IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

ADSSCCE: Analysis of Data Storage Security in Cloud Computing Environment

Ramalingam Sugumar[1*], K. Arul Marie Joycee[2]

[1,2]ChristhuRaj College, Panjapoor, Tiruchirappalli, Tamil Nadu, India

[*]*Corresponding Author: rsugusakthi1974@gmail.com*

Available online at: www.ijcseonline.org

Abstract--- Cloud computing contextual is a computing model for dealing and accessing services over the internet. It delivers variety of services to the recipient for on-demand. The very important service of the cloud environment is data storage. The data storage in the internet is varying day by day and the data size also varying based on the users need. The end users required the best security mechanism's. The motivation of this research is to encrypt and decrypt data efficiently and effectively protect the stored data. All over the world the data center is placed in many different locations to maintain and monitor the user data. It is more reliable storage but it has many securities related problems and different kinds issues. The problem is how to secure the data in cloud storage, to protect the data from unauthorized user's access, data is supposed to either encrypted format or unreadable form. This paper analysis the various cloud data storage security algorithms.

Keywords—Component, Formatting, Style, Styling, Insert (key words)

I. 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. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling 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. Because of these benefits each and every organization are moving their data to the cloud.

So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms. [1]

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption [2]. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms. [3]

II. DATA STORAGE SECURITY IN CLOUD COMPUTING

Cryptography

Cryptography is the art and science of hiding information or data from unintended users. Some examples of symmetric and asymmetric cryptographic algorithms are discussed below: [4]

Symmetric Encryption Algorithms

Symmetric key encryption algorithms [5] also known as private key encryption used the same key for both encryption and decryption. Some example of Symmetric key encryption algorithms is discussed below:

A. Data Encryption Standard (DES)

DES is a block cipher symmetric encryption algorithm with key size of 64 bit. It was the first encryption algorithm developed by IBM and accepted for use by America National Institute of Standard and Tech-nology (NIST) in1977.DES algorithms used only 56bits of it is data for encryption and the remaining 8bits is used for error detection. DES is considered in-secured because of it small key size and was replaced by Triple Data Encryption Standard.

B. Triple Data Encryption Standard (3DES)
3DES it is an improvement of DES algorithms. 3DES uses 192-bit key size because it uses three times the 64 bit keys length used by DES to encrypt and decrypt data. The encryption process of 3DES is similar with that of its predecessor just that 3DES applied three times DES to increase the security level of the data and that makes it one of the slowest block symmetric ciphers used today.

C. Advance Encryption Standard (AES)
AES algorithms was developed in 1998 and accepted by National Institute of Science and Technology America (NIST) in 2001. The algorithm was considered a replacement for DES and 3DES because of it key strength and flexibility. Today AES is accepted and used worldwide. AES encrypts data block of 128bit, 192bit and 256bit in 10, 12 and 14 rounds respectively. AES is used on varieties of devices and applications because of its flexibility and key strength.

D. Blowfish
Blowfish is 64bit block cipher with variable key lengths ranging from 32 to 448. As stated in Blowfish algorithm consists of two parts: key expansion part and data encryption part. Key expansion converts the key into several sub key arrays of total 4168 bytes. Data encryption part is done via 16 round Feistel network. Each round consists of the key permutation, and the key and data dependent substitution.

2.1.2 Asymmetric Encryption Algorithms
Asymmetric key encryption algorithms also known as public key encryption algorithms use different keys, private and public keys for encryption and decryption unlike the symmetric key encryption algorithms. Examples of some asymmetric key encryption algorithms are discussed below:

A. Rivest Shamir Adleman (RSA)
RSA is asymmetric key encryption algorithm developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. It was named after its developers Rivest, Shamir and Adleman. It uses two keys, public key and private key. The public key is known by all users while the private key is only known to the valid users for authentication and verifica-tion. The activities in RSA involve key generation, encryption and decryption. The key length of RSA ranges from 1042 to 4096.

B. Digital Signature Algorithm (DSA)
A digital signature algorithm is an electronic key used for verification and authentication of user or data in the cloud. The algorithm was initiated by National Institute of Science and Technology USA in 1991 to be used in their Digital signature standard (DSS) and was incorpo-rated in 1993. The algorithm works by first of all making choice of encryption parameters which will be shared across several users of the system and then in the second stage private and public key is created for single user. The signature is created with the private key by the sender and then it's verified and authenticated by the receiver using the public key. DSA has a key size of 3072bits. However, cryptography[6] has some challenges when handling complex data such as those in the cloud where the data are kept in different locations and processed from different data centers; the means of the transfer of these data from one location to another on the cloud would make the data appear suspicious to intruders because cryptography cannot hide the existence of these data during transfer from intruders. [7] [8]

