International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm

Dr. R. Sugumar,
Professor & Deputy Director,
ChristhuRaj College , Panjapoor,
Tiruchirappalli, Tamil Nadu India

K. Arul Marie Joycee,
Ph. D. Research Scholar,
ChristhuRaj College , Panjapoor,
Tiruchirappalli, Tamil Nadu India

Abstract: **Cloud computing is the well-known technology for scaling of extensive data and complex computation. Cloud computing has increased fast in many companies. Cloud computing offers many benefits in terms of low cost and accessibility of data. Increasing data volume is giving the bigger task of Data Centers (DCs) to provide a better quality of cloud computing. The main usage of cloud computing is data storage. It is more reliable and flexible to users to store and retrieve their data at anytime and anywhere. the security of cloud computing plays a major role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. Customers are wondering about attacks on the integrity and the availability of their data in the cloud from malicious insiders and outsiders, and from any collateral damage of cloud services. These issues are extremely significant but there is still much room for security research in cloud computing. This paper is to propose an encryption based algorithm it produces the data security in cloud storage.**

Keywords: Cloud Storage, Security, Encryption algorithm.

I-INTRODUCTION

Cloud computing has been envisioned as the next generation of distributed/utility computing. It is defined as 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. The National Institute of Standards and Technology (NIST) defines cloud computing by five essential characteristics, three service models, and four deployment models. The essential characteristics are on-demand self-service, location-independent resource pooling, broad network access, rapid resource elasticity, and measured service.

The main three service models are software as a service (SAAS), platform as a service (PAAS), and infrastructure as a service (IAAS). The deployment models include private cloud, public cloud, community cloud, and hybrid cloud.

Nowadays, cloud-computing paradigm can offer any conceivable form of services, such as computational resources for high performance computing applications, web services, social networking, and telecommunications services. In addition, cloud storage in data centers can be useful for users to store and access their data remotely anywhere anytime without any additional burden. However, the major problem of cloud data storage is security. Therefore, cloud data centers should have some mechanisms able to specify storage correctness and integrity of data stored on cloud.[1]

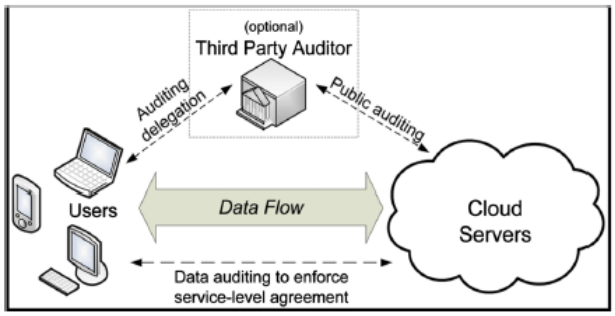

Fig1: Architecture of cloud storage environment

II- RELATED WORK

The authentication level of security by using two authentication techniques, time-based one-time password (TOTP) for cloud users verification and automatic blocker protocol (ABP) to fully protect the system from unauthorized third party auditor. The experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity.[1]

An encryption algorithm to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud. The problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage.[2]

A secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. This scheme is able to support dynamic groups. These dynamic groups are generating a group signature and dynamic broadcast encryption techniques, any cloud user can share data with others securely. The main purpose of this scheme is securely using cloud services storing and sharing by multiple owner groups.[3]

Propose a strategy to secure data by splitting the data into sections by using data splitting algorithm which assures data reliability. Prakar and Kak [4]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

The symmetric cryptographic algorithm named as AES (Advanced Encryption Standard). It is based on several substitutions, permutation and transformation. On the other hand security of the data in the cloud database server is the key area of concern in the acceptance of cloud. It requires a very high degree of privacy and authentication. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data.[5]

The architecture the intrusion detection and prevention is performed automatically by defining rules for the major attacks and alert the system automatically. The major attacks/events includes vulnerabilities, cross site scripting (XSS), SQL injection, cookie poisoning, wrapping. Data deduplication technique allows the cloud users to manage their cloud storage space effectively by avoiding storage of repeated data's and save bandwidth. The data are finally stored in cloud server namely CloudMe. To ensure data confidentiality the data are stored in an encrypted type using Advanced Encryption Standard (AES) algorithm.[6]

a secure cloud storage system supporting privacy-preserving public auditing. Further extend the result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the schemes are provably secure and highly efficient.[7].

Presents integrity auditing scheme which provides a complete outsourcing solution of data. After introducing notations considered and brief preliminaries, started from an overview of data Integrity auditing scheme. Then, presenting main scheme and show how to extent the scheme to support integrity auditing for the TPA upon delegations from multiple users. Finally, How to generalize integrity auditing keeping data privacy scheme and its support of dynamic data.[8]

Steganography and Cloud Computing, the security level of both can hold together and create a greater safety standard. The pixels are inverted and sent to Five Modulus Method (FMM) or Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT) algorithm based on its size and complexity. The steganography image is then transmitted to the receiver using the SaaS infrastructure. Using the Software as a Service (SaaS) Document Management, the image is stored, and shared to the receiver, which reduces the extra steps of upload and download, sending via email or any other meaning of communication. SaaS is Cost-efficient, secure, and scalable. Hence an efficient usage of its security and resources to create a system that can handle them in Cloud without any necessity to download an application to the network.[9]

III. PROPOSED ALGORITHM

The Proposed technique 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 the over proposed 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 our proposed 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 there machine. Since the user has no control over the data after his session is logged out, the encryption key play the very important role and its primary authentication for the user. Proposed algorithm is described below.

