International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

EDSMCCE : Enhanced Data Security Methodology for Cloud Computing Environment

Dr. Ramalingam Sugumar[1], K. Raja[2]
[1]Professor & Deputy Director, Christhu Raj College, Trichy, Tamil Nadu, India
[2]Ph.D Scholar , Christhu Raj College, Trichy, Tamil Nadu, India

ABSTRACT

Cloud computing refers internet based computing which is used to sharing of services. Different users place their data in the cloud. Hence, the fact that users no longer have physical possession of the possibly huge size of outsourced data causes the data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. In the reason of, fitness of data and security is a major concern. The security of cloud computing plays a vital role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. The main issue of cloud storage is to secure the data. Many of the security algorithms are available in the cloud computing environment. This proposed algorithm is also to ensure the data key generation very important. In this proposed method ANENC table is used to generate key and perform several versatile operation used to secure the data in cloud computing.

Keywords: Alpha Numeric, EN Cryption(ANENC), 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]

Figure 1. Cloud security

II. RELATED WORK

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.[1]

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.[2]

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.[3]

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.[4]

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] Propose a strategy to secure data by splitting the data into sections by using data splitting algorithm which assures data reliability. Prakar and Kak [6]

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.[7] a secure cloud storage system supporting privacypreserving 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 [8].

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.[9] Maragoni et al.[10] discussed several issuses of cloud security.

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 256 or key may be string (combination alphabets). But our proposed algorithm, key value range in between 1 to 127.

The given steps are the encryption algorithm steps.

Algorithm: 1 Encryption

Step 1: Count the Number 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 Decimal code value form the Tranpose Matrix ($A=A^T$)
Step 4: Store the values of A^T values in ascending order. (A[0],A[1],A[2],…..A[N])
Step 5: Apply to Shift row transformation
Step 6: Key generation. To construct ANeng table
Step 7: Find out the position of plain text in the ANeng key table. Take the equivalent value of plain text in which the row, column intersect
Step 8: Form a square matrix (S_X S >=N) for the key value (the key value contain decimal values) The maximum key size 36(6X6), if plain text is more than 36 characters the same key will be appended.
Step 9: Add the matrix A with key value.
Step 10: Read the message by, column by column using the key value 2431
Step 11: Find the modulus value of the matrix
Step 12: If the value <32 the add value+32
Step 13: Convert the ASCII code into character value

Figure 2: Proposed encryption algorithm

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 play the very important role and its primary authentication for the user. Proposed algorithm is described below. The key is generated by using ANenc table. The ANenc table construct by using 8X8 matrix and rows and columns are numbered from 1 to 8 and it contains alpha, numeric, two special characters. Alphabet uppercase A-Z and lowercase a-z, number 0-9, special character $, #. Figure 2 shows the encryption algorithms.

36	121	7	24
13	10	18	33
28	26	55	29
35	56	58	18

The detailed steps of encrypted algorithm.

Step 1: Count the Number of character (N) in the plain text without space.
Plain text : WelcomeToCollege
N= 16 (N = No. of Characters in the Message)

Step 2: Convert the plain text into equivalent ASCII code. And form a square matrix (S x S >=N).
The ANENC table generated by 8X8 matrix.
ASCII code value for the plaintext (Decimal Code) 87,101,108,99,111,109,101,84,111,67,111,108,108,101,103,101 To form a square matrix Form a 4 x 4 matrix.
Matrix= A

87	101	108	99
111	109	101	84
111	67	111	108
108	101	103	101

Step 3: Apply the converted Decimal code value form the Transpose Matrix ($A=A^T$)

87	111	111	108
101	109	67	101
108	101	111	103
99	84	108	101

Step 4: Store the values of A^T values in ascending order. (A[0],A[1],A[2],…..A[N])
Store the values form A[0] to A[15]matrix.

A[0]=87,A[1]=111,…..A[16]=101

Step 5: Apply to Shift row transformation

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

Step 6: Key generation. To construct ANeng table
The ANENC table consists of alphabets, numeric and two special characters.
Alphabetic: Upper case A-Z
Lower case a-z
Numeric : 0-9
Special characters: $,#

	1	2	3	4	5	6	7	8
1	A	a	I	i	Q	q	Y	y
2	B	b	J	j	R	r	Z	z
3	C	c	K	k	S	s	1	7
4	D	d	L	l	T	t	2	8
5	E	e	M	m	U	u	3	9
6	F	f	N	n	V	v	4	0
7	G	g	O	o	W	w	5	$
8	H	h	P	p	X	x	6	#

Step 7: Find out the position of plain text in the ANeng key table. Take the equilant value of plain text in which the row, column intersect the equilant position of WelcomeToCollege is 75,52,44,32,74,54,52,45,74,31,74,44,44,52,72,52.