III. RELATED WORK

Privacy Algorithms to Improve the Secure Framework for Cloud Computing Environment
The main aim of this work is to design an architecture that can help to encrypt and decrypt algorithm. In this work presenting an encryption algorithm to deal with the privacy problems in cloud computing and protect the data stored in the cloud. The privacy algorithm is also called the encryption and decryption algorithm. This method uses DES and RSA algorithm to generate encryption when a user uploads the text files in cloud storage, and opposite DES and RSA algorithm to generate decryption. It is the most popular algorithm to find all the cloud data storage. Encryption technique is a scientific solution for data protection in cloud. Therefore, the work is to look at database encryption approaches for ecommerce cloud functions. Database level relies on the encryption functions provided by DBMS. Like the databases Oracle, SQL Server, and Mysql. User from the private or public domain can request the file from the server. Encryption algorithm converts the data into Cipher text form by using the fixed key and only user have the key to decrypt the Cipher chain. That is, only one fixed key is used to encrypt and decrypt the cloud data. [9]

Rail fence Transposition Technique The rail fence technique is one of the transposition ciphers that get its name from the way, in which the plaintext it is encoded. In the rail fence technique, the plaintext is written downwards as a sequence of rows. Then moving up when we get to the bottom. For example, using the message of "**welcome cloud**",
with the cipher writes:

w l o e l u
e c m c o d

Now the reads off encrypted message are "w l o e l u e c m c o d".
In this technique, the same alphabets in the plaintext are rearranged. This technique alone cannot be satisfactory for privacy data storage.
Steps of Privacy Algorithm
A. Encryption Algorithm
Followings are the step in privacy encryption algorithm is as given below:
Step 1: Initialize: get the plaintext letter.
Step 2: Get the fixed key length from the range numbers (0 to 256).
Step 3: Assign the position (i) of the letter.
Step 4: Generate the ASCII value of the plaintext letter. Step 5: Assigned same fixed key length is considered as a key.
Step 6: Convert the plain text into equivalent ASCII code.
Step 7: Encrypted the value using addition.
Step 8: To apply the formula given below: E = (p + k) + i mod256
Step 9: The generate ASCII character of the corresponding decimal value in the result from the above given formula. This would be the cipher text.

Figure 1: Execution of entire encryption process

B. Decryption Algorithm
Step 1: Initialize: generate the ASCII value of the cipher text character.
Step 2: Here the same encryption fixed key length used.
Step 3: Assigned the position (i) of the cipher text.
Step 4: let subtract the value with ASCII code.
Step 5: To apply the formula given below:

D = ((c – k – i) + 256) mod 256

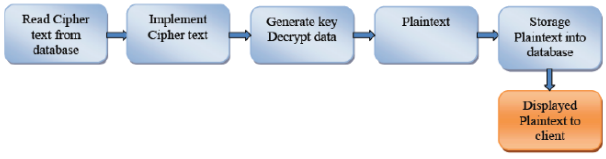

Figure 2: Execution of entire decryption process

Ensure and Secure Data Confidentiality using Data Obfuscation Technique

This obfuscation technique is used to secure the numerical data in the cloud storage. The user wants to encrypt the numerical data by obfuscation and then this technique is right and convenient. This technique is a symmetric crypto system. Here two key are used for encryption and decryption this two key are integer values.

This confidentiality system SUG-DO uses different mathematical operations such as Max ( ), Pow ( ), Mul ( ), Sub( ) , Mod(), Ascii( ) on numerical data. The keys are generated in cloud side and it forwarded to the end users. The keys are managed and maintained by the cloud service provider. [10]

The SUG-DO algorithm is given below
Algorithms- SUG-DO (digit Encryption)
The encryption algorithm steps.

Algorithm: 1 Encryption
Step 1: Count the Number of Numerical character (N) in the plain text without space.
Step 2: find the maximum value in the plain text as a Key K1 (MAX(PT)
Step 3: Product the K1 to Plain text Store the values to PRO.
Step 4: Calculate the Power of (PPT- *POW (PRO,3))*
Step 5: Take the key K2 from plain text position values.
Step 6: Subtract the K2 to PPT.
Step 7 : Modulo of SUB value
Val= MOD of SUB.
Step 8: Check the Val Value
a: If Val lessthan 32
Then Val = 32 +Val
Step9: Convert the Val into ASCII code.
Step 9: End

The followings are the detailed description of each step in the encryption algorithm.

