I J C T A, 9(2) 2016, pp. 445-453
© International Science Press

Efficient Data Retrieval in Cloud Using Combined Searchable Homomorphic Encryption Mechanism

Madhumitha T.[1] and R. Anitha[2]

ABSTRACT

Cloud computing is a technology that allows user to access information and the computer resources from anywhere a network connection is available. Data are stored and accessed in from a server with the help of services provided by cloud service providers along with security. Providing security is a major concern as the data is stored and retrieved from the server over an internet. This project aims to propose an Enhanced Combined Searchable Symmetric Homomorphic Encryption (CSSHE) model. The proposed model uses searchable symmetric mechanism using homomorphic encryption for the improved security and also reduces the retrieval latency. In this proposed model, data is encrypted with a PKE and computations for searching and evaluating are carried out on top of encrypted data. This paper aims at solving the problems on security issues with the help of searchable symmetric homomorphic encryption, which improves the data security & integrity, to reduce latency and reduces unauthorized access onto the cloud server.

Keywords: Cloud Computing, Searchable Symmetric Encryption, Homomorphic Encryption, Bloom filter.

INTRODUCTION

Cloud Computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power and specialized corporate and user applications. *Cloud can be deployed as Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud. The basic services offered by the cloud are categorized as Software as a Service, Platform as a Service and Infrastructure as a Service. Figure 1 shows the existing approach of various challenges in cloud computing environment. As per IDC standard, it is said that the adaption of cloud will be reduced only because of security issue. In order to recover these issues in cloud environment researchers have concentrated on security issues [10]. This paper proposes a novel concept called Combined Searchable Symmetric Homomorphic Encryption.*

Searchable Symmetric Encryption (SSE) is a method that allows user to search over their encrypted data on a third party storage provider in a private manner. It is based on symmetric cryptographic method like block cipher, pseudo-random function and hash functions. A major drawback is an inefficient index update as well as non-support of conjunctive (or) disjunctive keyword searches. Two different settings are used in SSE algorithm such as Non-Adaptive security and Adaptive security. Homomorphic Encryption (HE) is a form of encryption which allows specific types of computations to be carried out on encrypted data. This paper proposes a novel methodology which combines both searchable symmetric as well as homomorphic encryption. The rest of the paper is organized as follows: Section 2 summarizes the related

P. G. Student[1], Associate Professor[2], Dept. of Computer Science and Engg. Sri Venkateswara College of Engineering, Sriperumbudur, India, *E-mail: madhumitha.thachu@gmail.com, anitabalajim@yahoo.com*

