International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Privacy Preserving and Proficient Identity Search Techniques for Cloud Data Safety

M Gayathri Devi[1], R Janitha Mangala Lakshmi[2], R. Reena[3], R. K Kapila Vani[4]

[1,2]*Student, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India*
[3,4]*Assistant Professor, Department, of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India*

Abstract *- Cloud computing is one type of computing platform that is Internet based. One important feature of a Cloud service is Cloud storage. The cloud users may upload sensitive data in the Cloud and allow the Cloud server to maintain these data. Cloud computing provides flexible data management and ubiquitous data access. However the cloud storage provided by the cloud computing is not trusted .Normally data are secured by the organizations but nowadays some employees sell their access specifications to the hackers for commercial purposes. This paper provides an efficient method based on identity techniques to overcome such issues.*

Key Words: *Visual-Encryption, Collective Behavior, Data Signing, Visual-Cryptography*

1. INTRODUCTION

Cloud storage is a model of storage of data with a highly virtualized infrastructure made up of many distributed resources. In the cloud storage, the data is remotely maintained and managed. The users can store their data online and are able to access from any part of the world via the Internet connection. The biggest advantage of storing data in Cloud is that the users are provided with a broader range of access to distributed resources in a cost-efficient manner. This is because it eliminates the capital expenses such as buying the hardware, software and setting it up. Though it has many appealing advantages as a promising platform for the internet, this new data storage paradigm brings many challenging issues which have profound influence on the usability, reliability and performance of the overall system. Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unpredicted advantages. Considering the outsourced data and the client's constrained resource capability ,the core of the problem can be generalized as how the client find an efficient way to perform verification without the local existence in the data files. In order to tackle this problem this paper provides privacy preserving scheme based on identity verification mechanism through real time alive face detection video mode.

2. RELATED WORK

(a) Personalized Search Over encrypted data – Zhangjie Fu

When we consider the data privacy and security, it is recommended practice to encrypt the data before we upload into database. One of the most familiar way to search the encrypted data is searchable encryption schemes. According to this paper, an user model to record and analyze the user's search history, has been developed. With this model, query extensions for accessing multiple files by the user cloud also be supported. Here, three main entities are involved: data owner, user and the database / cloud server. The user interest model is built upon the user's long term history. And if the user needs to access any file or database content, then he makes a click request to database. The rank is given to the user and based on that rank only the user could either be allowed or be denied to access the data and the ranking is based on the access frequency, keywords and relative words to the search.

(b) Proof of retrievability with resource constraints – Jin Li

One of the main concerned problem with data storage is that the data integrity verification at untrusted servers. Proof of Retrievability(PoR) model supports dynamic data operations, as well as ensure security against reset attacks in the cloud server. A strengthened security odel by considering the reset attack against the storage server in the upload phase of an integrity verification scheme has been developed. In this paper, only the verification schemes with public verifiability is considered, that is any person who knows the public key can act as a verifier. Hence according to this paper it seems to be more rational and practical to equip the verification protocol with public verifiability which is expected to play a more important role in achieving better efficiency for cloud computing.

(c) Preliminaries Searchable encryption

It is a technique that could provide security and protect the data privacy and meanwhile enabled leverged preserved approach with combined public key cryptography and utilize scheme of approval.

3. EXISTING METHODOLOGY

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Searchable encryption is a novel technique that could protect the data privacy and meanwhile enable keyword query over encrypted documents. The notion of key-aggregate searchable encryption such that the data owner only sends a single key to a user to share a huge quantity of files. A regular language searchable encryption system resisting off-line keyword guessing attack consists o key generation of user and cloud server. Here the existing system uses Data signing algorithm.

Technique Definition:- (Data Signing Algorithm)

The user can only sign documents on that particular computer. The security of the private key depends entirely on the security of the computer.

Limitations of 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.

4. PROPOSED SYSTEM

The secure framework has been proposed here to ensure and realize that the service provided ensures security and large volumes of data can be securely possessed. Combining with revocation and proof of retrievability, we provide an efficient scheme of identity verification of the client for dynamic data file operations on cloud. For this purpose, the technique named Visual-Crptographic Encryption(VC-E) has been used in our developed scheme.

Technique Definition:- (VC-E)

A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

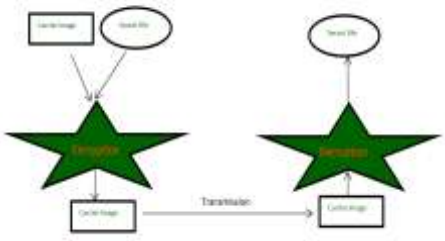

Fig. 1

Advantages of Proposed Scheme:-

- 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.

5. SYSTEM MODEL

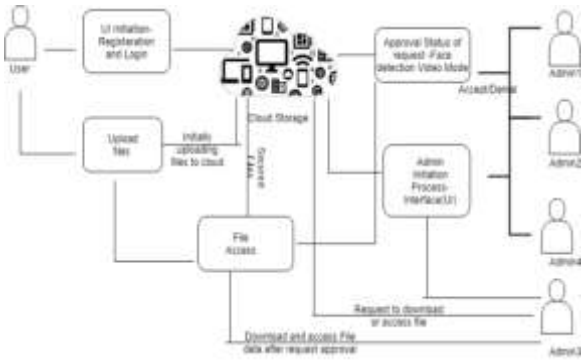

Fig. 2

The system architecture describes about the three major entities, namely, admins, user and the cloud server. This architecture defines about the various processes and operations taking place in the proposed scheme of our project. Here the cloud server is an important entity built over the logical perception of network. The user in the system plays the role in the phase of uploading file and admins involves in the rest of the UI request and response phases.

