Online Data Security for Secure Cloud Storage

V. Bhavatharani[1] S. Jaisudha[2] S. Kaavya[3] N. Indira[4]
[1]Assistant Professor [2,3,4]Student
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]Panimalar Engineering College, Chennai, India

Abstract— The capacity benefit given by cloud server is not completely trusted by clients. In an existing data are corrupted by the unauthenticated user with the help of the employees. Normally the data are securely handled by the organization but some employees sold their access specifiers to the hackers for money. Due to this issue, the data are not safe. We can use the advanced safe technology. The data are uploaded by the encryption format with video mode and the data are downloaded by the user with the help of face detection video mode when the data user accept the user request by the face detection video mode. Then the data are shared from one place to another. Here we are using the Encryption algorithm to share the data.

Key words: Face Detection Video Mode, Uploading File, Downloading File

I. INTRODUCTION

Loud storage is an emerging model of storage to provide scalable, elastic and pay-as-you-use service to cloud computing users. For individual usage, the subscribers enjoy the freedom to access to their data anywhere, anytime with any device. When cloud storage is utilized by a group of users, it allows team members to synchronize and manage all shared documents. Moreover, it also saves the user a lot of capital investment of expensive storage equipments.

Cloud delivers convenience to the customers and at the same time arouses many security and privacy problems. Since the data are physically stored on the multiple servers of the cloud service provider, the customers cannot fully in charge of their data. They worry about the privacy of the stored documents since the server may be intruded by hacker or the data could be misused by the internal staff for commercial purpose. The customers prefer to adopt the encryption technology to protect the data confidentiality, which meanwhile arouses another problem: how to execute data retrieval on the large volume of cipher text. It is almost unimaginable to ask the cloud subscriber to download all of their stored information and then decrypt and search on the recovered plaintext documents. No customer could tolerate the huge transmission overhead and the waiting time for the data retrieval result. Searchable encryption technology not only exerts encryption protection of the data, but also supports efficient search function without undermining the data privacy. The data user generates a token of the content that he wants to search using his private key. Receiving the token, the cloud server searches on the encrypted data without decrypting the cipher text.

The most important point is that the server learns nothing about the plaintext of neither the encrypted data nor the searched content during the data retrieval procedure. However, most of the available searchable encryption schemes only support some basic search patterns, such as single keyword search, conjunctive keyword search and Boolean search. Since the cloud computing is a fierce competition industry, it is of vital importance to provide good user experience. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.

II. LITERATURE SURVEY

In paper [1] Two-Factor Data Security Protection Mechanism for Cloud Storage System is published by Joseph K. Liu; Kaitai Liang in 2015 with factor revocability for cloud storage system.There exists cryptographic primitive called "leakage-resilient encryption".

In the work published in 2017 [2] by Qingchen Zhang ; Laurence T. Yang for As one important technique of fuzzy clustering in data mining and pattern recognition, the possibilistic c-means algorithm (PCM) has been widely used in image analysis and knowledge discovery. PPHOPCM can effectively cluster a large number of heterogeneous data using cloud computing without disclosure of private data.

In 2014 QingjiZheng ; Shouhuai Xu [3] published a work that proposed using cloud-based storage service, users can remotely store their data to clouds but also enjoy the high quality data retrieval services, without the tedious and cumbersome local data storage and maintenance. The encrypted data can be effectively utilized. We realize fine-grained owner-enforced search authorization by exploiting ciphertext policy attribute-based encryption (CP-ABE) technique.

Next paper [4] proposed by Victor Chang; MuthuRamachandran in 2015 by Offering real-time data security for petabytes of data is important for cloud computing. A recent survey on cloud security states that the security of users' data has the highest priority. This paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data.

The principle motive of paper [5] is in recent years have witness a considerable advance of Internet of Things with the tremendous progress of communication theories and sensing technologies. A large number of data, usually referring to big data, have been generated from Internet of Things.

In the paper [6] published by Huaqun Wang in 2014 The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible.