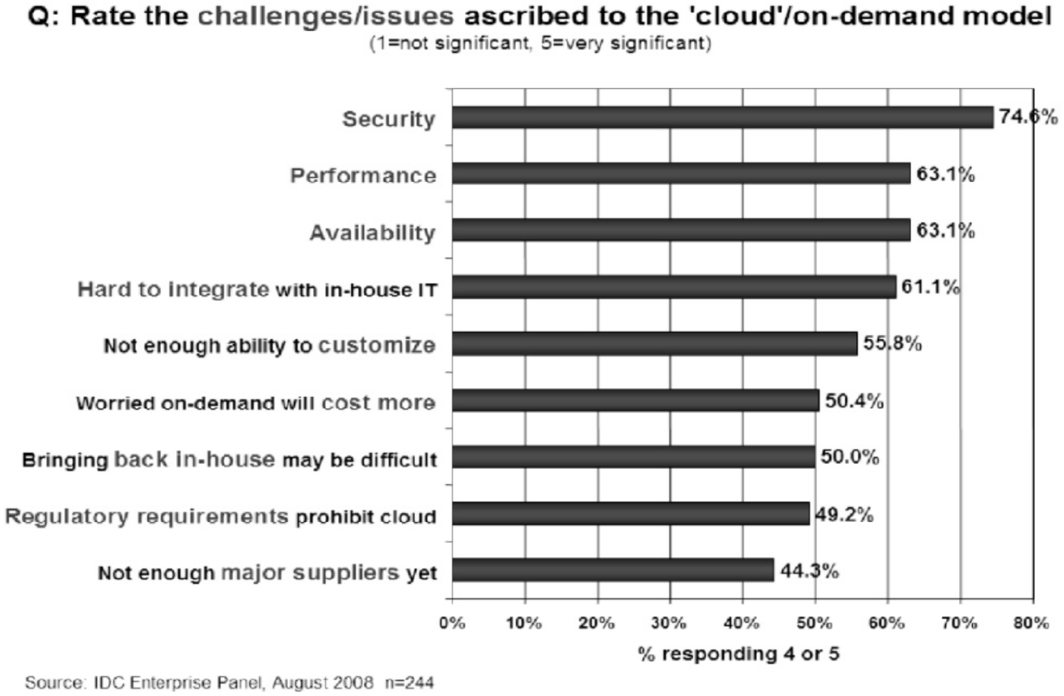

Figure 1: Issues ascribed to the cloud

work and the problem statement. Section 3 describes the system architecture model and discusses the detailed design of the system model. Section 4 describes the key generation mechanism and its distribution in a federated environment. Section 5 describes the proposed HMCBC structure design and issues of the proposed model. The performance evaluation based on the prototype implementation is given in Section 6 and Section 7 concludes the paper.

RELATED WORK

The related work discusses about the previous work and also discussed about how the data is retrieved in a secured manner.

Chirag modi *et al.*, [3] proposed security issues with various threats and various cloud services and the solution identified for security and privacy issues in cloud computing environment. Jung hee et al. [1] has proposed the public key encryption using somewhat homomorphic mechanism. Authors Jiadi Yu *et al.* [2] & Nagesh *et al.* [7] proposes Keyword based retrieval over encrypted data which supports multi-keyword search using two round searchable encryption. In this paper it is only focused on data privacy issues. Coa Ning *et al.*, [4] shows that the retrieval of data is done with the help of multi-keyword search and also implemented the keyword search method. The search method is performed using indexing form to get the relevant data from the server. Build index is a method for efficient data processing in cloud. R. Curtmola *et al.* [5] introduces the reviews on data security in cloud computing and it is based on the type of approach and also the type of validation. Some kind of encryption techniques are used for securing the data in cloud environment. Jiss *et al.*, [9] proposes a technique called homomorphic encryption i.e. perform computation on top of encrypted data. By performing computations it enables user to retrieve the data over encrypted data using ranking algorithm. Further needs to improve the security and efficiency of data using homomorphic encryption. Penmetsa *et al.*, [12] proposes a block chaining mode that can be used for confidential of data and authentication. Key is generated using Hilbert matrix form. Sharmila *et al.*, [6] proposes a novel scheme called homomorphic encryption based on different computations to be applied on encrypted data. Ranking algorithm is used for computations on top of the encrypted data. In this paper data can be searched and retrieved in an efficient manner. The major issue in this technique is key maintenance. User wants to improve the security based on Homomorphic encryption. Jung *et al.*, [11] implements a hybrid scheme of public-key encryption and somewhat homomorphic encryption. It improves the efficiency of Somewhat Homomorphic Encryption (SHE) algorithm. In this algorithm IND-CPA PKE without complicated message padding and SHE with large integer message space that can be used for obtaining efficient homomorphic decryption. Searchable symmetric technique is used for searching over the encrypted data. Low polynomial degree is used for somewhat homomorphic encryption. Public key Encryption and Somewhat Homomorphic Encryption is used for reducing the bandwidth and storage requirements of cloud server. Anitha *et al.* [8] has proposed about key distribution in improving the cloud security.

SYSTEM ARCHITECTURE

The system framework for the proposed model is as shown in figure 2. The proposed model enables the retrieval of data with the help of combined searchable symmetric homomorphic encryption mechanism (CSSHE). The combined SSE scheme allows users to search the encrypted metadata and to retrieve the cipher text in a secure way. In the proposed model the computations are carried out on top of the encrypted data using homomorphic encryption technique. The search is carried out based on the availability of the keyword. The proposed CSSHE scheme keeps the privacy of the sensitive information and allows the searching mechanism using keyword which is in an encrypted form. The proposed idea is a multi-keyword based searching schemes, which enables secure bloom filter based data structure for indexing. It enables us to get the retrieval result as the most relevant files that match users' requirement. In CSSHE, the concept of searchable homomorphic encryption techniques is introduced. Since the search operation is performed over encrypted data, information leakage can be eliminated and data can be searched and retrieved efficiently.

