Volume 1, Issue 4 (2021)
Article No. X
PP XX-XX

VIVA Institute of Technology
9th National Conference on Role of Engineers in Nation Building – 2021 (NCRENB-2021)

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Providing Secure Cloud for College Campus

Belamkar Shridhar Vitthal [1], Darade Hitesh Subhash [2], Qureshi Umair Nasim Ahmed [3], Prof. Vinit Raut [4]

[1, 2, 3, 4]*(Computer Engineering Department, Viva Institute of Technology, India)*

Abstract: *In colleges data stored on the server can be access by any college staff, student or professor. Data is very important and should not be altered or accessed without permission of its owner. But in these type of medium scale organizations server can be access by anyone. A better approach to maintain the data security and sustainable storage is cloud. Cloud provides user management for authentication and authorized access of stored data. Since data is upload in cloud through network therefore its security during this phase is very important. For this, encryption algorithms can be used to protect it from hacker. It provides efficient way to carryout operations such as uploading and downloading data. An efficient use of storage should be a primary concern for which data deduplication technique can be applied. Using this technique uploading of duplicate files can be avoided.*

Keywords - *Advanced Encryption Standard, Data Deduplication, Elliptic Curve Cryptography, One Time Password, Hybrid Cryptographic System*

I. INTRODUCTION

Cloud computing has rapidly become one of the most emerging technology due to its progressive services provided model of computing not only in the IT industry but also in the software and hardware industry. The Cloud referring to the servers that are passage over the Internet, and the software and databases that running on those servers. Cloud servers are find in data centres all over the world. By using cloud computing, users and corporate offices do not have to handle physical servers themselves or run software applications on their own machines. The cloud permit users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data centre, rather than locally on the user device [13].

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion which helped several organizations to save money and time adding convenience to the end users. This mechanism came up with increased flexibility, scalability and reliability where server is not capable of handling all these. Server cannot provide better user management to avoid unauthorized access. Data security is not strong in server where in cloud a strong encryption technique gives strong data protection. Since user management give access only to authentic user and each can access only there data so other data on the cloud can't delete, alter and misplaced by any means. Although with limited storage capacity cloud gives advantage of data duplication in which if same data user try to store on the cloud it will inform to user that the data is duplicated. And then it will discard that data. This lead efficient to use of storage.

II. LITERATURE SURVEY

The AES and RSA encryption algorithm is combined due to that data security on cloud increases. Key size of RSA encryption technique is large comparatively AES hence speed of encryption reduces [1]. AES

encryption technique is use to encrypt data to be store on the cloud which provide much more security to the data [2]. File versioning and verification is use for data deduplication to avoid wastage of storage. But it takes more computational time [3]. Image is encrypt using convergent scheme then hash value is calculated and this hash value will be send to S1 and S2 server for checking deduplication. By this if copy of image is already present on the cloud then storing same image again can be avoided. In this system only two server S1 and S2 is used and deduplication of image is only possible [4]. First and Last 50 bytes of the file will be extracted and then these 100 bytes will be compared with existing file to perform data duplication. If same data already stored then a copy of the data cannot store hence effective use of storage is possible. In some cases by comparing only first and last 50 bytes is not sufficient to check if file is already stored on the cloud [5].

In homographic encryption the data present in the cipher text form can processed, that is the computation can be done on the encrypted data, which produce the same result as if done on the actual data. It uses FHE scheme. It allows secure storage & processing on data in the encrypted form. The computation on encrypted data stored at cloud is possible [6]. The data for uploading cloud server is encrypted by AES. Encryption scheme and to enhance the security. AES key encrypt data using ECC algorithm. This algorithm is fast and safe in both direction such as upload & download of file. & it is multilevel encryption technique. As decryption technique is multilevel so if some data is lost then it is very difficult to decrypt the data [7]. Initially, an index is generated by Porter stemming then the Blowfish algorithm is applied for encryption of files. For authorized access, public key encryption based ECC is used for key generation. This paper investigates cipher text retrieval over cloud storage with some efficient techniques for privacy [8].

