IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

A Novel Approach for Sharing Encrypted Data Over Cloud

Prof B.S. Vamsi Krishna[1], Bingi Anu Reshma[2]

Professor, Dept of Computer Science Engineering, MVGR College of Engineering, Vizianagaram, Andhra Pradesh[1]

Student, Dept of Computer Science Engineering, MVGR College of Engineering, Vizianagaram, Andhra Pradesh[2]

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.

I. 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.
Public cloud: Any one can share data over public cloud.
Private cloud: Authorized users only access data from cloud.
Hybrid cloud: It is an computing environment, it uses a mix of on-premises, private cloud and third – party, public cloud services.

Fig 1: Types of cloud

Cloud computing relies on sharing of resources over a network to achieve coherence. 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.

Cloud services:
Infrastructure as a service (Iaas)
Infrastructure as a service in cloud represents the cloud infrastructure are self service models for accessing monitoring and managing remote data center infrastructure.
Egg: firewalls
IaaS-cloud service providers supply these resources on-demand from their large pools in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

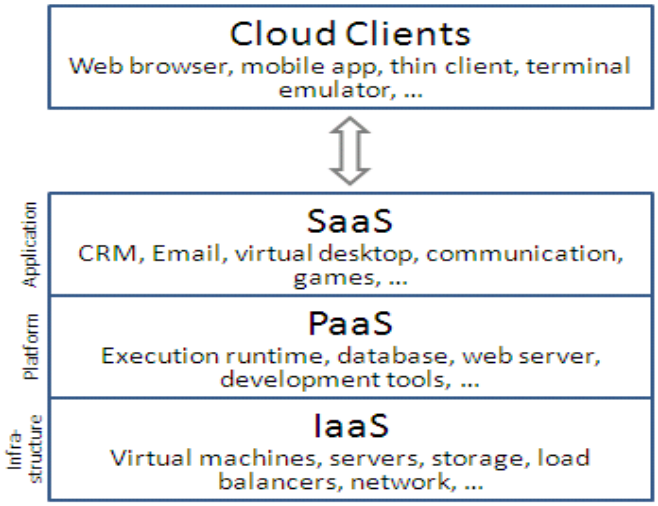

Fig 2: Services of cloud

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.

Platform as a service(PaaS)
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 or media.io.

Software as a service(SaaS)
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.

Problem statement:
In this project, the data owner sends keys for different files to user.so that the number of keys are increases including the number of files increases. To overcome this problem, and for more security we use KASE scheme by using AES algorithm ,we can implement the concept KASE. Because we can't find which user can access which file at which time. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.

II. RELATED WORK

1. Multi –user keyword search scheme for secure data sharing with fine grained access control
F. Zhao, T. Nishide , K. Sakurai are proposed a paper "multi-user keyword search scheme for secure data sharing with fine-grained access control" .There is a rich literature on searchable encryption, including SSE(searchable

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

symmetric encryption) schemes and PEKS schemes. In the context of cloud storage, keyword search under the multi-tenancy setting is a common scenario. In such scenario, the data owner would like to share a document with a group of authorized users, and each user who has the access right can provide a trapdoor to perform the keyword search over the shared document, namely ,the "multi-user searchable encryption "(MUSE) scenario.

In attribute based encryption (ABE) is applied to achieve fine-grained access control aware keyword search. As a result, in MUSE ,the main problem is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered. Key aggregate searchable encryption can provide the solution for the latter ,and it can make MUSE more efficient and particular.

2. Multi-key searchable encryption".

R.A .Popa ,N. Zeldovich proposed a paper multi-key searchable encryption" In the case of a multi-user application ,considering that the number of trapdoors is proportional to the number of documents to search over(if the user provides to the server a keyword trapdoor under each key with which a matching document might be encrypted), popa firstly introduces the concept of multi-key searchable encryption (MKSE). MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoors keyword in documents encrypted with different keys. The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user. This approach of MKSE inspires us to focus on the problem of keyword search over a group of shared documents from the same user in the multi user applications,and the adjust process in MKSE also provides a general approach to perform keyword search over a group of documents with only one trapdoor. However the adjust process of MKSE needs a delta generated from both users key and SE key of the document.

3. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

S. Yu, C. Wang, K. Ren, and W. Lou,Cloud computing ,this paradigm also brings many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by data decryption keys only to authorized users. However, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired,. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses the challenging open issue by, one hand defining and enforcing access policies based on data attributes and on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

4. Public Key Encryption with Keyword Search

D. Boneh, C. G, R. Ostrovsky, G. Persiano The problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user, Alice encrypted under Alice's public key, an email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search.

III. ANALYSIS AND DESIGN

System Analysis

Existing 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.

Disadvantages of existing system:

- Unexpected privilege escalation will expose all
- It is not efficient.
- Shared data will not be secure.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Proposed System:
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 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.

Advantages of proposed system
- It is more secure.
- Decryption key should be sent via a secure channel and kept secret.
- It is an efficient public –key encryption scheme which supports flexible delegation.
- To the best of our knowledge,the KASE scheme proposed in this paper is the first known scheme that can satisfy requirements.

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.