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.

The followings are the detailed step in the encryption algorithm.

Step1: Count No. of characters (N) in the message without space.
Plaintext – COMPUTERSECURITY
N= 16 (N = No. of Characters in the Message)
Step 2: Convert the plain text into equivalent ASCII code. And form a square matrix.

ASCII code value for the plaintext (Hexadecimal Code)
43,4F,4D,50,55,54,45,52,53,45,43,55,52,49,54,59
To form a square matrix Form a 4 x 4 matrix.
Matrix= A

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

43	4F	4D	50
55	54	45	52
53	45	43	55
52	49	54	59

Step 3: Transpose Matrix AT

43	55	53	52
4F	54	45	49
4D	45	43	54
50	52	55	59

Step 4: Store the values form A[0] to A[15]matrix.

A[0]=43,A[1]=55,…..A[16]=59

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)

2 4 1 3

55	54	53	52
52	49	54	59
43	4F	4D	50
53	45	43	55

Step 6: Take the key values 23,32,12,21 and Ex-Or with the each row of the matrix.

55	=	5	5
		0101	0101
Key 23=		0010	0011
		0111(7)	0110(6)

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 ,4,1,2,3)

Step 9: Convert the ASCII code into character value.

71	6B	42	74
76	60	51	72
77	7B	5D	64
66	66	5F	62

Encrypted Text: qkBtv`Qrw{]dff_b

76	77	66	71
60	7B	66	6B
51	5D	5F	42
72	64	62	74

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 key plays the major and main role in the encryption and decryption algorithm.

The given steps are the decryption algorithm steps.

Algorithm: 2 Decryption

Step 1: The encrypted text is converted into ASCII code values.

Step 2: Count the No. of character (N) in the decrypted text and form a square matrix S x S.

Step 3: Read the message in reverse order of the key value row by column.

Step 4: Take the key values 23,32,12,21 and Ex-Or with the each row of the matrix.

Step 5: Rearrange in to ascending order form A[0] to A[15]matrix.

Step6: To find the Transpose Matrix $(A^T)^T = A$

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: qkBtv`Qrw{]dff_b

Step2: Convert it into ASCII code, as below

71,6B,42,74,76,60,51,72,77,7B,5D,64,66,66,5F,62

Step 3: Read the message in reverse order of the key value row by column.

76	77	66	71
60	7B	66	6B
51	5D	5F	42
72	64	62	74

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

Step 4: Take the key values 23,32,12,21 and Ex-Or with the each row of the matrix.

76	=	7	6
		0111	01I0
Key 23=		0010	0011
		0101(5)	0101(5)

55	54	53	52
52	49	54	59
43	4F	4D	50
53	45	43	55

Now the message is,
43,4F,4D,50,55,54,45,52,53,45,43,55,52,49,54,59

Step 5: Rearrange in to ascending order form A[0] to A[15]matrix.

43	55	53	52
4F	54	45	49
4D	45	43	54
50	52	55	59

Step6: To find the Transpose of Matrix($A^T)^T = A$

43	4F	4D	50
55	54	45	52
53	45	43	55
52	49	54	59

Convert the ASCII code into equivalent character value.
Then, Decrypted result is, COMPUTERSECURITY

By end of all these steps in the decryption algorithm the original text is retrieved by the user.

VI. CONCLUSION

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. This paper proposed a symmetric based encryption algorithm for secure data storage in cloud storage. 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.

IV- REFERENCES

[1] 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) 2016:13.

[2] 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

[3] Sawase Akanksha and B.M.Patil, “A Secure Multiowner Dynamic Groups Data Sharing In Cloud”, International Journal of Advances in Engineering & Technology, Feb., 2016. ISSN: 22311963.

[4] Parakh A and Kak S, “Online Data Storage using Implicit Security”, International Journal of Information Sciences, vol. 179, no. 19, pp. 3323-3331, 2009.

[5] Vishal R. Pancholi, Dr. Bhadresh P. Patel,“ Enhancement of Cloud Computing with secure data storage using AES”, International Journal for Innovative Research in Science & Technology Volume 2 Issue 09 February 2016 ISSN (online): 2349-6010

[6] R. Shobana, K. Shantha shalini, S. Leelavathy V. Sridevi, “De-Duplication of data in cloud”, Int. j. chem. sci.: 14(4), 2016, 2933-2938,Issn 0972-768x.

[7] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, “Privacy-Preserving Public Auditing for Secure Cloud Storage”.

[8] Wale Amol D, Vedant Rastogi,“ Data Integrity Auditing of Cloud Storage”, International Journal of Computer Applications (0975 – 8887) Volume 133 – No.17, January 2016.

[9] Ihssan Alkadi, Sarah Robert ,“Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform”, Journal of Computer Science Applications and Information Technology. Received: October 12, 2016; Accepted: October 16, 2016; Published: January 20, 2017.