In the work published in 2014 [7], by Jin Li ; Xiao Tan; Xiaofeng Chen; The challenge is that the computational burden is too huge for the users with resource-constrained devices to compute the public authentication tags of file blocks.

III. EXISTING SYSTEM

In an existing data are corrupted by the unauthenticated user with the help of the employees.

In a normally the data are securely handled by the organization but some employees sold their access specifiers to the hackers for money.

Cloud computing is that the use of computing resources (hardware and software) that are delivered as a service over a network. Today, cloud computing generates lots of hype; it's each promising and scary. Businesses see its potential however even several issues have.

Security is considered one among the foremost essential aspects in everyday computing, and it's no completely different for cloud computing because of the sensitivity and importance of information keep within the cloud. Cloud computing infrastructures use new technologies and services, most that haven't been totally evaluated with respect to security. Cloud Computing has many major problems and issues, like data security, trust, expectations, rules, and performance problems.

A. *Drawbacks in Existing System*

- The user can only sign documents on that particular computer.
- The security of the private key depends entirely on the security of the computer.
- Confidentiality is one amongst the most important problems round faced by cloud systems since the knowledge is keep at a remote location.
- Integrity is preventing the improper modification of data. Conserving integrity like confidentiality is another major issue round faced by cloud systems.

IV. PROPOSED SYSTEM

In this technique, the data are uploaded by the encryption format with video mode. The data are shared in Encryption algorithm so unauthorized user are not accept the data.

One approach to attain trustworthy computations in cloud infrastructures is to adapt existing trusted computing solutions to the cloud computing paradigm or to use these solutions as building blocks in new cloud design models. the foremost distinguished approach to trustworthy cloud computing technology are specific below this approach delivers a scalable cloud computing platform that has customers with end to end security and end to end privacy.

It will build security into its services in accordance with security best practices and documents the way to use the safety options. It's necessary that we leverage these safety features and best practices to style a befittingly secure application environment. Guaranteeing the confidentiality integrity and accessibility of knowledge.

A. *Advantages in Proposed System:*

- An encrypting algorithm scrambles the message and it can only be unscrambled with a key created at the same time.
- Cipher algorithms are either symmetric or asymmetric for encryption security.

V. ARCHITECTURE DIAGRAM

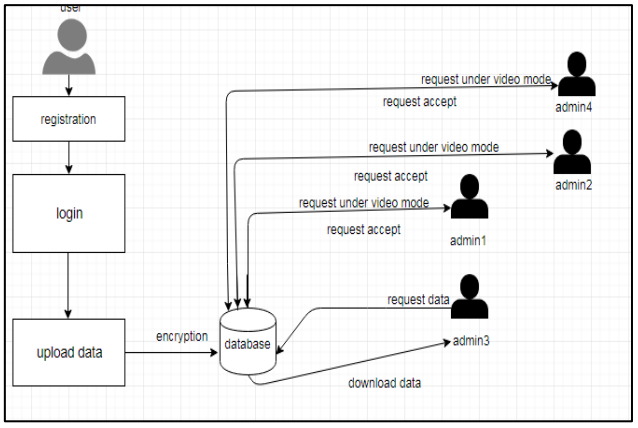


Fig. 1: System Architecture

A. *Explanation:*

Here user have to be register first after registration they have to be login after login .After login they can upload file after completion of file uploading that content will be encrypted it will be securable .That file will share to four admins if any user need that file they have to be register after login register after login they can send a request for file .for that request if four admins accepted then they can get the File. If any user hacked the remaining user can find that person face by using of web camera app .so it simple to identify.

VI. MODULE DESCRIPTION

- User interface design
- Login and File upload
- Security providing for File
- Admin Monitor
- View/Read File

A. *Module Description*

1) User Interface Design:

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

2) Login and File Upload:

User will login their account and upload a file or image, and that files/image are encrypt and store in admin side. Even uploaded user also doesn't access, before admin can accept.

3) Security Providing For File:

In this part Admin will maintain the file, if the one admin from the admin team wants file they wants an

acknowledgement of the other admins. The main motive is that secure the file.

