ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 20-24

Secure Cloud Storage with Face Detection Technology

M.Srudhi[1], V.Uma[2]

[1](cse, sriVenkateswara college of engineering and technology, India)
[2](cse, sriVenkateswara college of engineering and technology, India)

Abstract: *In any case, the capacity benefit gave by cloud server isn't completely trusted by clients. 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. Due to this issue, the data are not safe. To overcome this, we can go for the advance safe technology. In this technique, 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 only the data are shared from one place to another. In this technique, we are using the Encryption algorithm for share the data.*

Keywords: *secure cloud storage, regular language, searchable encryption, resist keyword guessing attack*

I. Introduction

Cloud 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 equipment's. Cloud delivers convenience to the customers and at the same time arouses many security and privacy problem. Since the data are physically stored on the multiple servers of the cloud service provider, the customers cannot fully in charge of their data.

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 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.

II. Implementation Techniques

2.1 The Java Framework

Java is a programming language originally developed by James Gosling at Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to bytecode that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere".

2.2 Object Oriented

1.Inheritance: It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding addition a features as needed.

2.Encapsulation: It is the mechanism of combining the information and providing the abstraction.

3.Polymorphism: As the name suggest one name multiple form, Polymorphism is the way of providing the different functionality by thefunctions having the same name based on the signatures of the methods.

4.Dynamic binding : Sometimes we don't have the knowledge of objects about their specific types while writing our code. It is the way of providing the maximum functionality to a program about the specific type at runtime.

2.3 Javaserver Pages - An Overview

Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. JSP provide excellent server side scripting support for creating database driven web applications. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy.

2.4 Evolution Of Web Applications

1. Scalability - a successful site will have more users and as the number of users is increasing fastly, the web applications have to scale correspondingly.

2. Integration of data and business logic - the web is just another way to conduct business, and so it should be able to use the same middle-tier and data-access code.

3. Manageability - web sites just keep getting bigger and we need some viable mechanism to manage the ever-increasing content and its interaction with business systems.

4. Personalization - adding a personal touch to the web page becomes an essential factor to keep our customer coming back again.

2.5 BENEFITS OF JSP

The JSP technology is platform independent, in its dynamic web pages, its web servers, and its underlying server components. That is, JSP pages perform perfectly without any hassle on any platform, run on any web server, and web-enabled application server. The JSP pages can be accessed from any web server.

2.6 Servlets

Earlier in client- server computing, each application had its own client program and it worked as a user interface and need to be installed on each user's personal computer. Most web applications use HTML/XHTML that are mostly supported by all the browsers and web pages are displayed to the client as static documents.

2.7 Java Servlets

Java Servlet is a generic server extension that means a java class can be loaded dynamically to expand the functionality of a server. Servlets are used with web servers and run inside a Java Virtual Machine (JVM) on the server so these are safe and portable.

III. Literature Survey

3.1 Two-Factor Data Security Protection Mechanism for Cloud Storage System.Joseph K. Liu, Kaitai Liang, Willy Susilo;2016

In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any ciphertext at any time. The security and efficiency analysis show that our system is not only secure but also practical.

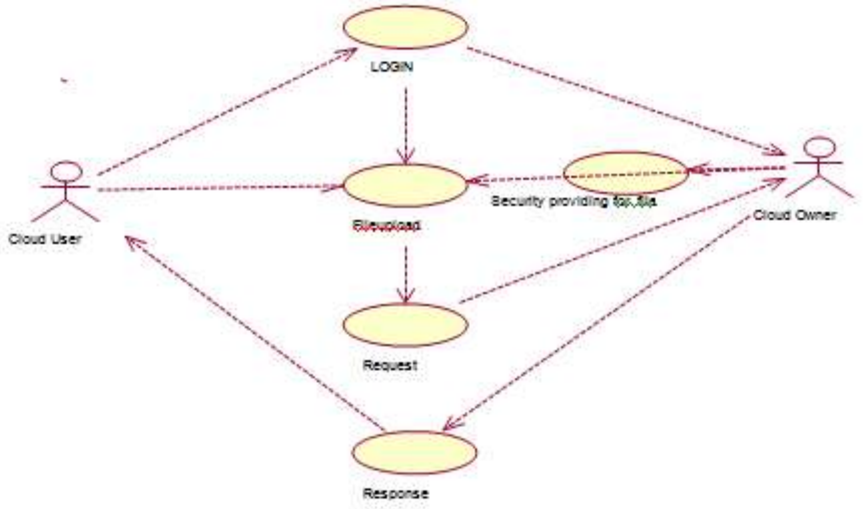
3.2 PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing.Qingchen Zhang, Laurence T. Yang, Zhikui Chen, and Peng Li.2017

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. However, it is difficult for PCM to produce a good result for clustering big data, especially for heterogenous data, since it is initially designed for only small structured dataset. To tackle this problem, the paper proposes a high-order PCM algorithm (HOPCM) for big data clustering by optimizing the objective function in the tensor space. Further, we design a distributed HOPCM method based on MapReduce for very large amounts of heterogeneous data.

