A Secure MSSS Scheme and AES Encryption over Cloud Data

Sreelakshmy D Unni
PG Scholar
Department of Computer Science and Engineering
Mangalam College of Engineering
Kottayam, Kerala
India

Neethu Maria John
Associate Professor
Department of Computer Science and Engineering
Mangalam College of Engineering
Kottayam, Kerala
India

Abstract: In this era Cloud plays a vital role in storage of all type of data. Thus the availability of data also increased. The data can be subscribed and maintained comfortably. It also solves the problem of excess computation cycles, software updates and handling high loads of data. AES is the encryption techniques used by worldwide. Most Significant Single Keyword Search (MSSS) is efficient search that uses Most Significant Digit (MSD) Radix Sort. The main challenge facing are security of data in Cloud. In this we propose Secure MSSS Scheme and AES Encryption over Cloud Data. AES is a symmetric encryption block cipher which allows different key length. Encryption is performed by interchanging characters of key and data. In this we are using a private cloud. The data uploaded to cloud is stored as encrypted file. Encryption performed using AES encryption algorithm. The data stored in the cloud is accessed by the allowed users of private cloud and searching of data done using MSSS. The MSSS scheme is faster soring array strings. Encryption solves the problem of security to an extent. AES will have 10, 12, 14 rounds of encryption.

Keywords: Cloud computing, AES Encryption, MSSS, Radix sort, Security, Symmetric.

1. INTRODUCTION

To get a pool of computing data owned and maintained by a third person via internet is termed as Cloud computing. The cloud includes network, storage, hardware and interfaces provide user to access computing data, services on demand those are independent of the location. The storage of user data which is already stored in some other locations. Cloud storage of data is like renting the asset according to your requirements. So that it avoid buying the whole infrastructure to perform a particular process. It mainly uses remote services through networks using various type of resources. By using cloud the user is capable of using maximum computing of data with the minimum hardware requirements. Location independency, scalability, device independency are the main advantages of using cloud. Private clouds are more secure than public clouds, it is a challenge to store data without keeping private information in cloud. So that we are encryption the data in cloud.

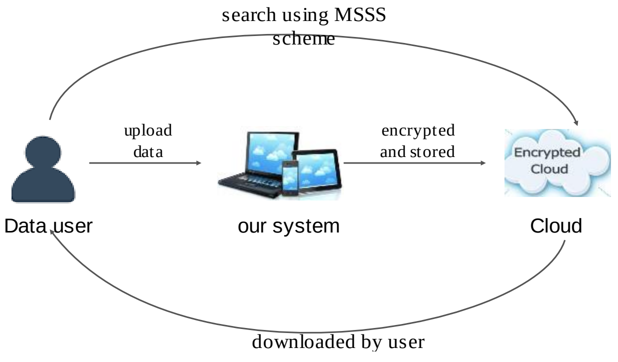

Fig 1: Overview of Proposed System

The encryption algorithm we are using here is AES Encryption algorithm. All of the organizations have their own private data's to keep secured, then we use encryption. AES is efficient encryption algorithm and is unbreakable when compared to other algorithms. AES is symmetric key encryption with separate key is used to for both encryption and decryption. The plain text chosen will be of length 64bytes to 52 bytes and 6 rounds with a complexity 2 126.8 encryptions. Key size of AES can be varied such as 128, 192, and 256. In this public key is used to perform encryption and private key used to perform the decryption.

2. RELATED WORKS

The encrypted and decryption are performed using the same secret key and data is stored in the disk. The algorithm used in this system is Advance Encryption Standard (AES). AES uses key size 128,192 and 256. The number of rounds 10, 12, and 14, respectively. The encryption is done by interchanging some of the characters with key and data in it. The main feature of the system is disabling the delete option in the right click menu for the encrypted files. To provide security to all these confidential data on the desktop by converting the plain text to cipher text when the file is encrypted. AES is unbreakable when compared to other algorithm. The confidential data on a desktop are encrypted using AES with a secret key to secure the files. Once the file is encrypted using secret key then the user has to enter the same secret key for the process of decryption. If the secret key entered is matching with the encryptions secret key, then file will be decrypted successfully else, file cannot be decrypted message is displayed [1].