Step1: Count the Number of characters (N) in the message without space.
Plaintext – 37, 54, 89, 42, 92, 77
Step 2: Maximum Value (MAX= 92)(K1=92)

Step 3: PRO= K1 * PT
PRO= 3404 (92 * 37)
Step 4: Calculate PPT = (POW (PRO, 3))
PPT= (POW, 3404,3)
PPT= 39442883264

Step 5: Take the PT as K2
Plaintext – 37, 54, 89, 42, 92, 77
Position - 1 2 3 4 5 6
SUB= 39442883264- 1
SUB = 39442883263

Step 6 : MOD of SUB by 256.
MOD = 39442883263 % 256
MOD= 191 ,Val= 191
Step 7: Suppose the value of Val is lessthan 32 then val= val +32
Step 8: ASCII value of Val
ASCII value of 191 = ┐
Encrypted Text: ┐■╜ⁿ√╟
Algorithm: 2 Decryption

The encrypted data is stored in the cloud storage. To retrieve the data from cloud, the decryption process is essential to get the actual data in the cloud storage area. Decryption is possible only with key values which are used for encryption algorithm. So the keys are plays the major and main role in the encryption and decryption algorithm.

Algorithm - Decryption.
Step 1: The encrypted text is converted into ASCII code values.
To find the PPT value
Step 2: add the value of SUB (i) and K2.

Step 3: Inverse cube value of PPT
Step 4: divided PPT value by MAX (PT)
Step 5: display the plain text (PT)

The followings are the detailed description of each step in the decryption algorithm.

Step1: Each character in the encrypted text is converted into equivalent ASCII code values.

Encrypted Text: ┐■╜ⁿ√╟

Equivalent decimal values of the above ASCII code, as

191,254,189,252,251,186

To find the PPT value

Step 2: Add the value of SUB (i) and K2.
SUB (1)+1, SUB(39442883263+K2
SUB (1)= 39442883264
Where K2 is the position of the PT

Step 3: Inverse cube of SUB(1)
PPT = 3404
Step 4: divided by the PPT with MAX (PT)
PT =PPT/MAX(PT)
PT = 3404/92
PT= 37
Now the original Plan Text,
37,54,89,42,92,77

Convert the ASCII code into equivalent numerical value. Then, Decrypted result is, 37,54,89,42,92,77
By end of all these steps in the decryption algorithm the original text is retrieved by the user.

DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm

The DSCESEA technique is to improve the classical encryption techniques by integrating substitution cipher and transposition cipher. This substitution and transposition techniques have used alphabet for cipher text. In this algorithm, first stage the plain text is converted into corresponding ASCII code (Hexa)value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 or key may be string (combination alphabets). But this algorithm, key value range between 1 to 256. This algorithm is used in order to encrypt the data of the user in the clouds. Users can store data on demand or for the applications without keeping any local copy of the data on their machine. Since the user has no control over the data after his session is logged out, the encryption key plays the very important role and its primary authentication for the user. This algorithm is described below. [11]

The given steps are the encryption algorithm steps.
Algorithm: 1 Encryption
Step 1: Count the No. of character (N) in the plain text without space.
Step 2: Convert the plain text into equivalent ASCII code. And form a square matrix (S X S >=N).
Step 3: Apply the converted HEXA code value form the Tranpose Matrix ($A=A^T$)
Step 4: Store the values of AT values in ascending order.
Step 5: Take the even column (2,4) vales Rewrite the row wise and odd column values (1,3) values rewire to the row *wise (R1=2c1, R2=4c1, R3=1c1,R4=1c3)*
Step 6: Take the key values 23,32,12,21 and Ex-Or with the each row of the matrix.
Step 7: Apply the encrypted value into the matrix in the same order
Step 8: Read the message by column by column. Using the key values (key values 2,4,1,3)
Step 9: Convert the ASCII code into character value.

IV. PERFORMANCE ANALYSIS OF LOAD BALANCING ALGORITH

The forthcoming part discusses various security algorithms and shows the results comparatively. Now we will analyses the various security algorithms by setting the configurations of the various components of the cloud environment using Microsoft azure real time cloud, which runs on ASP, SQL database and Microsoft azure as a deploying tool.

Table 1: Encryption Time for different Input Size

Input size (in bytes)	Privacy Algorithm Encryption Time	DSCESEA Algorithm encryption Time	SUG-DO Algorithm Encryption Time
328	0.035314	0.031324	0.031221
561	0.065321	0.062432	0.062002
899	0.104311	0.100211	0.100201
1535	0.350245	0.331267	0.331225

.