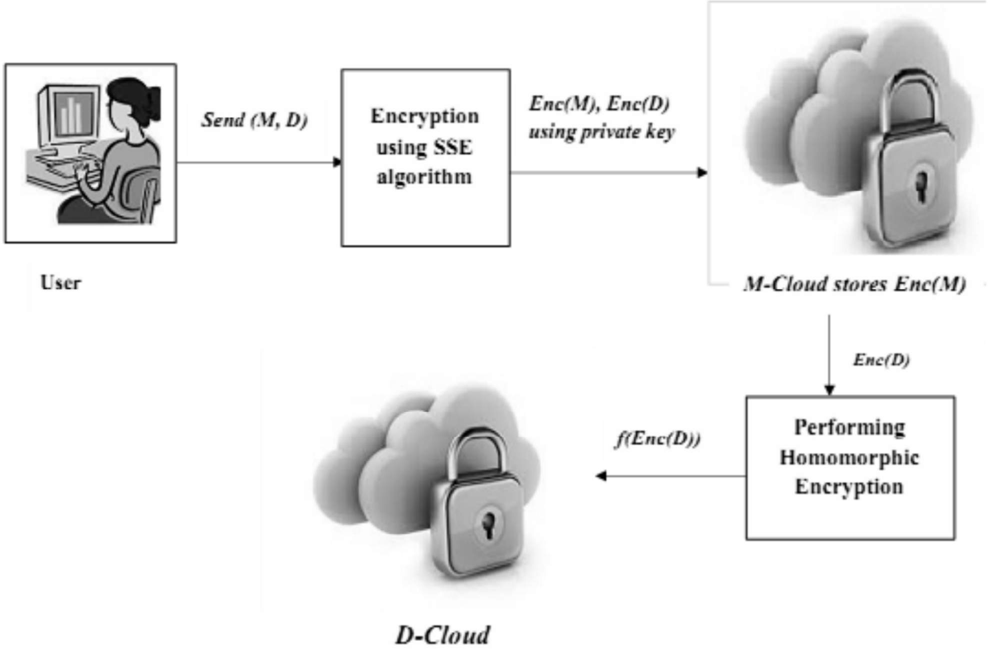
Send (M, D)
Encryption using SSE algorithm
Enc(M), Enc(D) using private key
User
M-Cloud stores Enc(M)
Enc(D)
Performing Homomorphic Encryption
f(Enc(D))
D-Cloud

Figure 2: Proposed System Architecture

In the proposed model when a user uploads a file the respective metadata attributes are extracted and is partially encrypted and stored inside the metadata cloud called *M-Cloud*. The data is encrypted using homomorphic encryption and is stored at the *D-Cloud.* The architecture also proposes a novel key generation methodology for both the SSE and the homomorphic encryption both a the M-Cloud and D-Cloud level. Functions of homomorphic encryption HE is a set of four function such as Generating a key, Encryption, Evaluation and Decryption.

MODULES

The proposed model has four modules namely:

A. Key Generation

B. Encryption

C. Search

D. Data Placement

A. Key Generation

Key generation is the process of generating keys for encryption and decryption of plain data. The proposed security model depends entirely on a complicated parameter called Cipher key. Cipher keys are generated using metadata attributes. The security model proposes key generation mechanisms. Key is generated at the user level and is represented as U_1 using Hilbert matrix based on cipher block chaining method. It is easy to implement and tackle the complexity of generating a key and it also produces a strong Avalanche effect making many values in cipher to undergo changes with one value change in the secret key. Key is generated in a matrix form based on number of metadata attributes and secret key. The block chaining modes of operation have been used to tackle the two issues for strengthening the key: Confusion and Diffusion. In proposed model, the Hilbert matrix is generated and is used for the key generation which is a special case of the Cauchy matrix. It gives as a symmetric and positive definite values. The determinant of the Hilbert Matrix is the reciprocal of an integer. It is invertible. Every sub matrix is also positive. The determinant can be expressed as follows: $H_{i,j} = 1 / (i + j – 1)$. Cipher Block Chaining is a block cipher mode that provides confidentiality. Each block of plaintext is XOR-ed with the previous cipher text block before being encrypted. One in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block.