PHASES OF SYSTEM

1. USER INTERFACE DESIGN

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals (user-centered design). Interface design is involved in a wide range of projects from computer systems, all of the projects that involve much of the same basic human interactions. 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 been created for the security purpose. In this login page we have to enter login user id and password. It will check username and password and validated to check if the credentials are valid. If we enter any invalid username or password we can't enter into login window to user window it will show an error message. So we are preventing unauthorized user from entering into the login window to user window. It would provide a good security for our project. So server contain user id and password server also check the authentication of the user. It improves the security and prevents from unauthorized user entering into the network. Here we validate the login user and server authentication. In the first module, there are two possible logins exist. Where one of

them is for the user to log in to the cloud and proceed with uploading of file and the other is for the admin to login and view requests, approve them and permit the requester to download the file. After the requests are viewed, the admins could either approve (accept) or decline the request made by the one of the admin to download the file.

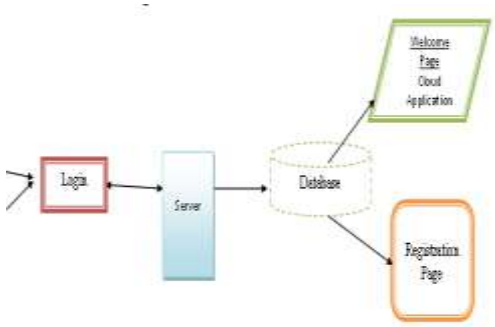

Fig. 3

2. F3ILE UPLOAD

The user will initially upload the files to the cloud that are secured by the face detection video mode. 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 cannot access, before admin can accept. This page is for uploading images and other media files. The users initially log in to their account for uploading the file. The uploaded file could then be downloaded if the admins approve the request by face detection video mode. Once the user log into the account and uploads file, after that the user himself also is not allowed to access or download file without the admin's approval.

3. PROVIDING SECURITY TO FILE

In this phase the main motto is to secure the files or data that are being uploaded by the user. Once if any of the admin requires a file to be accessed or downloaded for any purposes, they make a request. Here once of the request is made the request reaches rest of the admins so as to allow them to either accept one decline request by ensuring the security. When the request is made then the admins will be able to see three options available:

Options:

- View
- Accept
- Decline

All these options will enable the admins to ensure that the files are secured. So the module defines and ensures file security.

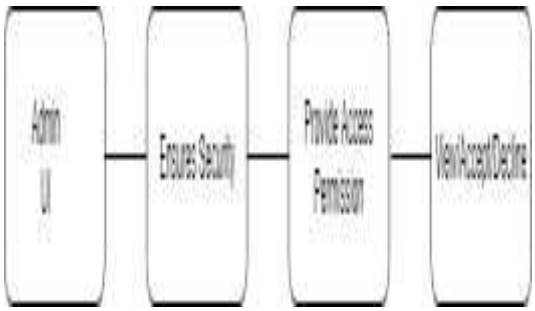

Fig. 4

4. ADMIN MONITORING PHASE

In this phase after the request for the file is been done it is sent to rest of the admins and then waits for the other admins to respond. Meantime the other admins notices the notification that has been sent. The notification contains the runtime video of the requested admin. The runtime video is been done using the application IP Webcam. This has a unique IP address which is to be given while sending the video request. Thus through this the other admins get a assurance that the requested admin is an authorized one.

Fig. 5

5. VIEW/READ FILE

- After all the admins check the notification and the runtime video they give their respond accordingly.
- They give their response either by accepting the request or declining it.
- Only when all the remaining admins have accepted the request the file could be accessed or downloaded by the admin.
- Even when one admin finds it insecure he could decline the request and the file could not be downloaded.

6. CONCLUSION AND FUTURE ENHANCEMENTS

CONCLUSION

In this paper, we had introduced a large universal searchable encryption scheme to protect the security of cloud storage system which realizes encryption and search function. The cloud service provider could test whether the encrypted cipher text is acceptable by the DFA embedded in the submitted search token. In the test procedure, no input data and secret information will be leaked to the cloud server. We also put forth a concrete construction with light-weight encryption and token generation algorithms. The proposed scheme is privacy-preserving and indistinguishable against Keyword Guessing Attack (KGA), which are proved in standard model. The comparison and experimental results confirms the low transmission and computational overhead of the scheme.

FUTURE ENHANCEMENTS

The new scheme performance proved that it efficiently secures the files for misuse by any of the admins and that it could use the resources provided when the problem size scaled up and even more it can be increased. Planned to implement a more effective approach by using more enhanced algorithms than using the VC-E algorithm to implement the new scheme.

7. REFERENCES

- Z.Fu, J.Shu, K.Ren. Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement. IEEE Transactions on Parallel and Distributed Systems, 2015.
- 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.
- Wang H. Identity-based distributed provable data possession in multicloud storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.
- Cui B, Liu Z, Wang L. Key-Aggregate Searchable Encryption (KASE)forGroupDataSharingviaCloudStorage[J].IEEE TRANSACTIONS ON COMPUTERS, 2014, 6(1): 1.
- Zhang Q, Yang L T, Chen Z, Li P. PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for BigData Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.
- Z. Shen, J. Shu, and W. Xue, "Preferred keyword search over encrypted data in cloud computing," In Proc. of 21st International Symposium on Quality of Service (IWQoS'13), 2013.