4) Admin Monitor:

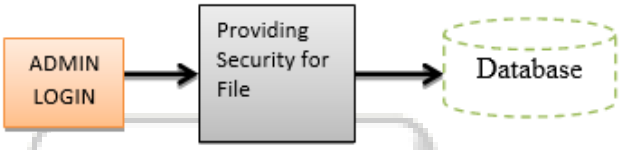
In this part admins will maintain the file, after that the admin will monitor the files in the way of video mode. If anyone of the admin from the admins team are going to request a file, the request will go by video mode.

5) View/Read File:

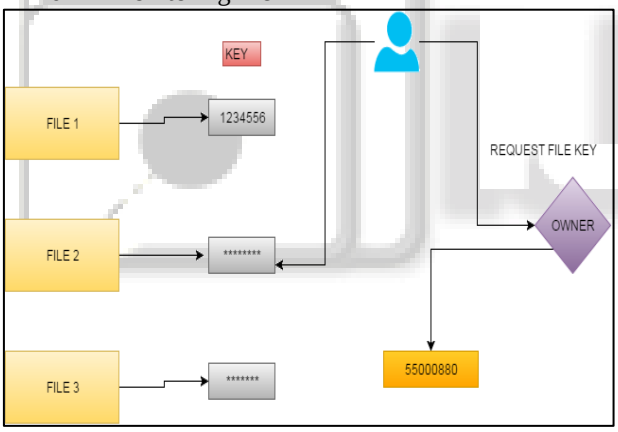
For reading each file which have been uploaded and split into 4 parts we should be owner of the file otherwise we should know the four different key which have been combined by random algorithm after reading the file you can also download the file otherwise with wrong key you can't open content.

– Login and File upload

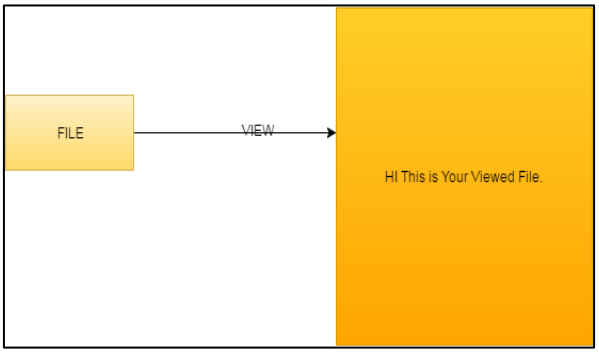
– Security providing for File



– Admin monitoring file



– View/Read File



VII. Conclusion

In this paper, we introduce a large universe searchable encryption scheme to protect the security of cloud storage system, which realizes regular language encryption and DFA search function. The cloud service provider could test whether the encrypted regular language in the encrypted cipher text is acceptable by the DFA embedded in the submitted search token. In the test procedure, no plaintext of the regular language or the DFA will be leaked to the cloud server. We also put forth a concrete construction with lightweight encryption and token generation algorithms. An example is given to show how the system works. The proposed scheme is privacy-preserving and indistinguishable against KGA, which are proved in standard model. The comparison and experiment result confirm the low transmission and computation overhead of the scheme.

VIII. Future Enhancement

An accumulation is often needed to gather the partial results from these parallel executions in different servers. The runtime system captures new events and run corresponding actions to analyze the page and store more URLs into the URL set to generate new events.

References

[1] Liu J K, Liang K, Susilo W, et al. Two-factor data security protection mechanism for cloud storage system[J]. IEEE Transactions on Computers, 2016, 65(6): 1992-2004.

[2] Zhang Q, Yang L T, Chen Z, Li P. PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.

[3] Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522C530. IEEE, 2014.

[4] Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.

[5] Zhang Q, Yang L T, Chen Z, Li P. Privacy-preserving doubleprojection deep computation model with crowdsourcing on cloud for big data feature learning[J]. IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735

[6] Wang H. Identity-based distributed provable data possession in multicloud storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.

[7] J, Tan X, Chen X, et al. Opor: Enabling proof of retrievability in cloud computing with resource-constrained devices[J]. IEEE Transactions on cloud computing, 2015, 3(2): 195-205.