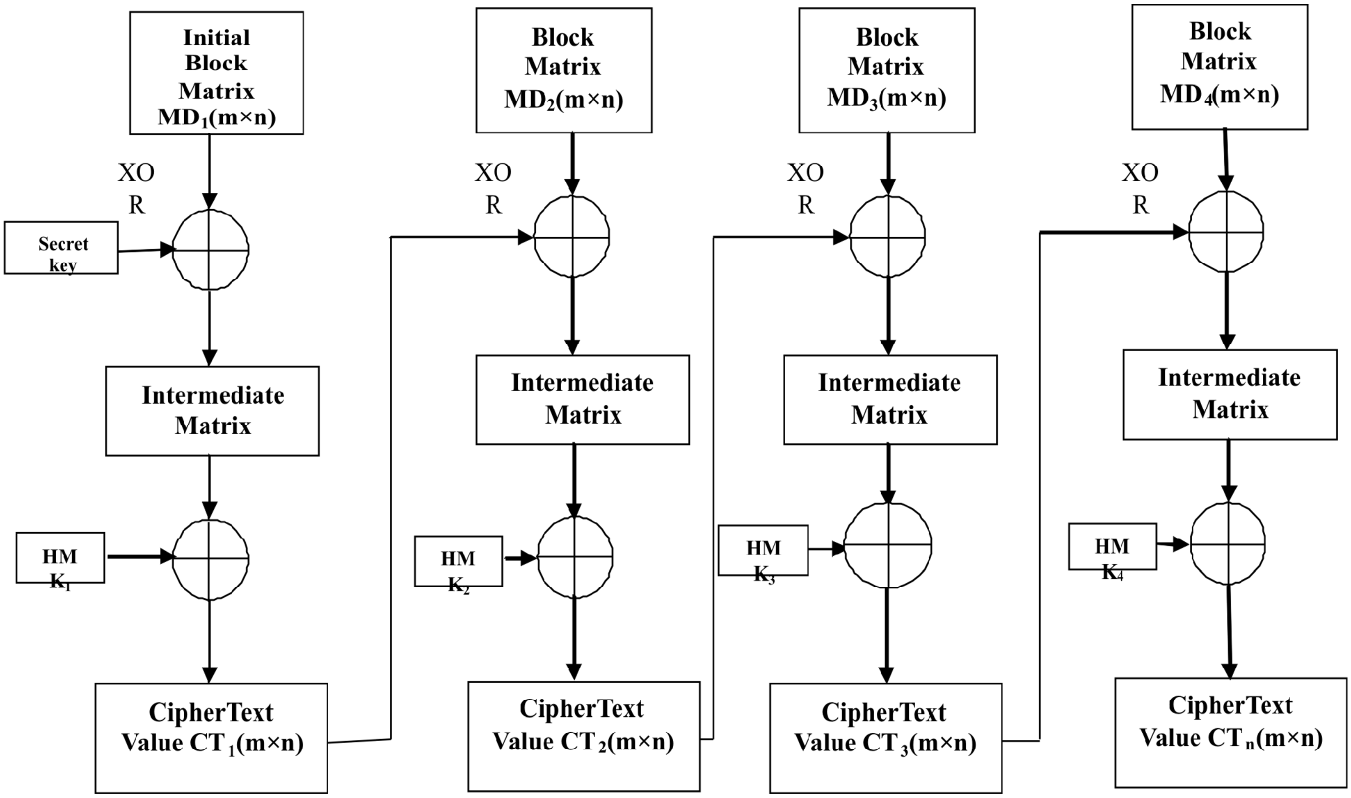

Figure 3: Cipher Key Generation using HMCBC Structure

Figure 3 shows the Cipher key generation using HMCBC structure. The key is generated using HMCBC algorithm with the help of cipher function Cipher function is defined as follows:

$$C(MD_n, S_K, K) = CT_n$$

where

MD_n- Metadata Attributes

S_k – Secret Key

K – Key

CT_n – Cipher text block

C is termed as Cipher Block Chaining.

