Original Research Article

J. Computing & Int. Systems (2017) 1–5

SACRED HEART RESEARCH PUBLICATIONS

Journal of Computing and Intelligent Systems

Journal homepage: www.shcpub.edu.in

ISSN: 2456 - 9496

Data Security Enhancement in Public Cloud Storage

*Dr. D. I. George Amalarethinam [#1], B. FathimaMary[*2]*

Received on 23 Mar 2017, Accepted on 15 May 2017

Abstract *— Data storage security is a highest concern in the cloud storage. Cloud offers huge amount of space to store their user data. This technology has proved itself as a new venture because of its ability for releasing massive computational storage with reducing cost from anywhere to any user at any time. User outsources their data to the cloud for flexible, efficient and seamless services. Once the data is sent to the cloud, the cloud service provider (CSP) alone is responsible for the data. Apart from the benefits, it has lot of security issues on the data stored in the cloud. When a user outsources the data to the cloud, there is possibility to attack the data at rest as well as data in transit. Now the concern is how to secure the data and rely on the services in cloud. In order to protect the data from unauthorized access, data should be in either encrypted format or masked format. Data security is one of the major issues which acts as an obstacle in the adoption of cloud computing. This paper discusses a confidentiality technique named as Ensured Data Security Strategy using Matrix Random Traversal (eDSSuMRT) and Dynamic Matrix Unique Character Encryption(DMUCE) technique which we have proposed earlier. The both of the techniques are based on symmetric encryption algorithm. It is helpful to enhance the security due to its complexity in encryption process. Experimental was conducted with the existing technique like AES. Both of the technique provides better performance and good security compare than existing techniques. Cipher text developed by this approach can be entirely different when compared to the plain text and will be suitable for the secure storage over the cloud.*

Keywords: *Cloud Computing, Cloud Storage, CSP, Security, Matrix.*

1 INTRODUCTION

Cloud computing is often referred as simply "cloud," is the delivery of on-demand computing resources over the internet on a pay-for-use basis. National Institute of Standard and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. The concept of cloud computing provides three kinds of services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

In that Infrastructure as a Service, Server, Storage and Network services are provided by the Cloud. The primary usage of cloud computing services is data storage. Cloud storage is a service model in which the data is maintained, managed, backed up remotely by a cloud storage service provider(CSP) and made available to users over a network. Many organizations and enterprises felt the difficulties about how to keep the data safe and how to manage those data's. Cloud storage provides enormous amount of space to store the huge volume of data. Once the data outsourced to the cloud, users need not worry about the data. Because, outsourced data to the cloud are kept by third party CSP. Apart from these benefits, a lot of issues occurred related to security, scalability, reliability, data maintenance and data migration etc. also taken care. Security plays a vital role in the cloud environment. Because, of security issues, People hesitate to adopt the cloud storage.

Confidentiality of data is enabled by using efficient cryptography technique [2].Cryptography is an effective tool that helps to protect the data from unauthorized access while data at rest in cloud server. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is the process of encryption and decryption. Cryptographic techniques are classified into Conventional and Public key cryptography [3]. Conventional cryptography is also referred as symmetric key cryptography. The same key is used for encryption and decryption in symmetric key cryptography. Public key cryptography is called as asymmetric key cryptography. Public key and private key are used for encryption and decryption respectively.

According to Tim Mather [4], symmetric encryption is better for data security than asymmetric encryption. Symmetric encryption is more suitable to handle encryption at minimum time, it is much faster than public key cryptography, it is easier to implement and generally requires less processing power. Data can be stored anywhere in any data centre and users don't have any rights to control and monitor the data.

* Corresponding author: E-mail: fathimamary02@gmail.com, di_george@ymail.com

[1] Dean of Science & Director (MCA), Jamal Mohamed College, Trichy, Tamilnadu, India.

[2] Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India.