The cloud deployment models, service delivery models of cloud computing, characteristic of cloud, cloud computing adopting risks, technology, cloud computing security problem and data encryption using RSA, DES and AES[2]**.** Now the 4G technologies and the development of 5G technologies profoundly changed people's life with wireless devices. Huge number of mobile applications produce sensitive data in many fields and most data stored in cloud. The complexity to search data over encoded information for wireless devices without strong computational capability. In this AES, DES, RSA are described to provide security. Cloud computing is the technology most used. It is a good solution for all of them because of personnel storage has not be used or this is less expensive. Cloud computing vulnerabilities are security issues and loss of data [7]. The classical solutions where threats come from two known sources inside or outside the network [2]. In this the threats originate from different sources because the data stored in cloud are from different sources. The different models of cloud and risk factors when adopting cloud computing, technology, security issues in cloud and data encryption using RSA, DES and AES [2].

The secure ranked multi-keyword search is multi-owner model. The cloud servers have to perform secure search without knowing the actual data of both keywords [3]. Efficiency of our proposed schemes experiments on real-world datasets are running. In this cloud servers are systematically construct a novel secure search protocol which helps to secure search without knowing the actual value of both keywords and trapdoors. The different data owners use different keys to encrypt their files and keywords [3]. A query is used to generate keys to authorized keys user can issue without knowing secret keys of these different data owners. Different type of works enables authorized data users to be secure, confidentiality, efficient search over multiple data set**.** To get search results and rank the system privacy keywords and files, we propose a novel Additive Order and Privacy Preserving Function family [3].Thus this approach is efficient in performance wise compared to very large data set and keyword set.

3.PROPOSED METHODOLOGY

Now a days many enterprise store and outsource data through cloud. By this the sensitive data's stored in cloud are much secure. The data have to keep secure is a very big problem. So that data's are encrypted and stored in cloud, data's such as financial, personal and government data's. From the encrypted stored data the user have to find their on data using MSSS. The user will request for the data and get the matching data without much knowledge about the encrypted cloud [4].

All files are encrypted, storage and searching is not a simple job in very large systems [9]. The cost of searching have been reduced without affecting the search request of the data stored in cloud. With the high security the document have to select accurate keyword search over encrypted cloud [10]. Unauthorized entitles or other service providers can't able to access data from this cloud. The MSSS will reduce the searching overhead and time over the AES encrypted cloud data. The index generation time is reduced to O(Nt*3) retrieval of data from encrypted cloud with top k single keyword [4] .

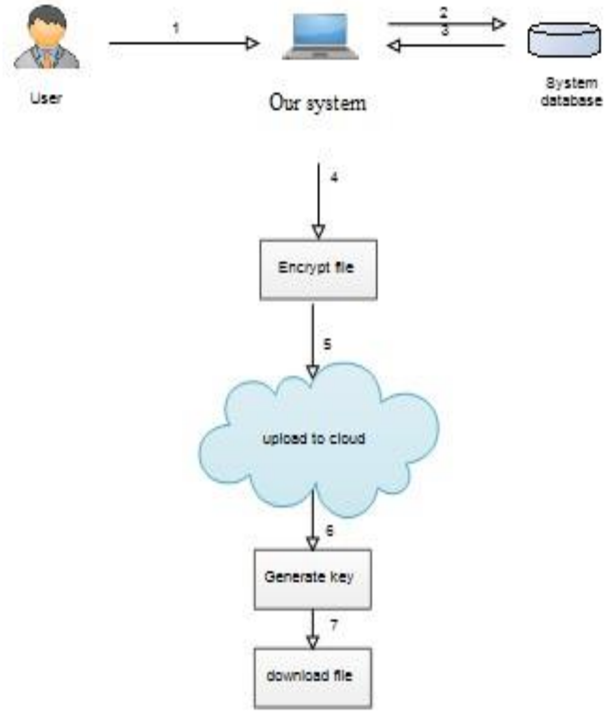

Fig 2: System Architecture

In the system architecture the user enters data into the system. Only the authorized user in the system can access this system. This system stores all passwords in the database in encrypted format. The data stored in the database is uploaded to cloud after performing the encryption using AES. When the user searches an encrypted file in cloud. The data file downloaded from cloud with a secret key send by system administrator to users email. This improves the security of the system and unauthorized access to the data files. The searching scheme here used is MSSS. The Steps are

1. An authorized user uploads data file into the system.
2. The system stores the data file in Data base to create a unique key for the data file.
3. The System administrator retrieve data file from base data base.
4. Then the System administrator perform the encryption of data file by AES encryption algorithm.
5. The encrypted file is uploaded to the cloud.
6. When a user searches the file in the cloud using MSSS search scheme, and request is send to administrator to download the data file.
7. The system administrator sends a secret key to the users mail and using that mail the user can download the data file