In the diagram as shown in figure 3, the given plaintext is converted into matrix form using Hilbert Matrix based Cipher Block Chaining mechanism. The initial block matrix is XOR- ed with secret key and that can be produced the output called intermediate matrix, matrix will be XOR-ed with a key using HMAC algorithm. The output of the matrix is Cipher Text value. Each block of the plaintext is XORed with the previous cipher text block before being encrypted. Here the metadata is a structural form of data(data about data). It contains number of attributes. It can easily analysed that if two cipher text block are same their corresponding plaintext block must be different because each block of the plaintext is tied up with the cipher text block of the previous block. It helps us to deal with redundancy problem in block cipher successfully. The Hilbert matrix is in a form of N×N matrix. Example for Hilbert matrix is as follows:

$$\begin{bmatrix} 1 & \frac{1}{2} & \\ & & \cdots \\ \frac{1}{2} & \frac{1}{3} & \end{bmatrix}$$

Algorithm 1: Procedure for Key Generation

```
Begin
Step 1. Read Metadata Attributes
Step 2. Apply SHA-3
Step 3. Generate Matrix $M_{mxn}$, split the matrix, and generate cipher tree
Step 4. Root value of cipher tree splitted into child nodes
  For i = 1 to n Repeat till n / 2 = 1
    Begin
      Step 4.1 Leaf node values =$MD_{1mxn}$
      Step 4.2 Add $MD_{1mxn}$, $S_{k(mxn)}$ $[MD_{1mxn} + S_{k(mxn)}] = D_{1mxn}$
      Step 4.3 Apply HMAC $(D_{1mxn}, HM_{K1}) = CT_{1mxn}$
      Step 4.4 Apply $CT_{1mxn}$ as input to the next block as secret key.
Step 5. Repeat the step till leaf node becomes null
Step 6. Write(C) Cipher key $C = CT_{N(mxn)}$
End
```

The cipher key $U_1 = CT_{N(mxn)}$

(B) Encryption

Encryption is the most effective way to achieve data security in cloud as the data is stored away from the user. The files can be read only by user who will have the right key to access it. In this proposed model, the two different approaches used for encryption are ESSE and HE. Metadata is encrypted using Enhanced Searchable Symmetric Encryption (ESSE). Data server is encrypted using Homomorphic Encryption (HE). The Enhanced Searchable Symmetric Encryption is a method that allows user to search over their encrypted data on a third party service provider in a private manner. Using the key generated by the user the extracted metadata are encrypted. The encrypted metadata is stored into the metadata cloud server. In this proposed model the stored metadata describes and locates the structural form of data and makes it easier to retrieve the data from the data cloud server. Metadata is created by Dublin Core Metadata Initiative (DCMI) standard that can be used for Data access. It supports keyword based information retrieval. The keyword is extracted with the help of TFIDF for identifying a set of words in a document.

$$\text{TFIDF} = W_i * \log(N/N_i)$$

Where,

W_i - Frequency of a term in the given document

N - Total number of documents in the collection

N_i - Number of documents containing that word.

The various technique are used in SSE algorithm such as: Secure Indexes, Keyword or ranked search and searches on encrypted data. In the existing model, SSE consists of five polynomial time algorithms (Gen, Enc, Trapdoor, Search, Dec). User wants to encrypt the metadata. Metadata is encrypted by using this techniques. It consisting of several attributes and it should be encrypted separately. The functionality of encryption technique is a trapdoor function. After encryption, the encrypted data is stored on the metadata server and then the computation is performed on top of the encrypted data using homomorphic encryption. Searchable Symmetric encryption is based on secure indexes. An index is a data structure that stores collection of document that supports efficient keyword search. Trapdoor function is used for the purpose of safety measures. It is an entrance point in an information processing system. The second approach of encryption is to encrypt the data by the Homomorphic Encryption (HE) at the data server level. It is an encryption method which allows computation on top of the encrypted data. These computing encrypted data is send to the cloud data server for retrieving the data in an efficient manner. Retrieval of data should be done only by using Filename or keyword or adding both filename and keyword should be done using Hash functions at which the user can upload the metadata to the metadata server and to download the data from the server. Search. The proposed model depends on ESSE algorithm for searching the encrypted data from the metadata cloud server. The searching technique is a method for getting the accurate result from the cloud server. Enhanced Searchable Symmetric algorithm has a function for performing searching operations using a private key in a cloud server.