Cloud storage increases very big issues concerning about data confidentiality. Hence it is needed to propose and implement efficient symmetric encryption technique to enhance the confidentiality of data security, while the data at rest in cloud storage[5][6].

2 RELATED WORK

This section describes some of the past related works already done to improve the security of data. Asif et al. [7] proposed new encryption algorithm for Data security in the Cloud. The proposed hybrid approach uses a data compression method to reduce the size of original data and then encrypt the data using ASIF Encryption Algorithm. Mohamed et al. [8] proposed framework ensures a trusted cloud environment that controlled by both the client and the cloud environment. In this framework, ElGamal based on Elliptic curve cryptography for data encryption/ decryption along with Diffie Hellman. This technique is used to generate a shared secret key between both of them.

Manikondan et al. [9] proposed Arocrypt Symmetric encryption technique to make the cloud data secure. Plaintext is converted into ASCII values. A square matrix is formed based on the number of characters in the plaintext. Kaur et al. [10] presented an approach to effective cloud data storage. The author designed client-server framework to store data securely on the cloud server. In this client - server environment, clients store their data on the server after logging into the system. The proposed environment uses Diffie-Hellman technique and AES technique for encryption and decryption. This technique takes more time for encryption and decryption.

Priya et al.[11] combined Ceaser cipher and Attribute Based Cryptography(ABC) and proposed symmetric algorithm to improve the data security at cloud data storage end. The literature review summarizes, existing encryption is based on substitution, transposition and shift operations. So it reduces the efficiency of techniques. This stimulates the need to propose an efficient technique to enhance the data security [12][13]. Santosh et al. [14] proposed Partitioning technique for Cloud Storage Security. Third Party Auditor is responsible for partitioning the data, secret key generation for each partition, encrypt each partition using respective keys, sending partition at appropriate cloud server. RSA algorithm is used for encryption and decryption. This proposed technique has taken more time for encryption and decryption. From the literature review, sophisticated symmetric encryption technique is needed for cloud users while the data is stored in cloud server.

3 METHODOLOGY

This methodology discusses the DMUCE [15], and eDssuMRT technique [16]. Both techniques are based on the symmetric key cryptography.

There are three processes involved like as encryption, key generation and Decryption. It ensures the confidentiality, and protects the data from unauthorized access when at rest in cloud storage.

A. DMUCE Algorithm

DMUCE algorithm performs encryption in two levels. Initially the unique characters (UCS) are collected from the plain text. From the UCS Actual Character Set (ACS) is created. In the first level unique character positions are encrypted and in the second level Actual character Set (ACS) is encrypted. In first level encryption, Encrypted Base Matrix (EBM) of size mxn is created where m is the number of unique characters and n is the maximum number of appearances of unique characters. The size of the row is set to the number of characters in ACS and the size of the column is set to the maximum number of occurrences of any character in ACS. This Matrix is called as EBM. The remaining columns and rows values are set to 0.The random integer generated is called as Random Matrix (RM). EBM is encrypted by performing the XOR operation with RM. XOR operation is performed only for non zero elements in the corresponding EBM. The resultant matrix Encrypted Matrix(EMAT) is more complicated by doing matrix transpose technique. The transpose of the EMAT is called as EMatT. Finally to improve the efficiency of DMUCE, sparse matrix concept is used.

Sparse matrices are specialized data structures, which allows to store only non zero elements and save a lot of memory and CPU time when working with such matrices. There are several techniques used in sparse matrix. In that Compressed Row Storage (CRS) techniques are used in DMUCE. CRS representation is good for numerical work. In DMUCE, non zero elements, column indices and row pointer are maintained according to the CRS algorithm. Finally, the non zero encrypted elements are maintained. This CRS matrix is called as EMatS. In the second level encryption, another random integer is generated and is called as Random Set (RS). ACS is encrypted by performing the XOR operation with RS. The resultant character set is called Encrypted Character Set (ECS). It will make the ACS more complicated and is very much useful for hiding the original character involved in the plain text. Finally, content of ECS and EMatS are considered as a cipher text. Figure 1 and 2 show the encryption and decryption steps.