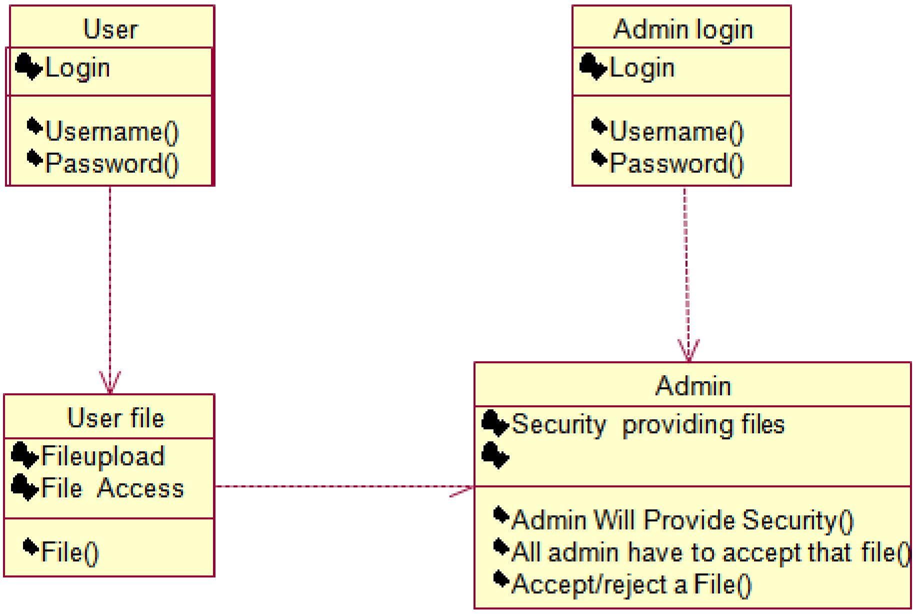
Finally, we devise a privacy-preserving HOPCM algorithm (PPHOPCM) to protect the private data on cloud by applying the BGV encryption scheme to HOPCM, In PPHOPCM, the functions for updating the membership matrix and clustering centers are approximated as polynomial functions to support the secure computing of the BGV scheme. Experimental results indicate that PPHOPCM can effectively cluster a large number of heterogeneous data using cloud computing without disclosure of private data..