(C) Data Placement

After performing the Homomorphic encryption mechanism, the encrypted data is located and sent to the cloud server with the help of Bloom’s data structure using bloom filter technique. Bloom filter is a probabilistic data structure which is suitable for storing the data in a structural form. In this model it provides the exact information to the user and performs the set membership queries in an efficient manner. The placement of data is carried out using the bloom placement technique at the *D- Cloud* location.

EXPERIMENT & RESULTS

The experimental results have been analysed in a cloud setup using eucalyptus for implementing Infrastructure as a service in a private environment. It contains node and cluster controller. It shows how the key is generated for strengthening the data which is stored in a cloud server. The out coming results of the proposed model is used to calculate the following performance metric, avalanche effect. It is defined as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text. Hence based on the avalanche effect the key strength is analysed which improves the cloud security. Thus the strength of the Cipher Text and the increased key size improves the security. The avalanche effect is calculated using the below equation.

$$Avalanche\,effect = \frac{Number\ of\ values\ changed\ in\ the\ cipher\ key\ C_k}{Total\ number\ of\ values\ in\ the\ cipher\ key\ C_k}$$

The figure 4 gives the comparative analysis of avalanche effect of the proposed model with the existing models.

From the figure 4, it is observed that the avalanche effect of the proposed model is greater when compared to the existing key generation algorithms. The number of rounds taken for executing the proposed algorithm is less when compared to existing encryption algorithms. The Table 1 below illustrates the comparison of proposed HMCBC algorithm with respect to existing algorithm under various features.