B. eDSSuMRT Technique

The eDSSuMRT technique improves classical symmetric encryption by integrating substitution cipher, transposition cipher and ASCII values. The existing encryption method uses substitution, transposition and ASCII values for corresponding alphabets. But the proposed technique uses neither ASCII values nor substitution and transposition of characters. Initially the words list(WL)and words position list(WPL) are generated from the plain text. If the words are repeated again, that words positions are stored in WPL instead of storing that word. Tokens are generated based on the WL and WPL.

A square matrix is formed based on the token. Maximum size of the matrix (Mat) is 25X25. Suppose, if the length of token is less than 100, matrix size is generated dynamically according to the length of token. The generated random integer is called as Random Number (RN). According to RN generation, tokens are placed possibly inside a Mat. Different possible matrix traversal is shown in figure 4. Based on RN, tokens can be placed anywhere inside a Mat. Read the Mat from top to bottom i.e column by column traversal and generate a another matrix named as Matrix Traversal (Mat(T)). Finally merge all block of Mat(T) and considered as a Cipher Text(CT). The secret key is having a main role in encryption and decryption. Figure 3 shows the eDSSuMRT Encryption steps and the Figure 4 shows the eDSSuMRT Decryption steps.

Input: Plain Text, Secret Key
Output: Cipher Text
Steps:

1. Create UCS from file
2. Create EBM for size m x n where m is Number of Unique Characters and n is Maximum Number of appearance of any character.
3. EBMij=Position(c) $\forall c \in U$
4. Create RM using random Integer
5. EMat=EBM XOR RM except 0 values in EBM
6. $EMat^T$=Transpose(EMat)
7. $EMat^S$=SparseMatrix($EMat^T$)
8. Create ACS from UCS
9. Create RS using random character
10. ECS=ACS XOR RS
11. SK Generated with RM base and RS base with random string

Fig. 1 DMUCE Encryption Technique

Input: Cipher Text, Secret Key
Output: Plain Text
Steps:

1. RSBV<=Extract from SK
2. RMBV<=Extract from SK
3. Create RS from RSBV
4. Create RM from RMBV
5. ECS<=Read from File
6. $EMat^S$<= Read from File
7. $EMat^T$=Generate($EMat^S$)
8. ACS=ECS XOR RS
9.
10. EMat=Transpose($EMat^T$)
11. EBM =EMat xor RM except 0 values in EMat
12. Create Heap DH for size m x n
13. DH_{ij}<= ACS_i using EBM_{ij}

Fig.2 DMUCE Decryption Technique

Input: Plain Text, Secret Key
Output: Cipher Text
Steps:

1. Read Words from file
2. Create WL and WPL from file
3. Create token using WL and WPL
4. N=count(token)
   // N-Number of characters in tokens
   // Create the matrix Mat. The size of matrix is 25x25. If N>100 then divide the tokens into 100 character block and form the matrix for each block. If N<100 then size of matrix is created dynamically based on N.
5. Create RN using Random Integer
6. Mat =Random Traverse(token)
7. Mat(T)=CBCT(Mat)
8. CT=Merge all Mat(T)
9. Create Heap EH
   EH<= Create EF using CT
10. SK Generated from RN

Where
WL stands Words List
WPL stands Words Position List
MAT stands Matrix
RN stands Random Number
MAT (T) stands MAT Traversal
CBCT stands Column by Column Traversal
CT stands Cipher Text
EH stands Encrypted Heap
EF stands Encrypted File
SK stands Secret Key

Fig.3 eDSSuMRT Encryption Technique

Input: Cipher Text, Secret Key
Output: Plain Text
Steps:

