IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 3 (March. 2019), ||S (III) || PP 01-10

Enhancing Data Safety Through Dual Layer Security Protection in Cloud Network

Sudipta Sahana[1], Suchismita Gupta[1], Debabrata Sarddar[2]
[1]*Department of Computer Science and Engineering, JIS College of Engineering, Kalynai*
[2]*Department of Computer Science and Engineering, University of Kalyani, Kalynai*
Corresponding Author: Sudipta Sahana

Abstract: As visualized by the researchers, Cloud Computing is the next-generation architecture of IT Enterprise. Cloud computing relies on shared computing resources rather than having local servers or personal devices to handle applications. Cloud Computing moves the application software and databases to the large data centers, which distinguishes it from the traditional solutions, where the IT services are under proper physical, logical and personnel controls. Security in cloud is the current discussion in the IT world due to the increasing number of breaches and technological attacks. In this paper we focus on providing a dual layer security to the data to be transmitted and stored in cloud storage. The first stage of encryption is provided in the user end and then the data is transmitted via the transmission network in the cloud network. The second stage of encryption is implemented at the server end before storing the data in cloud storage.

Keywords: Cloud Computing, Dual Layer Security, Cloud Data Center, Rail Fence Cipher, Cloud Storage.

Date of Submission: 06-03-2019 Date of acceptance: 25-03-2019

I. INTRODUCTION

Cloud Computing an online based package of computer services where applications, servers, storage are shared to an organization's computer and devices through the network. The National Institute of Stands and Technology (NIST) has defined 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."

Cloud computing offers a number of evident advantages that revolutionized the world of information technology. Experts and researchers understate it as the future of information architecture that would find prominence in large scale applications. It's ability of extend users to access services based on individual requirements with little or minimal intervention that has the immediate effect of mitigating procedural delays, sets apart cloud computing in terms of enterprise computing and network. Further, resources on the Cloud are accessible from almost anywhere with network access.

Besides these, Cloud Computing have some security concerns as well, which could be classified into two broad categories: security issues faced by cloud providers and security issues faced by their customers. Both the providers as well as the consumers must ensure their share of responsibility to safeguard their data. The need for safeguarding arises when an organization elects to store data on the public cloud, its ability to have physical access is lost to the servers hosting its information. This results into risking the sensitive data to the attackers. Sometimes more than one customer's data is stored on one server. This may lead to leaking of data to other customers. All these situations need to be avoided in order to keep the data safe. This could be done by ensuring proper data isolation and logical storage segregation. Proper encryption of data before storing it at the data centers could add up to the security of the data in cloud. Dual Layer Encryption, one at the client end and the other at the data center end provides high security to the data.

II. RELATED WORK

Rajiv Mishra et al. [1] proposed a paper on the need for multiple layers of security in cloud computing for security issues. Various security issues along with the cloud security controls have been discussed.

DebabrataSarddar et al. [2] introduced a paper that focuses n resourceful load balancing coupled with a technique of reducing flooding. An efficient routing with reduced carbon emission is ensured by this system.

Aarti Singh et al. [3] introduced a work that explores various levels of security concerns in the cloud environment. The work also focuses on the mechanisms available for addressing them.

Mahima Joshi et al. [4] implemented an idea that would benefit both customers and service providers by providing several architectures that combine recent and non-standard cryptographic primitives in order to solve the problem of building a secure cloud storage service on the top of a public cloud infrastructure where the customer lacks complete trust on the service provider. It provides the overview of recent advances in cryptography motivated specifically by cloud storage.

Ahmed Albugmi et al. [5] proposed a paper that discusses data security in cloud computing. It includes the study of data in the cloud and its security related aspects. It deals with the details of data protection methods and approaches used in the world to ensure maximum data protection by reducing risks and threats.

Bhavna Makhija et al. [6] proposed an introduction to a cloud computing which in future could be adopted by the governments, manufacturers and academicians. It builds a robust data security between CSP and User. Third Party Auditor, data security and security algorithms of different papers are introduced to the technology of cloud computing.