1.MSSS

Algorithm 1: Most Significant Multi-keyword Search (MSSS)

```
Initialization Phase
input     :          A set of n Data Files F = (f1, f2, . . . , fn)
output    : Index file generated from extracted keyword I
Function: Build Index(K, F )
for fi ← 1 to n do
each file  fi ∈F ;
Scan F and Extract the distinct word in fi, denoted as a W =
(w1, w2, w3, . . . wn, ) ; Normalized and filter the stop words
from W ;
for j ← 1 to m do
each file  wi ∈W ;
1)        Calculate the Score S for each keyword wi
according to equation 1;
2)        MSD() to sort the Index I;
3)        Compute α(wi) for each keyword wi according to
equation 2;
4)        Store the hid(fi)||α(wi)||Si as an element in the
posting list of I' ;
5)        Encrypt the Index file  I';
6)        Replace I' with I''
      return I'';
```

1.1Radix Sort

This algorithm arranges string in ascending or descending order. The algorithm process the string of grouping keys which have the same significant position and value. The two type of radix sort are LSD and MSD. Here we are using MSD (Most Significant Digit).

1.2 MSD

MSD uses lexicographic ordering which is suitable for sorting strings such as word or fixed length integer.MSD radix sort starts the string processing from right side that is opposite to LSD. The MSD stops processing by rearranging reaches the prefix of the key MSD sort uses multiple level of bucket.

2. AES

AES is a symmetric key encryption technique which consist of 4 encryption stages. The stages are Substitution Bytes, Shift Rows, Mix Columns, and Add Round Key. AES require block size to be 128 bits, the state array of different size block has only 4 rows in other ciphers. The number of columns depend on size of the block. The data on cloud is encrypt using secret key with AES as encryption algorithm. The user have to give 16 bytes of secret key twice to uniform the secret key [1].

Table: AES Versions

Version	Key Length	Block Size	No: of Rounds
AES -128	4	4	10
AES -192	6	4	12
AES -256	8	4	14

Once a file is encrypted using a secret key, the decryption have to be performed using the same secret key which have been used for encryption. If the secret key changes or misplaced then the decryption cannot be performed. The deletion of encrypted file can be also performed in this cloud. In this we have to select the file for encryption. The file selected have to upload to cloud. Then the file have to be perform encryption and uploaded. Then the file is stored in the cloud. When the user needs the file we search the file using MSSS and download the file with the help of a key that is given to authorized user. Only by inserting the key we can download the file from the cloud.

The 4 Stages of AES [5]

1. Sub Bytes transformation is a nonlinear byte substitution for each block of data.
2. Shift Rows transformation cyclically shifts the bytes within the block.
3. Mix Columns transformation groups 4bytes together forming 4-term polynomials with a fixed polynomial mode.
4. Round Key transformation adds the round key with the block of data

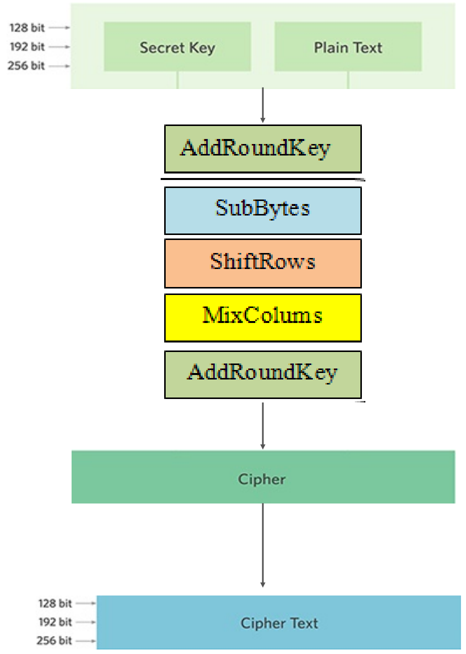

Fig 3: AES encryption steps

4. EXPERMENT AND RESULTS

The three encryption algorithms are symmetric block cipher. The AES uses 128,192,256 bits key length which can use variable length keys [8]. The DES uses 56 bit key length and triple DES uses 168 and 112 key length used by Triple DES [6].Block size of data also used by AES is 128, 192, 256 bits. DES uses 64 bit data block size. Triple DES also use 64 bit of data.There is graph Fig 4 which compares the security or usage of these three algorithms. From this we can conclude that AES is better than DES and Triple DES. The MSSS scheme which use index storage space of cloud server which reduced and it creates an index storage of files [4]. So the search time will be reduced over the encrypted cloud. The searching time of MSSS is efficient compared to Greedy Depth First Search algorithm shown in Fig5. Storage overheadand computation time is reduced. Real data which reduces index store and keyword search time over the encrypted cloud.