1. SK<=Extract RN
2. EH<=Extract EF
3. EF<=Extract CT
4. CT<=Extract all block Mat(T)
5. Mat(T)<= Extract Mat using CBCT
6. Mat<=Extract tokens
7. Merge all Mat block
8. Regenerate token
9. Regenerate WL and WPL from token
10. Create Heap DH

DH<= Create DF using WL and WPL

Where
DH stands Decrypted Heap
DF stands Decrypted File

Fig.4 eDSSuMRT Decryption Technique

4 METHODOLOGY

The Techniques are implemented in Java. Encryption and decryption time of eDSSuMRT and DMUCE technique with various file sizes are compared with AES technique shown in table 1 and table 2. The graphical representation of the table 1 and table 2 is shown in figure 5 and 6.

TABLE I

COMPARISON BASED ON ENCRYPTION TIME IN MILLI SECONDS

File Size(MB)	AES	DMUCE	eDSSuMRT
1	2964	2933	2370
2	5424	5396	4283
3	8347	7859	6512
4	11170	10322	9031
5	14213	12700	11293

TABLE II

COMPARISON BASED ON DECRYPTION TIME IN MILLI SECONDS

File Size(MB)	AES	DMUCE	eDSSuMRT
1	3005	2937	2374
2	5321	5401	4240
3	8354	7863	6547
4	11283	10329	8844
5	14142	12706	11368

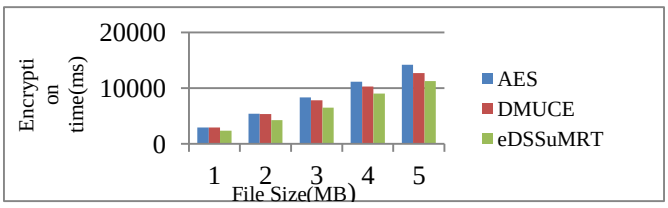

Fig.5 Comparison of Encryption Time

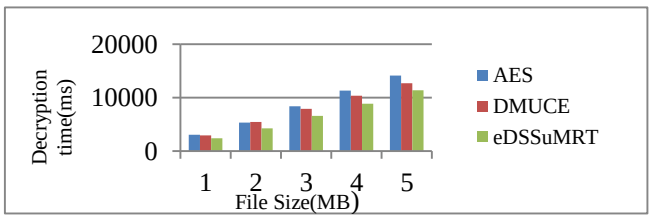

Fig.6 Comparison of Decryption Time

In Table 1, when the file size is 1 mb, AES technique produces the encryption time as 2964 ms DMUCE technique produces the encryption time as 2933 ms and whereas the eDSSuMRT technique produces in 2370 ms. Similarly when the file size is 5 mb, AES technique produces the encryption time as 14213 ms and DMUCE technique gives the encryption time as 12700 ms and the proposed eDSSuMRT technique takes 11293 ms. In Table 2, when the file size is 1 mb, AES technique produces the decryption time as 3005 ms and DMUCE technique produces the decryption time as 2937 ms whereas the eDSSuMRT technique produces in 2374 ms. Similarly when the file size is 5 mb, AES technique takes 14142 ms EDMUCE technique gives the decryption time as 12706 ms and the whereas the eDSSuMRT technique takes 11368 ms. Figure 5 and Figure 6 shows the graphical representation of these techniques.

Times taken for these techniques are calculated for different sizes of data. The result shows that the DMUCE and eDSSuMRT technique has taken minimum time duration for encrypting and decrypting the data of different sizes when compared to the existing technique. From the analysis, both DMUCE and eDSSuMRT techniques get minimum time. Hence, confidentiality of data is improved by these proposed approaches.