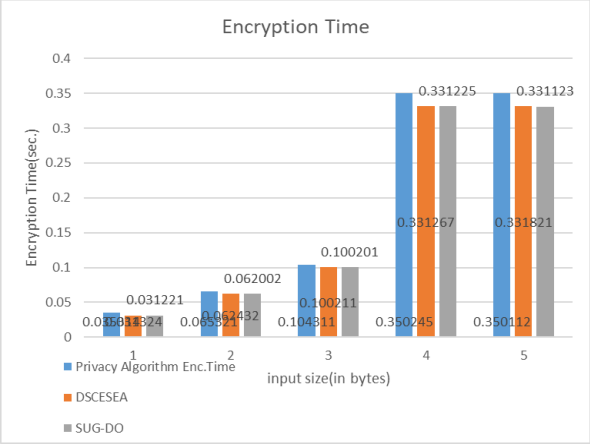

Figure 3: Comparision of Encryption Time

Table 2: Decryption Time for different Input Size

Input size (in bytes)	Privacy Algorithm Decryption Time	DSCESEA Algorithm Decryption Time	SUG-DO Algorithm Decryption Time
328	Njp0u	0.010345	0.010334
561	0.036045	0.021123	0.021112
899	0.104436	0.100223	0.100122
1535	0.221032	0.211029	0.211012

.

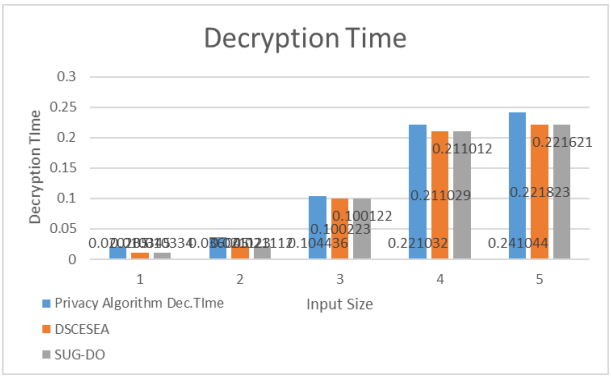

Figure 4: Comparison of Decryption Time

The DSCESEA and SUG-Do algorithm takes minimum time for encryption and decryption. The tables above Table1 and Table2 shows the execution time corresponding to different input sizes. Figure 3 and 4 shows that comparison of execution processing time in encryption and decryption with respect to different key range. So the time consumption for converting cipher data to the original data. The privacy algorithm takes maximum time for encryption and decryption. This shows that the DSCESEA and SUG-DO algorithm used minimum time for encryption and decryption process. This is due to the use of enhanced approach, which increases the data storage security. Finally, as a result are compared and analyzed, we can see that the DSCESEA and SUG-DO algorithm approach takes minimum time in comparison to a privacy algorithm.

V. CONCLUSION

The main conclusions of the study may be presented in a short Conclusion Section. In this section, the author(s) should also briefly discuss the limitations of the research and Future Scope for improvement.

VI. PREPARE YOUR PAPER BEFORE STYLING

This paper analyzed various data security algorithms in cloud computing environment like privacy, DSCESEA and SUG-DP algorithms. The cloud computing environment Security and Privacy are important role in storing of data in that location. So many researchers are work in that area. Cryptographic techniques are used to provide secure communication between the user and the cloud. The generated key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders. The main advantages of this work are only the authorized user can access the cloud storage data. The future work will focus on additional privacy for cloud data storage in the cloud computing environment.

REFERENCES

[1] Shakeeba S. Khan, Prof.R.R. Tuteja," Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 1, January 2015.

[2] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", El-Booz et al. EURASIP Journal on Information Security ,2016.

[3] Fortine Mata, Michael Kimwele, George Okeyo, "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish)" , International Journal of Science and Research, Volume 6 Issue 3, March 2017.

[4] S. Balamurugan, Dr. S. Sathyanarayana, Enhanced Security as a Service to Protect Data in Public Cloud Storage", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2016.

[5] Adamu Ismail Abdulkarim, Boukari Souley, "An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography" International Journal of Scientific & Engineering Research Volume 8, Issue 7, July-2017.

[6] A.M. Vengadapurvaja, G. Nisha, R. Aarthy, N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security", Science direct- 7th International Conference on Advances in Computing & Communications, Cochin, India , August 2017.

[7] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[8] Sawase Akanksha and B.M.Patil, "A Secure Multiowner Dynamic Groups Data Sharing In Cloud", International Journal of Advances in Engineering & Technology, Feb., 2016.

[9] Anshu Chaturvedi, D.N.Goswami, Rakesh Prasad Sarang, "Privacy Algorithms to Improve the Secure Framework for Cloud Computing Environment" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2017.

[10] Dr. R. Sugumar, K. Arul Marie Joycee,"DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm" International Journal of Engineering Research & Technology, Vol. 6 Issue 10, October – 2017.

[11] Dr. R. Sugumar, K. Arul Marie Joycee ,"Ensure and Secure Data Confidentiality in Cloud Computing Environment using Data Obfuscation Technique", International Journal Of Advanced Studies In Computer Science And Engineering, Volume 6, Issue 12, 2017.

