E, "The Management of Security in Cloud Computing", International Conference on Information Security for South Africa (ISSA), Sandton Johannesburg , 2-4 Aug. 2010, PP 1-7, ISBN:978-1-4244- 5493-8,DOI: 10.1109/ISSA.2010.5588290.

[3] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", International Conference on Services Computing, Vol 5, Issue 2, 06 May 2011, PP 220-232, ISSN
:1939-1374, DOI: 10.1109/TSC.2011.24.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,
Z. Peterson, and D. Song, "Provable data possession at untrusted stores", Alexandria Virginia USA, October 29– November 2 2007, ACM 978-1-59593-703.

[5] Z Hao, S Zhong, N Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", International Conference on knowledge and data engineering, Vol 23, no 9, September 2011, ISBN: 1041-4347/11.

[6] C Gentry, "Fully homomorphic encryption using ideal lattices", Bethesda Maryland USA, May 31–June 2 2009, PP 169–178, ACM 978-1-60558-506.

[7] Arjun Kumar, Byung Gook Lee, Hoon Jae Lee, Anu, "Secure Storage and Access of Data in Cloud Computing", International Conference on ICT Convergence, Jeju Island, 15-17 Oct. 2012, PP 336-339, ISBN: 978-1-4673-4829-4, DOI:10.1109/ICTC.2012.6386854.

[8] M Jensen, J Schwenk, N Gruschka, L L Iacono, "On Technical Security Issues in Cloud Computing", International Conference on Cloud Computing, Bangalore, 21-25 Sept. 2009, PP 109-116, ISBN: 978-1-4244-5199-9, DOI:
10.1109/CLOUD.2009.60.

[9] Ming Li, Shucheng Yu, Ning Cao, Wenjing Lou, "Authorized private keyword search over encrypted data in cloud computing", 31st International Conference on Distributed Computing Systems, Minneapolis MN, 20-24 June 2011, PP 383-392, ISBN: 978-1-61284-384-1,DOI:
10.1109/ICDCS.2011.55.

[10] C Wang, K Ren, J Wang, "Secure and practical outsourcing of linear programming in cloud computing", International Conference on infocom, Shanghai, 10-15 April 2011, PP 820-828, ISBN:978-1-4244-9919-9, DOI:
10.1109/INFCOM.2011.5935305.

[11] R Gennaro, C Gentry, B Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers", 30th annual conference on Advances in cryptology, Berlin, 2010, ISBN: 3-642-14622-8 978-3-642-14622-0.

[12] Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", International Conference on parallel and distributed systems, Vol 24, no 9, September 2013, ISSB : 1045-9219/13.

[13] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, Hangzhou, 23-25 March 2012, PP 647-651, ISBN: 978-1-4673-0689-8, DOI: 10.1109/ICCSEE.2012.193.

[14] Bhabendu Kumar Mohanta, Debasis Gountia, "Fully homomorphic encryption equating to cloud security: An Approach", IOSR Journal of Computer Engineering (IOSR- JCE), Vol 9, Jan-Feb 2013, PP 46-50, ISSN: 2278-8727.

[15] S Hohenberger, A Lysyanskaya, "How to securely outsource cryptographic computations", February 16, 2005,
PP 1-19.

[16] C Gentry, "Computing arbitrary functions of encrypted data", Magazine on Communications of the ACM, New York, Vol 53, March 2010, PP 97-105,
DOI:10.1145/1666420.1666444.

[17] Cloud Computing: Special theme, European research consortium for Informatics and mathematics (ERCIM), ISSN 0926-4981.