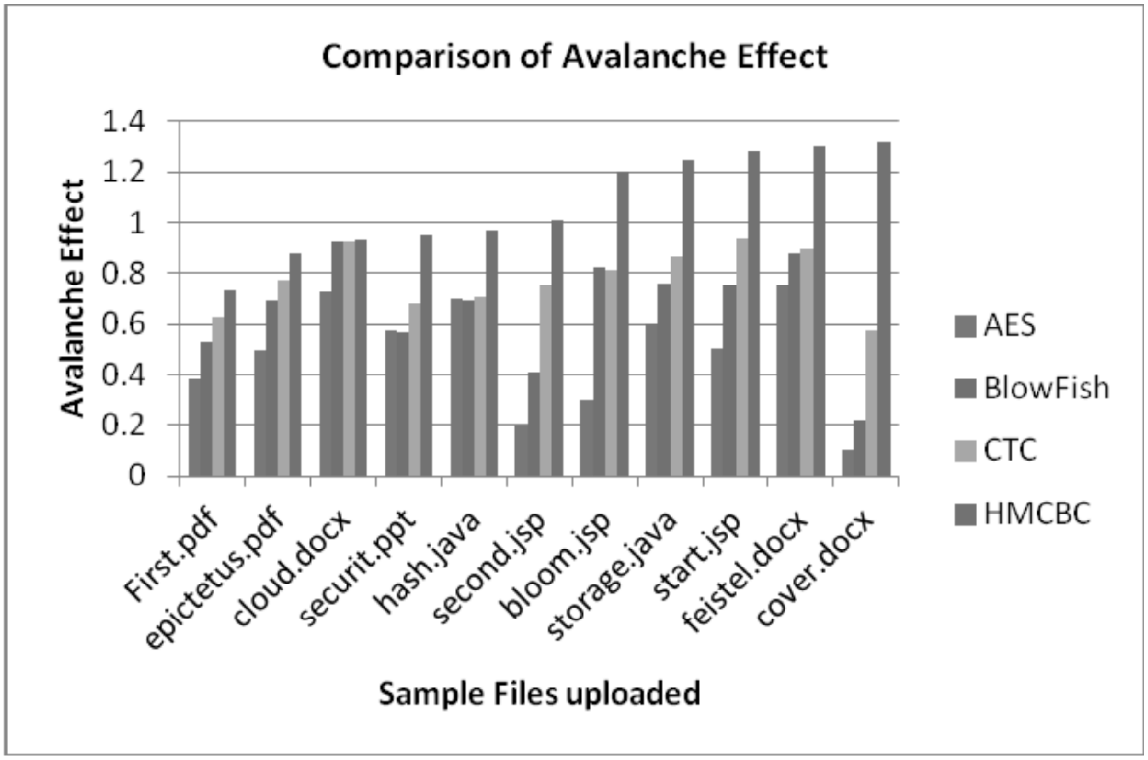

Figure 4: Comparative analysis of Avalanche Effect

CONCLUSION

Cloud computing is a new emerging technology that faces many security challenges. In this paper presents the security frameworks that can be used to provide security to the data stored in a cloud environment and also to retrieve the data in a secured manner. Further, it has proposed a security framework which decouples the third party auditor from the cloud security scenario and provides security by its own. The combined homomorphic based searchable security mechanism is a promising technique, which can be applied in any remote storage systems.

Table 1
Comparison of Proposed HMCBC Algorithm

Features Analysed	*Algorithms*					
	DES	*AES*	*Two Fish*	*Blow Fish*	*MMFN*	*HMCBC*
Created By	IBM in 1975	Joan Daemen & Vincent Rijmen in 1998	Bruce Schneier in 1993	Bruce Schneier in 1993	2013	2015
Algorithm Structure	Feistel Network	Substitution-Permutation Network	Feistel Network	Feistel Network	Modified Feistel Network	Cipher Block chaining
Rounds	16	10, 12 or 14	16	16	4	4
Key Size	56 bits	128 bits, 192 bits, 256 bits	128 bits, 192 bits or 256 bits	32-448 bit in steps of 8 bits. 128 bits by default	256*6 bits	256*32 bits
Type	Block cipher	Block cipher	Block cipher	Block cipher	Block cipher	Block cipher
Block Size	64 bits	128 bits	128 bits	64 bits	64 bits	64bits
Key Strength	Low	Low	High	Very High	Very High	Very High
Existing Cracks	Brute force attack, differential crypanalysis, linear cryptanalysis, Davies' attack	Side channel attacks	Truncated differential cryptanalysis	Second-order differential attack	NO	Yet to Apply
Avalanche Effect	Less	Less	Moderate	Moderate	High	High

REFERENCES

[1] Jung Hee Cheon; Jinsu Kim, "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption,", IEEE Transactions on Information Forensics and Security, Vol.10, No. 5, pp. 1052-1063, 2015.

[2] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, Minglu Li, "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, Vol.10, No. 4, pp. 239-250, 2013.

[3] Chirag Modi *et al.*, "A survey on security issues and solutions at different layers of Cloud computing", Proc. International conference on Cloud Security issues, 2012.

[4] Coa, Ning, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel & Distributed Systems, Vol. 25, No. 1, pp. 222-233, 2014.

[5] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS'06, 2006.

[6] R. Sharmila, "Secure Retrieval of Files Using Homomorphic Encryption for Cloud Computing", IJRET: International Journal of Research in Engineering and Technology, pp. 2321-7308, 2014.

[7] Nagesh Jadhav, Jyoti Nikam, Sayli Bahekar,"Semantic Search Supporting Similarity Ranking Over Encrypted Private Cloud Data", International Journal of Emerging Engineering Research and Technology Vol. 2, No. 7, PP215-219, 2014.

[8] R. Anitha, Saswati Mukherjee, "Metadata Driven Efficient CRE based Cipher Key Generation and Distribution in cloud Security", International Journal of Security and Its Applications, Vol. 8, No. 3, 2014.

[9] Jiss Varghese, Lisha Varghese, Fabeela Ali Rawther," Enabling Search and Retrieval over Encrypted Data Using Homomorphic Encryption", International Journal of Innovative Research in Science, Engineering and Technology,Vol.3, No. 5, 2014.

[10] Qiang Tang, “Nothing is for Free: Security in Searching Shared and Encrypted Data”, IEEE Transactions on Information Forensics and Security, Vol.9, No. 11, 2014.

[11] Jung Hee Cheon and Jinsu Kim “A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption”, IEEE Transactions on Information Forensics And Security, Vol. 10, No. 5, 2015.

[12] Penmetsa Raja, V. Krishna, A. S. N. Chakravarthy, and P. S. Avadhani, “A Cryptosystem Based on Hilbert Matrix using Cipher Block Chaining Mode.” International Journal of Mathematics Trends and Technology, pp. *1110-1498,* 2011.