Rajesh Bose et al. [7] introduced an idea whose objective is to simplifying the process of data storage as well as data retrieval on cloud network. This provides optimum access over varying internet connection speeds. Constant calculations of the closest cloud network is been relied upon, which depends on factors such as available bandwidth, latency history, storage space level, and constant geographical location.

K.Govinda et al. [8] proposed an idea that implements digital signature method to protect the privacy and integrity of outsourced data in the cloud environment.

John Harauz et al. [9] introduced an idea that describes the Security Content automation protocol (SCAP).Benefits provided with latest cloud computing paradigm with reference to the latest report released by NIST is also added. It gives insight as to what SCAP is trying to do. It states that many tools for system security, such as patch management and vulnerability management software, use proprietary formats,nomenclatures, measurements, terminology, and content.

Balachandra Reddy Kandukuri et.al [10] proposed an idea that focuses on some of the security issues that have to be included in Service Level Agreement (SLA). SLA is a document which defines the relationship between service provider and the recipient, typical Service level agreement contents includes Definition of services, Performance management, Problem Management, Security, Disaster recovery, proper termination of transaction also they have stated a methodology to standardize SLA's.

III. PROPOSED WORK

Security is the major concern now a day both in shard channel and in cloud data centers. Intruders always try to hack the cloud server installed in data centers. In our proposed approach we have focused on dual layer security for the data. Before sending the data to the data center entire message will be encrypted at client side, that ensure cipher text communication from client to data center end. After receiving the cipher text message at data center end entire message goes through a 2nd layer encryption which makes the original message secure double time and then it will be stored at data center storage. Although the intruder is able to hack the server still he / she will be unable to reveal the original text.

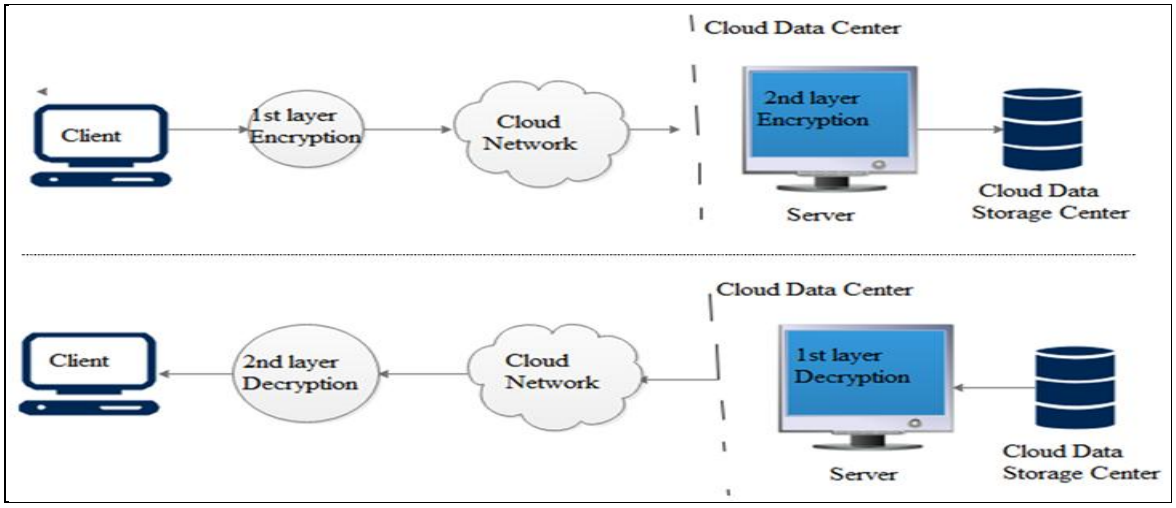

Fig. 1- Network Diagram of Dual Layer Encryption and Decryption

Security is the major concern now a day both in shard channel and in cloud data centers. Intruders always try to hack the cloud server installed in data centers. In our proposed approach we have focused on dual layer security for the data. Before sending the data to the data center entire message will be encrypted at client

side, that ensure cipher text communication from client to data center end. After receiving the cipher text message at data center end entire message goes through a 2nd layer encryption which makes the original message secure double time and then it will be stored at data center storage. Although the intruder is able to hack the server still he / she will be unable to reveal the original text.

