INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2334 - 2338
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

FINE GRAINED AND KEY-AGGREGATE BASED VULNERABLE DATA ACCESS CONTROL IN CLOUD COMPUTING

S.Sowmiya, PG Scholar, Dept Of Computer Science Engineering, Mailam Engineering College, Villupuram.

P.R.Jayanthi, Associate Professor Of Computer Science Engineering, Mailam Engineering College, Villupuram.

Abstract:

Data sharing is an important functionality in cloud storage for searchable encryption. In this paper, we describe how to securely, efficiently and flexibly share data over multi users in cloud storage. We developed a secret key for multi users which are group key and normal single key. We describe group key as a constant-size ciphertexts. Such that efficient delegation of decryption rights for any set of ciphertexts are possible. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. We provide formal security analysis of our schemes in the standard model. In this paper, we developed AES algorithm for secret key generation. In which a data owner only needs to distribute a group key and normal single key for each file or more than one file to the user for data privacy purpose.

Keywords: Data Sharing, Searchable Encryption, Group Key, Data Privacy, cloud storage.

1. INTRODUCTION

Cloud computing is a recently evolved computing terminology based on utility and consumption of computing resources. It involves groups of remote servers and software networks that allow centralized data storage and online access to computer services .cloud storage emerged as a solution of data shared over the internet. Clouds can be classified as public, private or hybrid. Cloud computing relies on sharing of resources over a network to achieve coherence.

Fig.1. Cloud Structure

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2334 - 2338
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

Cloud computing focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per some limitations. This can work for allocating resources to users. Cloud computing facility serves different users from different places. This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space etc. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses. To deploy their applications, cloud users must install operating-system and their application software on the cloud infrastructure. In this, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill Iaas services on a utility computing basis.

2. RELATED WORK

Cloud services includes a platform as a service for applications and other development. What developers gain with Paas is the framework they can build upon to develop. It makes the development, testing and deployment of applications simple and quick. In this model, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity. Some PaaS offers like Microsoft Azure and google app engine, the underlying computer and storage resources scale automatically to match application demand, then the cloud user does not have to allocate resource manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environment. Even more specific application types can be provided via PaaS, such as media encoding as provided by services as bitcoding , transcoding cloud.

Saas is also one of the service in the cloud. This can applicable, in the business model using software as a service(SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud. Cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud users own computers,which simplifies maintenance and support. Cloud applications are different from other applications in their scalability. Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user,who sees only a single access point. To accommodate a large number of cloud users.

3. DESIGN SYSTEM

This implies the necessity of securely distributing to users a large number of keys for both encryption and search ,and those users will have to securely store the received keys and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data .the implied need for secure communication , storage and complexity clearly renders the approach impractical. To overcome the problem which is in existing system ,by proposing the novel concept of key aggregate searchable encryption(KASE) and instantiating the concept concrete KASE scheme,in which a data owner only needs to distribute a group key and single key to a user for sharing a large number of documents, and the user

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2334 - 2338
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

only needs to submit a group key and normal key to the cloud for each file querying the shared documents by using AES (Advanced Encryption Standard)algorithm. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient. We first define a general framework of key aggregate searchable encryption(KASE) composed of seven polynomial algorithms for security parameter.

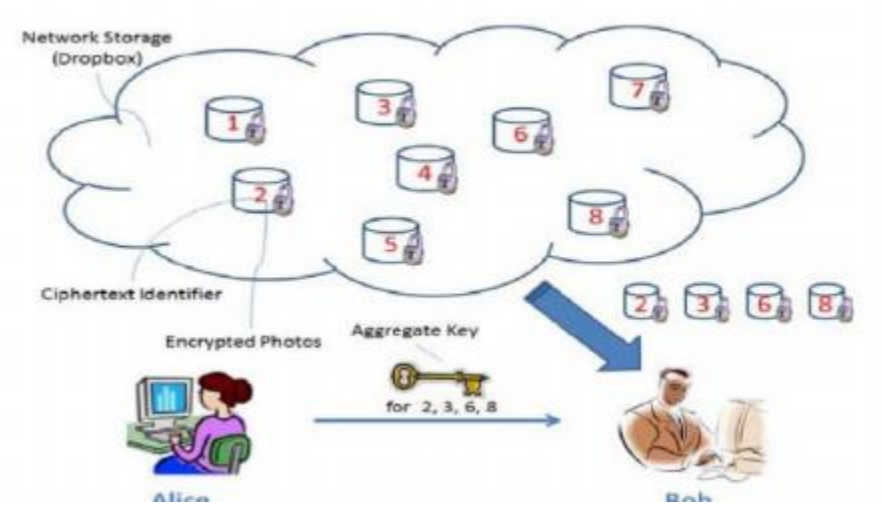

Fig.2.System Architecture

Architecture of the system consists two actors, one is the data owner Alice and other one is the user Bob. Here the data owner sends a aggregate key that is also consider as group key send to authorized users who are already registered in owner website. Here we developed two types of keys i.e one is group key for group of files ,and also single key for single file. group key is for more secure to data. Data owner can upload only .txt files to cloud server.

AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

4. ANALYSIS

AES is an iterative rather than Feistel cipher. It is based on „substitution–permutation network". It comprises of a series of linked operations, which involves to replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2334 - 2338
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

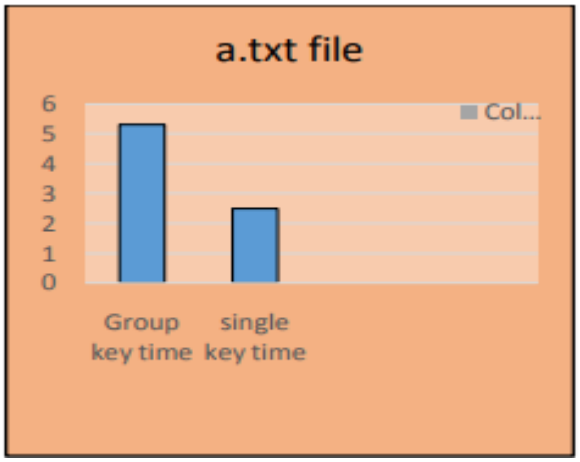

Fig.3. System Architecture

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns. Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round. The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related. The process of decryption of an AES ciphertext is similar to the encryption process ,in the reverse order. Each round consists of the four processes conducted in the reverse order.

CONCLUSION

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we first propose the concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage. However, if a user wants to query over documents shared by multiple owners, he must generate multiple group keys and single keys to the cloud, for more security.

REFERENCES

[1] F.Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.

[2]https://www.cloudendure.com/blog/top-6-cloud-computing-books-read-2016/

[3]https://journalofcloudcomputing.springeropen.com/

[4]https://www.ieee.org/conferences_events/conferences/conferencedetails/index.html?Conf_ID=36860

[5]http://tgs.freshpatents.com/Cloud-Computing-bx1.php

[6] cloud computing website http://www.explainthatstuff.com/cloud-computing-introduction.html [7] web page in http://www.htmlgoodies.com/beyond/webmaster/toolbox/article.php/3900716/Cloud-Computing-for-Web-Developers.html.