IV. SYSTEM DESIGN

4.1 Use Case Diagram:



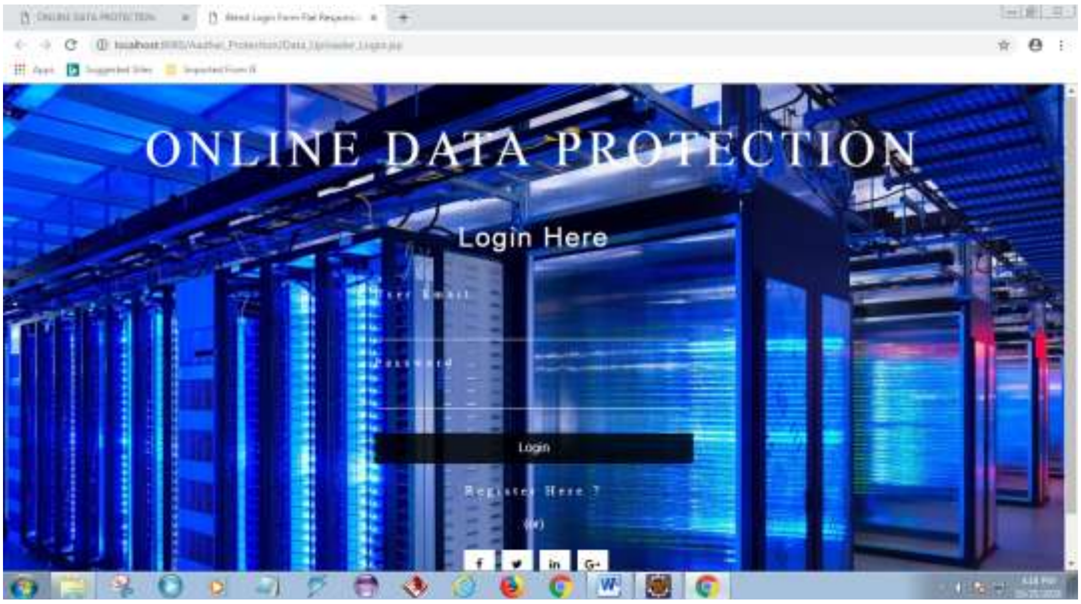
4.2 Class Diagram



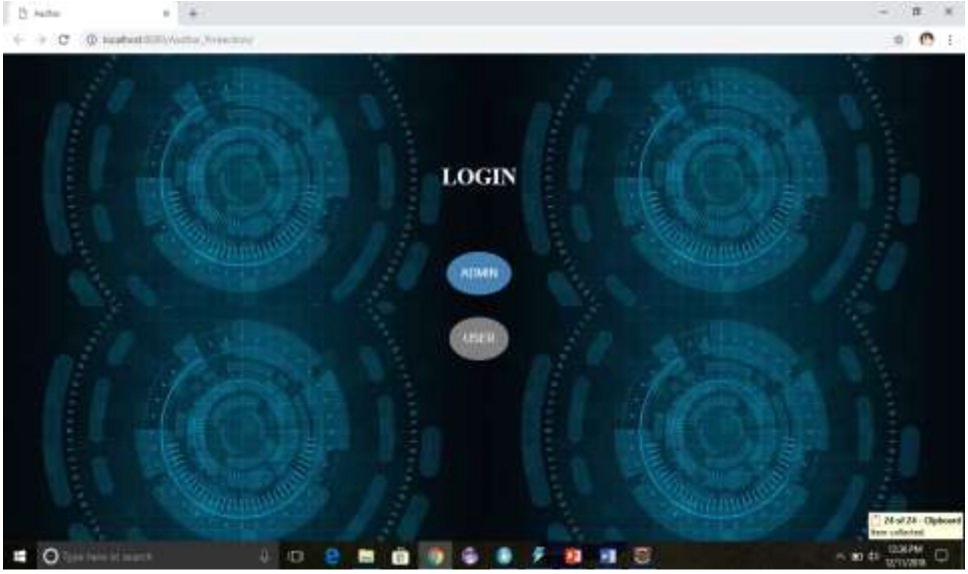
V. Module Description

5.1 User Interface Design:

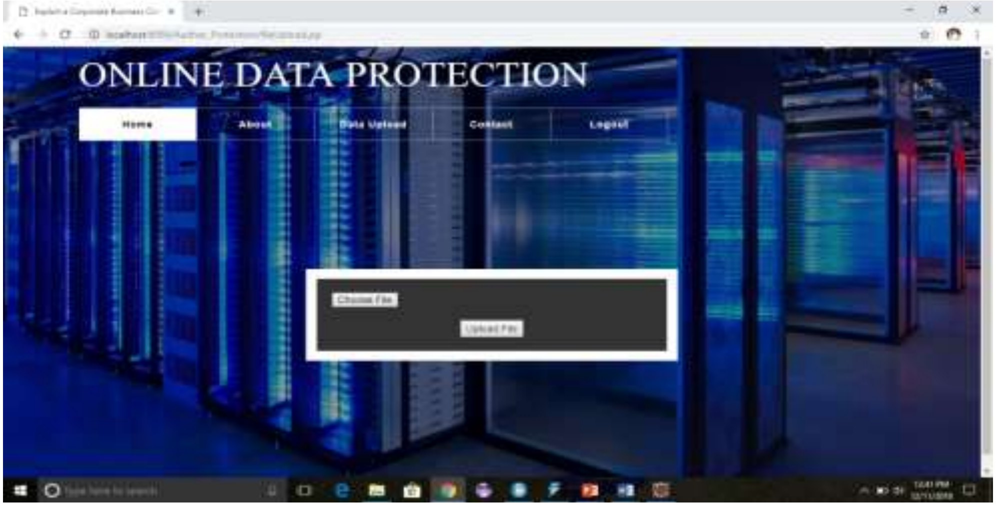
This is the first module of our project. Theimportant role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid 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.



5.2 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.



5.2 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.



5.2 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.

5.3 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.

5.4 **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.

VI. 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.

Acknowledgements

In future enhancement the design principle of this system is to reduce thetransmission, storage and computation burdens of the dataowners and the data users. Since the cloud server haspowerful computation resources, it is acceptable to offload a part of the users' computation burden to the cloud server.

References

[1]. Erl T, Cope R, Naserpour A. Cloud computing design patterns[M]. Prentice Hall Press, 2015.

[2]. Li Z, Dai Y, Chen G, et al. Toward network-level efficiency for cloud storage services[M]//Content Distribution for Mobile Internet: A Cloud-based Approach. Springer Singapore, 2016: 167-196.

[3]. 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.

[4]. 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.

[5]. 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.