Enhance Privacy Preserving Data Encryption over Multi keyword Ranked Search in Cloud Computing

Ms. Aamrapali Murlidhar Tamgadge
R.T.M. Nagpur University, India

Abstract— An enhance privacy preserving data using multi-keyword ranked search scheme over encrypted cloud data increasing popularity of cloud computing, data owners are motivated to share data to the cloud server's security and cost reduction. Data should be encrypted before outsourcing to any site for privacy and security purpose. In this paper, we present a multi-keyword ranked search over encrypted cloud server, which supports insertion and deletion with encryption and decryption of files (text/audio/video files), for this we construct a special Advanced Encryption Standard, also known by its original name Rijndael.

Key words: Cloud Computing, Rijndael Algorithm, Infrastructure, Internet, DES, AES, Encryption, Decryption

I. INTRODUCTION

Cloud server enable users to enjoy on-demand network access to a shared pool of configurable resources with great efficiency with the minimal overhead. As of this individuals and enterprises are being motivated to share their data to the cloud server .Abundant works have been proposed under different models to achieve searching functionality, such as single, multi-keyword, ranked, multi-keyword ranked search, etc. Recently, some dynamic schemes have been proposed to support insertion-deletion over encryption-decryption. This paper proposees secure tree-based search scheme over encrypted cloud data, which supports multi-keyword ranked search and dynamic operation on the document collection. Specifically, the vector space model, the widely used "Term Frequency (TF) × Inverse Document Frequency (IDF)" models are combined in the index construction and query generation to provide multi-keyword ranked search scheme. In order to obtain high search efficiency, we construct a tree-based index structure and propose a "Greedy Depth-first Search" algorithm based on this index tree. The secure AES algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors.

1) Here we design a searchable encryption scheme that supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection.
2) The special structure of the tree based index seaching kept the complexity of the proposed scheme fundamentally logarithmic.
3) Encryption and Decryption of files using Advanced Encryption Standard (AES)

II. LITERATURE REVIEW

Cao et al. [26] realized first privacy preserving multi keyword ranked search, in which documents and queries are represented as vectors of dictionary size. With coordinate matching, documents are ranked according to the number of matching keywords.

However, Cao et al.'s scheme does not consider the importance of different keywords, thus is not accurate enough. In addition, the search efficiency of the scheme is linear with the cardinality of collection of document.

Sun et al. [27] presented a secure multi-keyword search scheme which supports similarity based ranking. The authors constructed a special searchable index tree based on vector space model and adopted cosine measure together with TF*IDF to provide rank search results. Sun et al.'s search algorithm achieves better-than-linear search efficiency but results in precision loss.

III. EXISTING METHODOLOGIES

A. PlainText Data Retrival

The existing methods which are based on keyword based information retrieval, are widely used on the plaintext data that cannot be directly applied to the encrypted format of data. Fetching audio video encrypted data from the cloud and decrypt locally is yet not implimented. Multi keyword search schemes retrieves searching based results based on the presence of keywords, which cannot provide acceptable result. However, data should be encrypted before outsourcing for privacy preservig, which obsoletes the data utilization like keyword-based document retrieval.

The existing system provided only text data files cryptrography with multi keyword search. These multi keyword searching schemes fetch searching results based on the presence of keywords, which cannot provide acceptable result.

IV. PROPOSED SYSTEM

In this, we are using AES encryption process using encrypted keys are very complex combinations. The purpose of applying AES technique is to completely secure the records and abstain from the utilization of single secret code. The randomly created secret keys are exceptionally unpredictable combination along these lines client won't retain it exactly. In this system user first register in to the system then if he/ she is an authorized user and having an encrypted key then only he can upload a file to a system these files are stored in an encrypted format, our system proposed an advance types of file including Text, word, pdf, audio and video files. User can able to download the files if is having decrypted key, for this user have to send the request for the access key to the administrator who upload that file , we are providing the actual data to the authorised users only.This provides security to the person to protect their information from others. If user needs to download any file they need to request that particular file, then this request will pass to auditor then automatically user get a secret key to their mail and during download verification will be required. The secret code sent to their mail will be given in the verification part, then the file will downloaded. Advantages: The passkeys are very complex thus user will not be able to fully memorize them.

A. Architecture

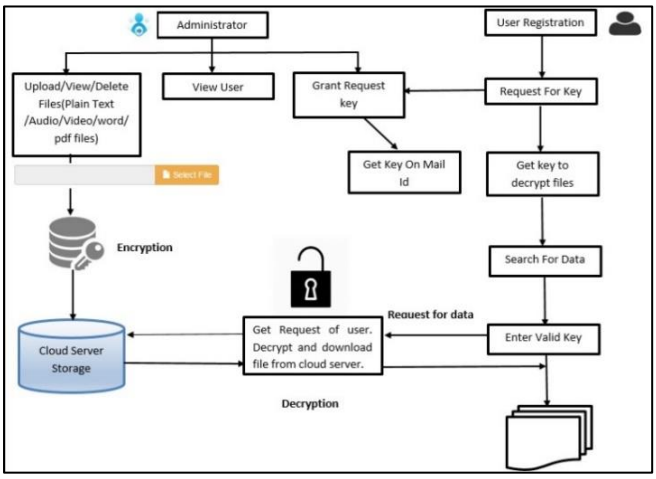

Fig. 1: Architecture of Enhance Privacy Preserving Data Encryption-Description

In first step user will register in to the system, When he got successful login with authenticated credentials user can send his data to the system to stored in in the cloud server , our proposed system will encrypt the data with encrypt key saved it to the cloud server.

User can request for decrypt key to the system for the decryption of the data .if user is having exact matching key then can decrypt the data.

