EFFICIENT REGULAR LANGUAGE SEARCH CLOUD STORAGE

Mr. C. Palani Nehru, Assistant Professor, Dhanalakshmi Srinivasan College of Engineering and Technology
Mr. R. Anandan, Assistant Professor, Dhanalakshmi Srinivasan College of Engineering and Technology
Chandini G:, Student, Dhanalakshmi Srinivasan College of Engineering and Technology

ABSTRACT Cloud computing provides flexible data management and ubiquitous data access. However, the storage service provided by cloud server is not fully trusted by customers. Searchable encryption could simultaneously provide the functions of confidentiality protection and privacy-preserving data retrieval, which is a vital tool for secure storage. In this paper, we propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. The large universe construction ensures the extendability of the system, in which the symbol set does not need to be predefined. Multiple users are supported in the system, and the user could generate a DFA token using his own private key without interacting with the key generation center. Furthermore, the concrete scheme is efficient and formally proved secure in standard model. Extensive comparison and simulation show that this scheme has function and performance superior than other schemes.

KEYWORDS:- Cloud, Deterministic finite automata, Efficient regular language,Secure

1. INTRODUCTION

The main aim of this work is to provide integrity of an organization data's which is in public cloud and retrieving data's

in encrypted form and retrieving information.

Project ScopeIn this work, cloud storage of secured data's of various fields and retrieving those data's whenever necessary. All those data's will be in different formats like text, image, video etc and all these will be encrypted and stored in database DFA search technique is used to read the data's in the form of encrypted data and convert the data's into regular language and display those information to authorized user whenever they need. In server side operations they can also manipulate all the data's which they uploaded.

Product Perspective

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.

[Type text]

2. MATERIALS AND METHOD

The purpose of the System Analysis is to produce the brief analysis task and also to establish complete information about the concept, behavior and other constraints such as performance measure and system optimization. The goal of System Analysis is to completely specify the technical details for the main concept in a project. In existing system the data's which are uploaded by the server side are all Stored in the database with all formats in the regular language so that the security of data's are very less and there is a possibility of information theft and information loss possibility is there, so in future only encrypted data's alone should be stored in cloud.

Most of the available searchable encryption schemes only support some basic search patterns, such as single keyword search, conjunctive keyword search and boolean search. Existing Searchable encryption technology not only make use of 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 ciphertext. 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. 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.

An efficient large universe regular language searchable encryption scheme for the cloud is proposed which provides privacy-preserving and secure against the off-line keyword guessing attack (KGA). In this project, the encryption algorithm takes as input a public key and regular language described string with arbitrary length. Then, the generated ciphertext is outsourced to cloud server. In the data retrieval phase, user defines a deterministic finite automata (DFA) and generates a search token of the DFA using his secret key. The DFA defines a set of transitions, an initial state and an accept state. If and only if the regular language embedded in the ciphertext is acceptable by the DFA of the search token, the file will be regarded as a match file. This test process is executed by the cloud server without knowing any plaintext of the regular language and the DFA. Olnpropsedsytem, confedential data access will be secured by setting the search previlages for the users and also triple DES technique has used. Software is divided into separately named and addressable components called modules that are integrated to satisfy problem requirements. Modularity is the single attribute of software that allows a program to be intellectually manageable. A module is a part of a program. Programs are composed of one or more independently developed modules that are not combined until the program is linked. A single module can contain one or several routines. The proposed system consists of four main modules. They are:

- Safe page file upload
- Authorized user's page to access cloud
- Server side data manipulation
- 4)Data owner and user authentication

[Type text]

- Due to this design of Triple DES as an encrypt—decrypt—encrypt process, it is possible to use a 3 TDES (hardware) implementation for single DES by setting Kl K2 and to be the same value. This provides backwards compatibility with DES.
- Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K l. In other words, user encrypt plaintext blocks with key Kl, then decrypt with key K2, and finally encrypt with Kl again. Therefore, 2TDES has a key length of 112 bits.
- Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.
- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
- A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

3. RESULTS AND DISCUSSIONS

The requirement specification is a technical specification of requirements for the software products. It is the first step in requirement analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenario from the user, an operational and an administrative perspective. The purpose of software requirement specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface , hardware and software requirements. It defines how the client ,team and audience see the project and its functionality.

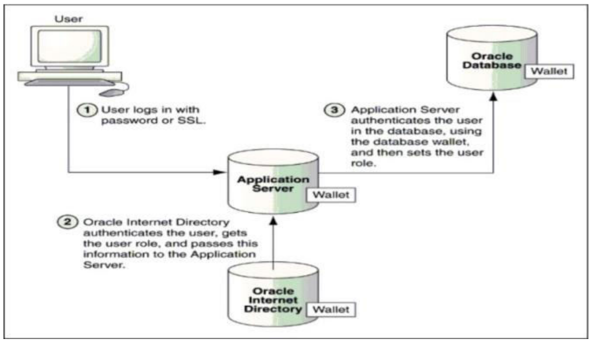
User
Oracle Database
Wallet
① User logs in with password or SSL.
③ Application Server authenticates the user in the database, using the database wallet, and then sets the user role.
Application Server
Wallet
② Oracle Internet Directory authenticates the user, gets the user role, and passes this information to the Application Server.
Oracle Internet Directory
Wallet

Fig. 3.1 Architecture Diagram

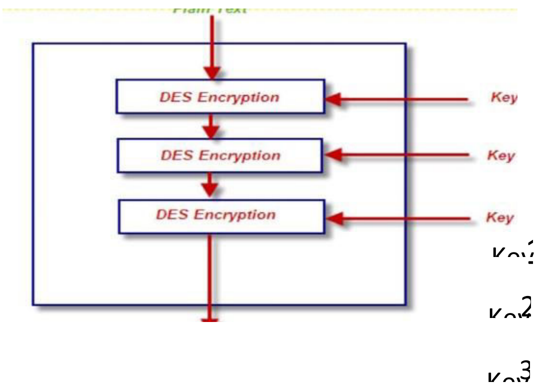

Fig. 3.2. TRIPLE DES

Algorithm(Encryption)Plain

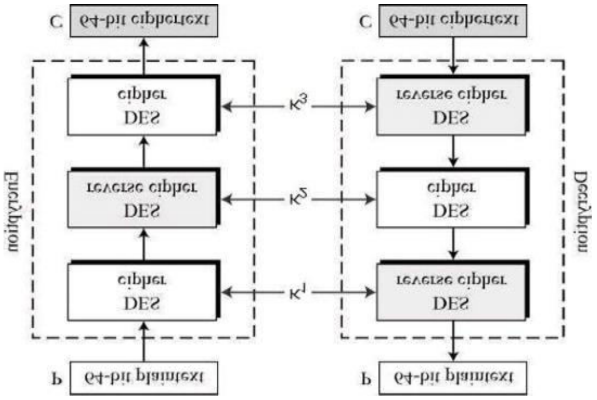

Fig.3..3 TRIPLE DES DATA FLOW DIAGRAM

4. CONCLUSION

In our User Plain password Hash Hashed password Generate negative password encrypt Authentication data table International Journal of Engineering Research & Technology .. ENPs. In the end, we analyzed and compared the attack complexity of hashed password, salted password, key stretching and the ENP. Here we introduced 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. For future work, 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

[l]. A. 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]. Sookhak M, Gani A, KhanMK, et al. Dynamic remote data auditing for securing big data storage in cloud computing [J]. Information Sciences, 2017, 380:101-116.

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

[5]. 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.

[6]. 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.

[7]. Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[C]//Theory of Cryptography Conference. Springer Berlin Heidelberg, 2007:535-554.