It describes and compare different techniques such as ABE (Attribute Based Encryption), MLE (Message Locked Encryption), Symmetric encryption algorithm, PoW (Proof-of-ownership). In this paper survey of various techniques used for data deduplication is done [9]. To remove data redundancy from available offline or online data storage as well as provide the security of data which helps to improve the performance of system. Selective deduplication uses the request based deduplication techniques which reduces the bursty traffic on network [10]. This paper investigates encryption schemes currently implemented in many secure products in cloud environments. Where each encryption scheme is evaluated and analyzed in its efficiency, security and functionality for big data on the cloud [11]. The data of the user may be stored in a shared cloud storage system instead of storing in devices of cloud service provider. Data security of cloud storage and to formulate corresponding cloud storage security policy [12].

III. PROPOSED SYSTEM

Figure 1 shows, first user have to first create an account and login by providing valid credentials and if the credentials are invalid then user have to retry the same process again & again till the user entered the correct or valid credentials.

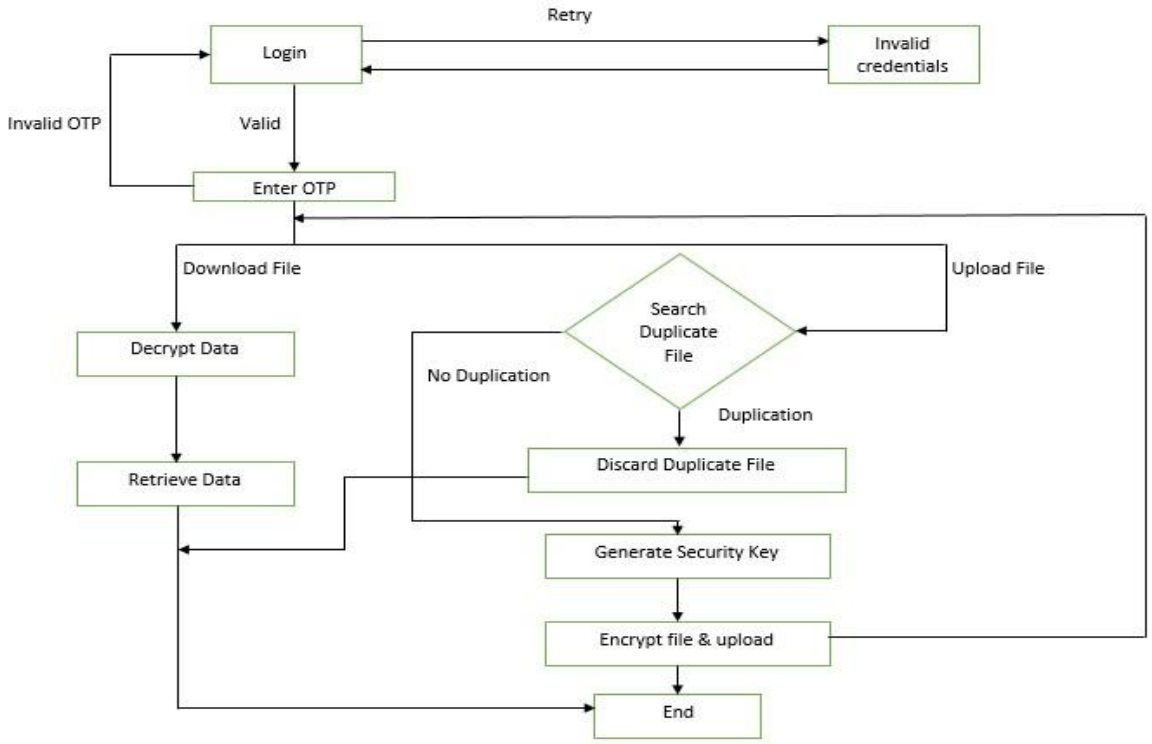

Fig 1: System Flow Diagram

After that user have to enter OTP which ensure strong user authenticity with two factor authentications, an extra layer of security is added to the account to prevent someone from logging in, even if password is already known. This extra security measure requires user to verify the identity using a randomized 6-digit code will be send to user each time attempt to log in [14]. Now user can either upload files on the cloud and can be download files from cloud. While uploading and downloading to ensure data security a hybrid cryptographic encryption technique is used that is different text files of different sizes are taken as input. After taking text file as input, AES algorithm is applied for encrypting the text file. AES will encrypt the text using a key which is not its own but generated by elliptic curve cryptography algorithm (ECC). Encrypted text file is uploaded to the server after encryption using AES. Client will download the encrypted file from the server. Using the same key generated by elliptic curve cryptography algorithm, client will decrypt the encrypted text. After decryption is successfully done client will have the original text file.