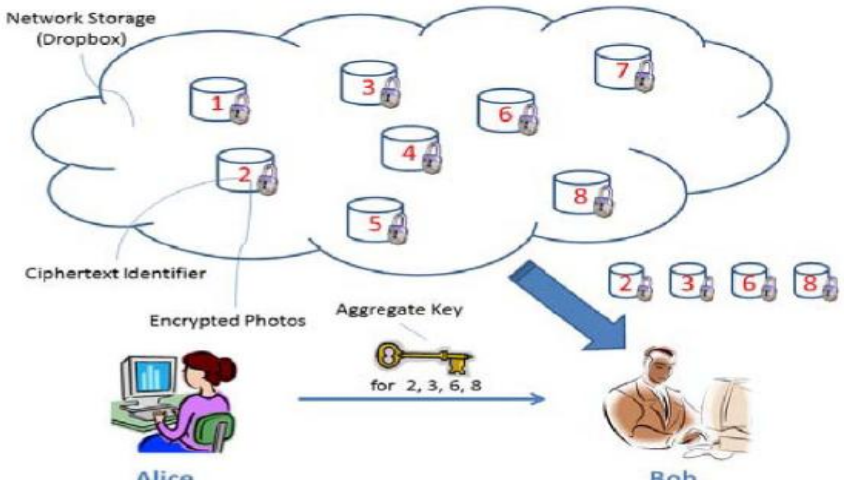

Fig 3: system architecture

Here we does not develop trapdoor key, only develop secret key(group key) for group of files and also single key.

Setup
This is run by the owner to set up the scheme. It takes as input a security parameter and outputs the necessary keys.

Encrypt
This algorithm is run by the data owner to encrypt the document and generate its keywords' ciphertexts. For each document it will generate single key. When more than one files uploaded and shared then data owner will be send group key and single key of single files.

Decrypt
This is run by user to decrypt files by using secure keys which are generated by data owner through secure channel ex:email.

AES Algorithm: The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) network. The more popular and widely adopted symmetric encryption algorithm is the Advanced Encryption Standard (AES). Its found as six time faster than triple DES.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

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.

The features of AES are

- Symmetric key and block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES

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 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.

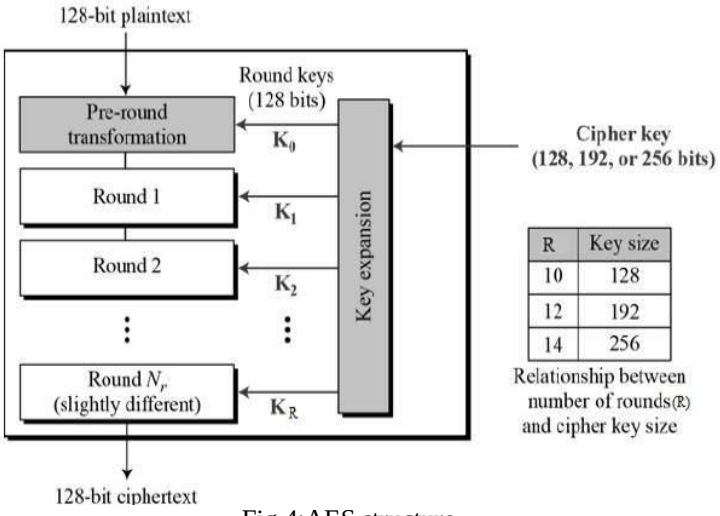

Fig 4:AES structure

Encryption Process works as:

Here, we defined to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process as below:

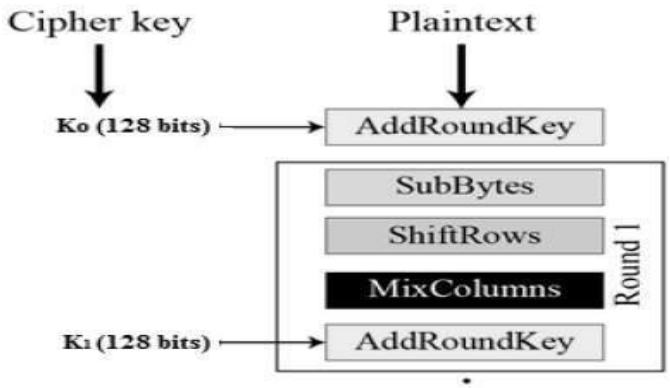

Fig 5 **:** Encryption process

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Byte Substitution (SubBytes)
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.

Shiftrows
Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix 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.

Addroundkey
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.

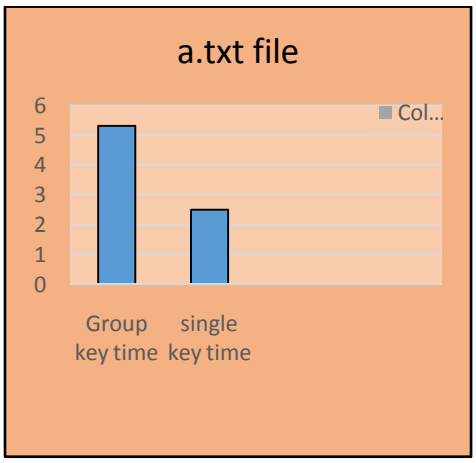

Fig 6:key generation time

Decryption Process
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

- Add round key
- Mix columns
- Shift rows
- Byte substitution

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.

IV. 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.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

In a KASE scheme, the owner only needs to distribute a single key to a user and also send group key(aggregate key) for group of files when sharing lots of documents with the user, then the user only needs to submit a group key and single key when he queries over all documents shared by the same owner. 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.htm
[8] Leica Manual and Data Book" http://ieeexplore.ieee.org/document/7254697/
[9] Master thesis by Rehan saleem https://lup.lub.lu.se/luur/download?func=download File&recordOId=1764306&fileOId=1764311
[10] Technical report by Prashant gupta https://www.slideshare.net/swtprashu/report-on-cloud-computing-by-prashant-gupta
[11] Collusion resistant broadcast encryption with short ciphertexts and private key. https://link.springer.com/chapter/10.1007/11535218_16
[12] Data security and privacy in wireless body area networks" http://ieeexplore.ieee.org/document/5416350/