A SECURE SEARCHABLE ENCRYPTION FRAMEWORK FOR PRIVACY CRITICAL CLOUD STORAGE SERVICES

K Nivedha[1], Department of Computer Applications,
Mr, R. Ambikapathy[2], MCA, M.Phil., Assistant Professor,
Krishnasamy College of Engineering and Technology, Cuddalore.

ABSTRACT

Searchable encryption has received a attention from the research community with various constructions being each asymptotically optimal complexity for specific metrics (e.g., search, update). The recent attacks and deployment efforts have shown that the optimal asymptotic complexity. Dynamic Searchable Symmetric Encryption (DSSE) framework called Incidence Matrix (IM)-DSSE, which achieves a high level of privacy, efficient search/update, and low client storage with actual deployments on real cloud settings. Search and update operations can be performed effectively with minimal information leakage. The client to perform search and update operations in a secure manner, in which files can be securely retrieved/updated while leaking least information to the server.

Keywords: Search, Update, Encryption.

INTRODUCTION

The rise of cloud storage and computing services provides vast benefits to the society and IT industry. One of the most important cloud services is data Storage-as-a-Service (SaaS), which can significantly reduce the cost of data management via continuous service, expertise and maintenance for resource-limited clients such as individuals or small/medium businesses. Despite its benefits, SaaS also brings significant security and privacy concerns to the user. That is, once a client outsource his/her own data to the cloud, sensitive information (e.g., email) might be exploited by a malicious party (e.g., malware). Although standard encryption schemes such as Advanced Encryption Standard (AES) can provide confidentiality, they also prevent the client from querying encrypted data from the cloud. This privacy versus data utilization dilemma may significantly degrade the benefits and usability of cloud systems. Therefore, it is vital to develop privacy-enhancing technologies that can address this problem while retaining the practicality of the underlying cloud service.

EXISTING SYSTEM

- Storage-as-a-Service (SaaS), which can significantly reduce the cost of data management via continuous service, expertise and maintenance for resource-limited clients such as individuals or small/medium businesses.
- SaaS also brings significant security and privacy concerns to the user. Once a client outsource his/her own data to the cloud, sensitive information (e.g., email) might be exploited by a malicious party (e.g., malware).

Drawbacks of Existing System

- Sensitive information might be exploited by a malicious party.
- Security and privacy concerns to the user.
- No dynamism on searching data
- Lack of update capacity

PROPOSED SYSTEM

- New DSSE framework which can achieve a high security and be compatible with current cloud infrastructure.
- Privacy-preserving email and file storage services, where the client can be able to store, search and update their sensitive data (e.g., email, photos) on the cloud.

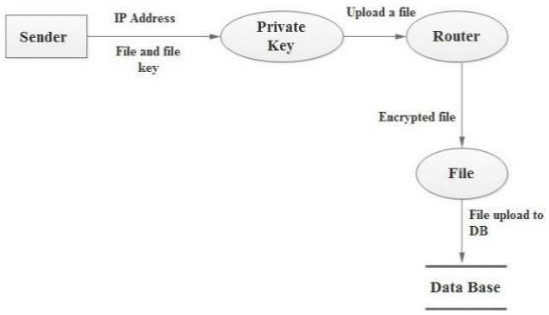
Advantages of Proposed System

- Highly secure against File-Injection Attacks
- As a significant improvement over the preliminary version,
- Updates with Improved Features
- High performance analysis of each scheme with different hardware and network settings.

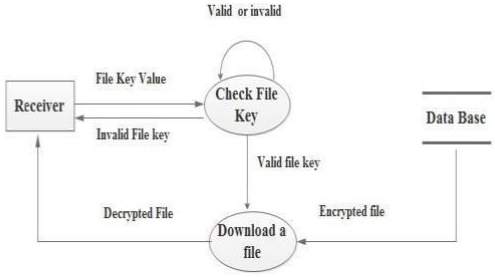
DATA FLOW DIAGRAM

Data flow diagram are represented below

Level 1



Level 2



MODULES

The modules are listed below

- Authorize clients
- Upload file into encrypt format
- Data store
- View files
- Uploaded files
- Retrieve file into decrypt format
- File content attack details

MODULE DESCRIPTION

Authorize clients

Authorization is a process by which a server determines if the **client** has permission to use a resource or access a file.

The below figure represents the authorize data owners.

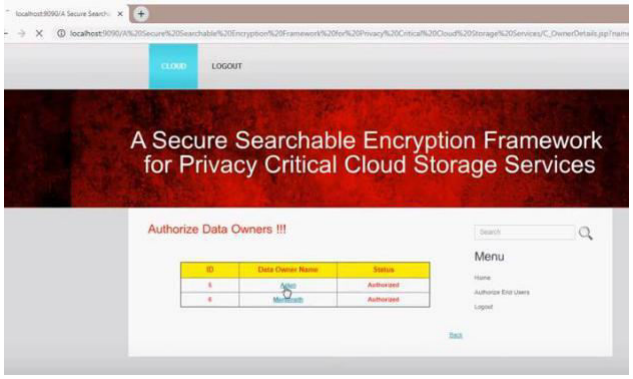


Figure 1- Authorize data owners

Upload file into encrypt format

- The **translation** of data into secret code. **Encryption** is the most effective way to achieve data security.
- Secret key or password that enables you to decrypt it.

The below figure represents the file upload.

Figure 2- Uploaded files **Data store**

A data store is a respirate for persistently storing and managing collections of data.

View files

- A file viewer is an application software that present the data stored in a computer file.
- The file contents are generally displayed on the screen.

Uploaded files

Uploading is the transmission of a file from one computer system to another, usually larger computer system.

Retrieve file into decrypt format

- The conversion of encrypted data into its original form is called decryption.
- It is generally a reverse process of decryption.

File content attack details

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove or reveal information without authorized access permission.

CONCLUSION

In this article, we presented IM-DSSE, a new DSSE framework which offers very high privacy, efficient updates, low search latency simultaneously. Our constructions rely on a simple yet efficient incidence matrix data structure in combination with two hash tables that allow efficient and secure search and update operations. Our framework offers various DSSE construction, which are specifically designed to meet the needs of cloud infrastructure and personal usage in different applications and environments. All of our

schemes in IM-DSSE framework are proven to be secure and achieve the highest privacy among their counterparts. We conducted a detailed experimental analysis to evaluate the performance of our schemes on real Amazon EC2 cloud systems. The achieved results showed the high practicality of our framework even when deployed on mobile devices with large datasets. We released the full--edged implementation of our framework for public use and analysis.

REFERENCE

Thang Hoang, Attila A. Yavuz, Member, IEEE and Jorge Guajardo, "A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services", IEEE Transactions on Services Computing, 2019.