If user want to upload file on cloud it will be first check whether this file is already present on cloud or not this step ensure efficient use of storage by use of data deduplication. Data deduplication works by comparing chunks of data or objects (files) in order to detect duplicates. Deduplication can take place if the block of data file matches with other block of file which is there in the cloud then it should simply discard that duplicate file.

IV. PARTIAL IMPLEMENTATION

In the partial implementation the encryption and decryption of file, two step verification and data deduplication is done. But setup (installation) of cloud part is remaining and that will be completed soon. The encryption of particular file is done by using AES and ECC algorithm and that file contain the text which is stored as text.txt. The decryption of the same file is done properly and the file saved in project folder with name decrypted file. The OTP part is completed via authentication codes. The data deduplication program first finds files with matching sizes. It then runs an MD5 hash to find duplicate files. The MD5 hashing algorithm is a one-sided cryptographic function that accepts a text of any length as input and returns as output a fixed-length digest value to be used for authenticating the original text.

V. CONCLUSION

A Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion for that first required to implement AES and ECC encryption algorithm for strong data protection with efficiency. For that a Hybrid Cryptographic System (HCS) required which will combines the benefits of both symmetric and asymmetric encryption. During the design of the system to make sure of trusted authentication thereby allowing the feature of One Time Password (OTP) so user first enter login credential after that user have to enter OTP which ensure strong user authenticity. If user want to upload file on cloud then first it will be compare with stored files for duplication and if there is match then it will be discarded otherwise it will be store on cloud and by use of this technique data deduplication will be achieved. This data deduplication program first finds files with matching sizes. It then runs an MD5 hash to find duplicate files. Integrating all this features to make secure cloud and setup of cloud part is work in progress completed in future.

REFERENCES

[1] Akshay Arora, Anmol Rastogi, Abhirup Khanna, Amit Agarwal, "Cloud Security Ecosystem for Data Security and Privacy", 2017 7th International Conference on Cloud Computing, Data Science & Engineering.

[2] Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi, "Data Security in Cloud Computing Using AES Under HEROKU Cloud", 2018 27th Wireless and Optical Communication Conference (WOCC).

[3] Dhanaraj Suresh Patil, R. V. Mane, V.R.Ghorpade, "Improving the Availability and Reducing Redundancy using Deduplication of Cloud Storage System", 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA).

[4] Zhaocong Wen, Jinman Luo, Huajun Chen, Jiaxiao Meng, Xuan Li , Jin Li, "2014 International Conference on Intelligent Networking and Collaborative Systems", 2017 7th International Conference on Cloud Computing, Data Science & Engineering.

[5] Bhairavi Kesalkar, Dipali Bagade, Manjusha Barsagade, Namita Jakulwar, "Implementation of data deduplication using cloud computing", KITE/NCISRDC/IJARIIT/2018/CSE/105 IJARIIT(ISSN: 2454-132X).

[6] H. R. Nagesh, L Thejaswini, "Study on encryption methods to secure the privacy of the data and computation on encrypted data present at cloud", 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC).

[7] Bappaditya Jana, Jayanta Poray, Tamoghna Mandal, Malay Kule, "A multilevel encryption technique in cloud security", 2017 7th International Conference on Communication Systems and Network Technologies.

[8] Srinivas Mudepalli, V. Srinivasa Rao, R. Kiran Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing", International Conference on Intelligent Computing and Control Systems ICICCS 2017.

[9] Milind B. Waghmare, Suhasini V. Padwekar, "Survey on techniques for Authorized Deduplication of Encrypted data in Cloud", 2020 International Conference on Computer Communication and Informatics (ICCCI -2020), Jan. 22-24, 2020, Coimbatore, INDIA.

[10] Mr. Nishant N.Pachpor, Dr. Prakash S.Prasad, "Improving the Performance of System in Cloud by Using Selective Deduplication", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018) IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1.

[11] Chungsik Song, Younghee Park, Jerry Gao, Sri Kinnera Nanduri, William Zegers, "Favored Encryption Techniques for Cloud Storage", 2015 IEEE First International Conference on Big Data Computing Service and Applications.

[12] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based On Cloud Storage", 2017 IEEE 3rd International Conference on Big Data Security on Cloud.

[13] https://www.cloudflare.com/learning/cloud/what-is-the-cloud/, last accessed on: 12/10/2020.

[14] https://www.fidelity.com/security/how-two-factor-authentication-works/, last accessed on: 16/10/2020.