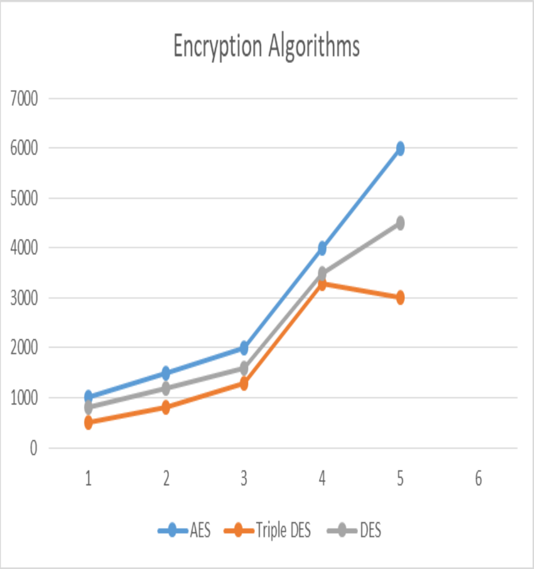

Fig 4: Comparison of encryption algorithm

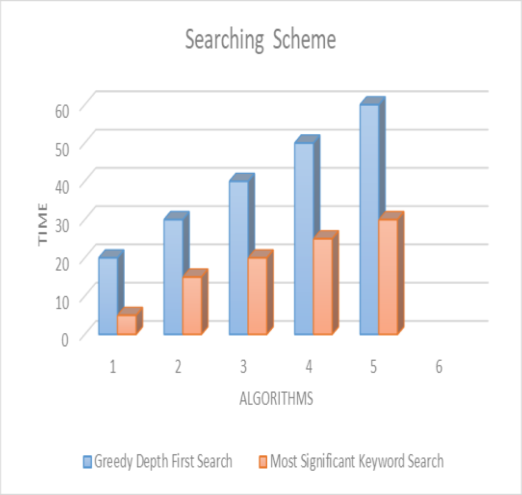

Fig 5: Comparision of Searching schemes

5. CONCLUSION

Now a days the data security issues are increasing day by day in cloud. Searching data in the encrypted cloud is a complex problem. In this for encryption we are using AES encrypted cloud and MSSS searching scheme for searching data. The combination of AES and MSSS will have high efficiency with the data security, storage and efficiency in searching the data's in cloud. In this Radix Sort, MSD is used. for searching of stored data over encrypted cloud. The performance of the system is improved as the searching time required is less compared to other searching algorithms. The AES encryption is much secure than the other encryption algorithm. So that the system will be highly efficient and data is secure in the cloud

REFERENCES

[1] Securing Files Using AES Algorithm. Aditya Rayarapu, Abhinav Saxena, N.Vamshi Krishna, Diksha Mundhra.

[2] A Survey on Security Using Encryption Techniques in Cloud Gaurav Jain, Vikas sejwar P. G. Scholar.

[3] A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEETavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] MSSS: Most Significant Single-keyword Search over Encrypted Cloud Data Raghavendra S, Geeta C M, Shaila K, Rajkumar Buyya, Venugopal K R, S S Iyengar, L M Patnaik.

[5]https://www.vocal.com/cryptography/advanced encryption-standard-aes.

[6] A Study of Encryption Algorithms AES, DES and RSA for Security by Dr. Prerna Mahajan & Abhishek Sachdeva IITM, India.

[7] Secure User Data in Cloud Computing Using Encryption Algorithms Rachna Arora, Anshu Parashar Research Scholar, HCTM, Kaithal, Haryana (Associate Professor, HCTM, Kaithal, Haryana.

[8] Advanced Encryption Standard (AES) Standard (AES) Raj Jain Washington University in Saint Louis Saint Louis, MO 63130 Jain@cse.wustl.edu.

[9] Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data Ning Cao†, Cong Wang‡, Ming Li †, Kui Ren ‡, and Wenjing Lou† †Department of ECE, Worcester Polytechnic Institute.

[10] A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data. Cengiz Orencik∗, Murat Kantarcioglu† and Erkay Savas∗ ∗Faculty of Engineering and Natural Sciences Sabanci University, Istanbul, 34956, Turkey† Department of Computer Science The University of Texas at Dallas Richardson, TX 75080, USA.