1stLayer Encryption at Client end:

1. Input a plain text from user.
2. Each string from the input is substituted by their corresponding octal values.
3. The octal values are then converted to their corresponding binary 8-bit representation.
4. Group binary representation of eight consecutive characters in order to form an 8*8 matrix. If required compensate the matrix with padding with zeros.
5. Divide each row of the matrix into two halves forming Left Half (LF) and Right Half (RF) of four bits each. Perform bit-wise XOR operation between LF and RF and replace the bits of the LF by the resultant XOR operation values. Thus, obtain a new matrix.
6. Substitute each row of the matrix by their corresponding decimal values. Write them serially.
7. Replace each decimal value to their corresponding ASCII characters.
8. A first layer cipher text is thus formed and transmitted through the transmission media.

After the implementation of the first layer encryption the cipher text is transmitted through the transmission media from the client end to the data center end.

2nd Layer Encryption at Data Center end:

1. Process the cipher text received at data center end by substituting each character from the received cipher text with their corresponding ASCII values.
2. Perform the following operation on each character:

Ci = Pi mod 26

Where, Ci is the resultant numeric value

Pi is the ASCII value obtained from Step 1

Store the quotient in an array named Quotient [ ], in the data centre.

3. Substitute the resultant numeric value to their corresponding alphabets.
4. Perform rail fence cipher over the alphabets obtained from above step.
5. Store the resultant cipher text and the Quotient array in the index in the data center.

The final cipher text is thus stored securely in the data center of the cloud.

When the user needs to fetch his/her data from the cloud, the cipher text and the quotient array stored at the data center are searched in the index table at the data center and are worked upon by the first layer of decryption.

1st Layer Decryption at Data Center end:

1. Perform Backtracking Rail Fence Cipher with thecipher text fetched from the data center end.
2. Substitute the resultant alphabets to their corresponding numeric values.
3. Fetch the 8*8 matrices from the allocated address at the data center and with each quotient value of the Quotient array perform the following calculation:

Pi = Qi * 26 + Ci

Where, Pi is the resultant numeric value (ASCII value)

Qi is the quotient value from the stored array

Ci is the Numeric value obtained from Step 2

4. Substitute each ASCII value obtained from the above step with their corresponding ASCII characters.
5. A cipher text is thus formed and is transmitted through the transmission media.

The cipher text obtained for the 1st layer decryption is transmitted from the data center end to the user end using the cloud network.

2nd Layer Decryption at Client end:

1. Fetch the transmitted cipher text from the transmission media.
2. Replace each character by their corresponding ASCII values.
3. Substitute each ASCII value with their corresponding 8-bit binary representation.
4. Group binary representation of eight consecutive characters in order to form an 8*8 matrix.
5. Divide each row of the matrix into two halves forming LF and RF of four bits each. Perform bit-wise XOR operation between LF and RF and replace the bits of the LF by the resultant XOR operation values. Thus, obtain a new matrix.
6. Convert each row of the matrix to their corresponding Octal values. Ignore the padding part.
7. Substitute each octal value with their corresponding ASCII character values.

8. Obtain the plain text.

Thus, the user receives the data he/she has stored in the cloud data center.