5 CONCLUSIONS

Cloud Storage provides cost-effective services to individual users as well as organization. It provides huge amount of space to outsource the data to the cloud. Organization and enterprises do not possess full infrastructure to maintain their data with their premises. Data outsourcing helps to effectively maintain their data in cloud storage. But, data security plays a vital role in Cloud. Due to this reason, organization and enterprises are hesitant to outsource their data to the cloud. This paper discusses a new confidentiality technique named as DMUCE and eDSSuMRT technique to address the security problems in cloud storage. This work introduces an additional level of security using the character position. In the existing work, repetition of cipher text value takes place when the characters are repeated in the plain text because of ASCII value. In DMUCE and eDSSuMRT, there is no repetition of values. Even though the repetition of same character takes place, it takes the character position for each occurrence of the character. By adopting this, any intruder may find it difficult to ascertain the information being stored. An experimental result shows that DMUCE and eDSSuMRT technique offer better performance than the existing technique. In future, both the algorithms are tested against the security by security analysis tool called hackman tool.

REFERENCES

[1] Buyya R, Vecchiola C, S. ThamaraiSelvi," Mastering Cloud Computing Foundations and Applications Programming" ,Elsevier, pp.1-469,2013.

[2] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Elsevier Science Publishers; vol.25,pp.599–616,2009.

[3] Kelsey Rauber, "Cloud Cryptography", International Journal of Pure and Applied Mathematics, Vol. 85, pp. 1-11, 2013.

[4] Mather T., Kumaraswamy S. and Shahed, L., "Cloud security and privacy", Chapter 4, O'Reilly Media, Inc, pp. 61-71, 2009.

[5] Tushar Kanti Saha, A B M Shawkat Ali, "Storage Cost Minimizing in Cloud – A Proposed Novel Approach Based on Multiple Key Cryptography", Proceedings of the IEEE Asia- Pacific World Congress on Computer Science and Engineering, IEEE, pp.1–9,2014.

[6] Balajee Maram, K. Lakshmana Rao, Y. Ramesh Kumar, "Encryption and Decryption technique using 2-D Matrices", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, April 2013.

[7] Md Asif Mushtaque, Harsh Dhiman, Shahnawaz Hussain, " A Hybrid Approach and Implementation of a NewEncryption Algorithm for Data Security in CloudComputing", International Research Publication House, Vol.7, pp.669-675, 2014.

[8] Ayman Helmy Mohamed, Aliaa A.A. Youssif, Atef Z. Ghalwash, " Cloud Computing Security Framework based on Elliptical Curve", International Journal of Computer Applications, Vol.110, No. 15,pp.45-51,2015.

[9] S. Monikandan, Dr.L.Arokiam, "Arocrypt: A Confidentiality Technique For Securing Enterprise's Data In Cloud", International Journal of Engineering and Technology,Vol.7,Issue.1, pp.245-253,2015.

[10] Sandeep Kaur," Using Encryption Technique for Effective Data Storage", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5,Issue 3,pp.616-621,2015.

[11] Aayushi Priya, Y.K. Rana, B.P. Patel," Design and Implementation of an Algorithm to Enhance Cloud Security", International Journal of Computer Applications, Vol.113, pp.41-47, 2015.

[12] Karun Handa, Uma Singh," Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, Vol.4,Issue 5, pp.786-791,2015.

[13] S. Arul Oli,Dr.L.Arokiam," A Novel Approach for Ensuring Data Confidentiality in Public Cloud Storage", International Journal of Computer Applications,Vol.0,pp.1-5,2014.

[14] Santosh Jogade, Ravi Sharma, Rajani Kadam," Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique", International Journal of Emerging Research in Management &Technology,Vol.3,pp.133-138,2014.

[15] Dr.D.I.George Amalarethinam, B.FathimaMary, " DMUCE- A Confidentiality Enabled Technique To Improve Cloud User Security", International Journal of Applied Engineering Research, Vol.10,Issue 10,2015.

[16] Dr.D.I.George Amalarethinam, B.FathimaMary," eDSSuMRT- Ensured Data Security Strategy Using Matrix Random Traversal in Cloud Storage Environment", International Journal of Applied Engineering Research, Vol.10,Issue 82,2015.