B. How Safe is AES 256 Bit Encryption?

AES-256 is used among other places in SSL/TLS across an Internet. It's is among the top encryptions schemes. In theory it's not crack able since the combinations of keys are massive. Although NSA has categorized this in Suite B, they have also recommended to use higher than 128-bit key encryption scheme. AES is an iterative rather than Feistel cipher scheme for encryption and decryption. It is based on the substitution of the permutation network. It also comprises of a series of linked operations, some of them involve replacing of inputs by some scpecific number of outputs (substitutions) and others have involve shuffling of the bits around (permutations). AES performs its operations based on the bytes rather than the 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 a matrix − Unlike DES, number of rounds in AES is variable in size and depends on the length of key which are using. AES algorithm 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.

1) Algorithm

1) Step 1: Authentication Process
a) Authentication of user and grant access rights to the user for new user.
b) User send request to administrator to provide a key for data accessing purpose,
c) Administrator will send the key to the user.
2) Step 2: Uploading file
a) Data owner can upload number of files (f1, f2….fn) to the cloud server.
b) Internally system will encrypt the files and send to the cloud server.
c) f and f' will be encrypted.
d) Upload encrypted f and f' to cloud server.
3) Step 3: File Retrieval
a) User can search the data uploaded on server.
b) To retrive the specific file user have to enter a valid key provided to them.
c) f' will be decrypted to f.
d) Download encrypted f'to f to the local machine.

An AES algorithm to provide efficient multi-keyword ranked search.

The secure Rijndael algorithm is utilized to encrypt the index and query vectors.

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.

The features of AES are as follows

– Symmetric key symmetric block cipher

128-bit data,

– 128/192/256-bit keys
– Stronger and faster than Triple-DES
– Provide full specification and design details

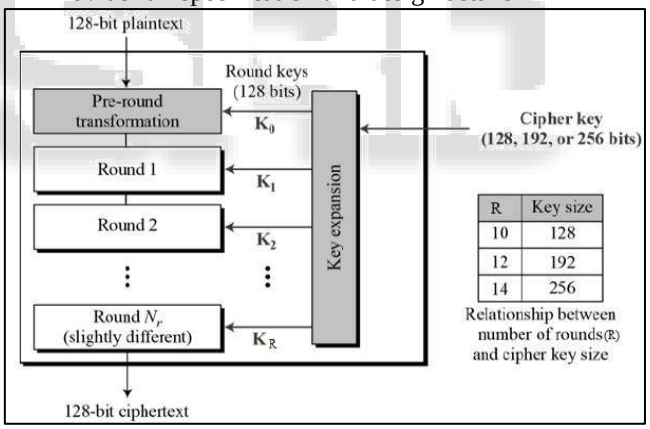

Fig. 2:

V. PROPOSED METHODOLOGIES

A. Techniques/Tool Required

1) Hardware Requirements

– System : Pentium IV 3.5 GHz.
– Hard Disk : 40 GB.
– Monitor : 14' Colour Monitor.
– Ram : 2 GB.

2) Software Requirements

– Operating system : Windows 7 Ultimate.
– Coding Language : ASP.Net with C#
– Front-End : Visual Studio 2013 and advance vesrions of visual studio.
– Remote Server : Cloud Server.
– Database : Sql Server 2012

– Other Advance Technologies : Ajax , Javascript ,CSS

3) Module

1) Administrator
2) Data Users
3) Cloud Server Module
4) Cipher text Module

4) Administrator

In administrator module, admin have right to provide allow the user to share data on cloud server though this system.

Admin will grant a key to user to share the data. This key is generated using multi keyword ranked search scheme for this we construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. Second activity of the data is to enctyption and decryption of data, which we are go in to discuss in cipher text module.

5) Data Users

Data user is the user of the system and are having file/data that, he wants to outsource to the cloud server.

In first step user need to register in to the systme after successful registration ,user request will go to administrator to provide the access to the user,once admin will grant(send authentication mail to user email id) an access to user can able to upload/ fetch encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key.

6) Cloud Server

A cloud server is a server that is built, hosted and delivered to store and share data over the Internet. Cloud server is a remote server, exhibits the same functionality as local but it can be access over the remotely over internet.

In this module we are using cloud server to store and access the data over internet, but before sharing data we are doing encryption of data using AES Based Rijndael algorithm.

B. Cipher-Text Module

In this model, we have perform the encryption decryption of the files , in our system cloud server only accept the encrypted data with the authorized user can decrypt the file Encryption decryption performed using AES Rijndael algorithm.

VI. Outcome possible results

"Cloud computing uses the internet to deliver online services instead of keeping hardware and software at your office."
Following are some reasons found why companies perefer to use cloud services.

– Maintaining Focus on the Business
– Business Agility
– Reduced Capital Expenditures
– Scale
– Access from Anywhere
– Staffing Efficiency

VII. Conclusion & future scope

In conclusion, I am pretty confident that I have learned and introduced the main concepts of traditional cryptography through these four parts. I also believe that I have a general understanding of Triple Data Encryption Standards and its security issues comparing with Advanced Encryption Standards.

References

[1] K. Ren, C.Wang, Q.Wang et al.,"Security challenges for the public cloud," IEEE Internet Computing, Vol. 16, No. 1, pp. 69–73, 2012.
[2] S. Kamara, K. Lauter, "Cryptographic cloud storage," In Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.
[3] C. Gentry,"A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.
[4] D. X. Song, D. Wagner, A. Perrig,"Practical techniques for searches on encrypted data," In Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[5] Y.-C. Chang, M. Mitzenmacher,"Privacy preserving keyword searches on remote encrypted data," In Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.
[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," In Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006
[7] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.
[8] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.
[9] Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.
[10] For AES Cryprography from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