Step 7: form a square matrix (S x S >=N) for the key value (the key value contain decimal values)

75	52	44	32
74	54	52	45
74	31	74	44
44	52	72	52

Step 8: Add the matrix A with key value.

75	52	44	32
74	54	52	45
74	31	74	44
44	52	72	52

+

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

=

162	163	155	140
183	121	153	146
185	134	182	145
145	151	156	160

Step 9: Read the message by, column by column using the key value 2431
Apply key 2431

163	121	134	151
140	146	145	160
155	153	182	156
162	183	185	145

Step 10: Find the modulus value of the matrix
Find modulo of 127
163 mod 127 =36

36	121	7	24
13	10	18	33
28	26	55	29
35	56	58	18

Step 11: If the value <32 the add value+32
If PT<32 (x=32)
163 mod 127 =36

36	121	39	56
45	42	40	33
60	58	55	61
35	56	58	40

Step 12: Convert the ASCII code into character value

The encrypted text is: $y'8_*(!<:7=#8:(

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. Fig.3: shows the decryption algorithms.

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: Subtract ANeng table key value with matrix A
Step 5: Reverse shift row transformation
Step 5: Rearrange in to ascending order form A[0] to A[15]matrix.
Step 6: To find the Transpose of Matrix (AT)T = A
Step 7: Stop

Fig.3: Proposed decryption algorithm.

To run the decryrtion algorithm the original plain text WelcomeToCollege is discovered.
Step 1 and 2: The encrypted text is converted into ASCII code values.
The encrypted text is:$y'8_*(!<:7=#8:(

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

163	121	134	151
140	146	145	160
155	153	182	156
162	183	185	145

Step 4: Subtract ANeng table key value with matrix A

162	163	155	140
183	121	153	146
185	134	182	145
45	151	156	160

87	111	111	108
109	67	101	101
111	103	108	101
101	99	84	108

-

=

75	52	44	32
74	54	52	45
74	31	74	44
44	52	72	52

Step 5: Reverse shift row transformation

87	111	111	108
101	109	67	101
108	101	111	103
99	84	108	101

Step 5 and 6: Rearrange in to ascending order form A[0] to A[15]matrix.
: To find the Transpose of Matrix $(A^T)^T = A$

Matrix= A

87	101	108	99
111	109	101	84
111	67	111	108
108	101	103	101

ASCII code value for the plaintext (Decimal Code)
87,101,108,99,111,109,101,84,111,67,111,108,108 ,101,103,101.

The plain text is WelcomeToCollege

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

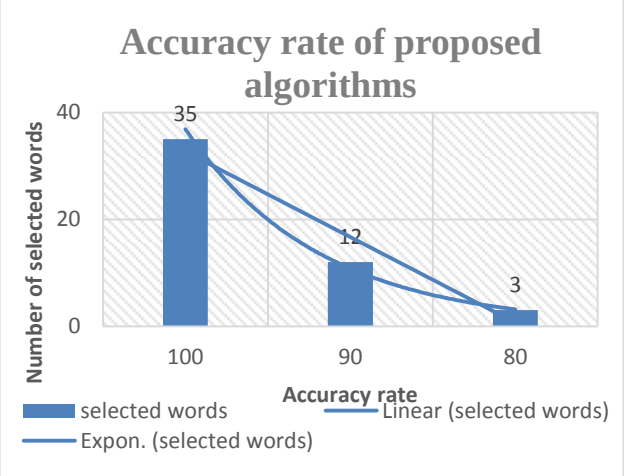
IV. EXPERIMENTAL RESULTS

The proposed algorithm examined by using 50 sample words with different types of characters. In this experiment, out of 50 words 35 words are successfully encrypt and decrypt perfectly (100%). Remaining 15 words, 12 words are occurred single character error and 3 words are occurred three character errors. The accuracy of security is calculated using equation – 1.

$$\text{Accuracy of Security} = \frac{X}{N} X100 \quad \text{----------(1)}$$

X - Number of selected words
N - Total number of words

String(words)	Accuracy (%)		
	100	90	80
50	35	12	3



V. 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. Based on the experimental results, the proposed algorithm performance is good.

VI. REFERENCES

[1]. 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.

[2]. Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based onetime password and automatic blocker protocol", El-Booz et al. EURASIP Journal on Information Security (2016) 2016:13.

[3]. 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

[4]. 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

[5]. 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.

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

[7]. 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.

[8]. 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".

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

[10]. Maragoni Mahendar1, Malipatel Anusha2," Privacy-Preserving Public Auditing for Secure Cloud Storage" IJ of Scientific Research in Computer Science, Engineering and Information Technology Vol. 3, Issue 1, pp.242-246, 2018.