IV. METHODOLOGY

1st Layer Encryption at client end:

1. Input plain text: Hello World
2. Octal values for each character:

Character	Octal Value		Character	Octal Value
H	110		W	127
e	145		o	157
l	154		r	162
l	154		l	154
o	157		d	144
space	40			

3. Binary 8-bit representation of octal values:

Octal Value	Binary Representation		Octal Value	Binary Representation
110	01101110		127	11111111
145	10010001		157	10011101
154	10011010		162	10100010
154	10011010		154	10011010
157	10011101		144	10010000
40	00101000			

4. 8*8 matrix formation with padding:

0	1	1	0	1	1	1	0
1	0	0	1	0	0	0	1
1	0	0	1	1	0	1	0
1	0	0	1	1	0	1	0
1	0	0	1	1	1	0	1
0	0	1	0	1	0	0	0
1	1	1	1	1	1	1	1
1	0	0	1	1	1	0	1

1	0	1	0	0	0	1	0
1	0	0	1	1	0	1	0
1	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

5. Resultant matrix after XOR operation between LF and RF:

1	0	0	0	1	1	1	0
1	0	0	0	0	0	0	1
0	0	1	1	1	0	1	0
0	0	1	1	1	0	1	0
0	1	0	0	1	1	0	1
1	0	1	0	1	0	0	0
0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	1

1	0	0	0	0	0	1	0
0	0	1	1	1	0	1	0
1	0	0	1	0	0	0	0

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

6. Binary to Decimal Values:

Binary Representation	Decimal Value		Binary Representation	Decimal Value
10001110	142		10000010	130
10000001	129		00111010	58
00111010	58		10010000	144
00111010	58		00000000	0
01001101	77		00000000	0
10101000	168		00000000	0
00001111	15		00000000	0
01001101	77		00000000	0

7. ASCII characters of Decimal values:

Decimal Value	ASCII Character		Decimal Value	ASCII Character
142	**Ä**		130	**é**
129	**ü**		58	:
58	:		144	**É**
58	:		0	NULL
77	M		0	NULL
168	**¿**		0	NULL
15	SI		0	NULL
77	M		0	NULL

8. Resultant 1st layer cipher text to be transmitted:

Ä ü : : M **¿** SI M **é** : **É** NULL NULLNULLNULLNULL

After the implementation of the first layer encryption the cipher text is transmitted through the transmission media from the client end to the data center end.

2nd Layer Encryption at Data Center end:

1. ASCII values of the characters of the cipher text obtained:

Character	ASCII Value		Character	ASCII Value
Ä	142		**é**	130
ü	129		:	58
:	58		**É**	144
:	58		NULL	0
M	77		NULL	0
¿	168		NULL	0
SI	15		NULL	0
M	77		NULL	0

2. Performing the following operation on each character:

Ci = Pi mod 26

Where, Ci is the resultant numeric value

Pi is the ASCII value obtained from Step 1

The quotient, Quotient[ ] = {5,4,2,2,3,6,0,3,5,2,5,0,0,0,0,0}, is stored in the data center.

Pi	Ci		Pi	Ci
142	12		130	5
129	25		58	2
58	6		144	5
58	6		0	0
77	25		0	0
168	12		0	0
15	15		0	0
77	25		0	0

3. Alphabets corresponding to the Numeric Values:

Numeric Value	Alphabet		Numeric Value	Alphabet
12	M		5	A
25	Z		2	G
6	G		5	O
6	G		0	A
25	Z		0	A
12	M		0	A
15	P		0	A
25	Z		0	A

4. Rail fence cipher over the alphabets obtained from above step:

M	G	Z	P	A	O	A	A
Z	G	M	Z	G	A	A	A

5. Resultant cipher text is stored in the data center:

M G Z P A O A A Z G M Z G A AA

The final cipher text is thus stored securely in the data center of the cloud.

When the user needs to fetch his/her data from the cloud, the cipher text and the quotient matrix stored at the data center are worked upon by the first layer of decryption.

1st Layer Decryption at Data Center end:

1. Backtracking Rail Fence Cipher with the cipher text fetched from the data center end:

M		G		Z		P		A		O		A		A	
	Z		G		M		Z		G		A		A		A

2. Numeric values of the Alphabets:

Alphabet	Numeric Value		Alphabet	Numeric Value
M	12		A	5
Z	25		G	2
G	6		O	5
G	6		A	0
Z	25		A	0
M	12		A	0
P	15		A	0
Z	25		A	0

3. The quotient array, Quotient [ ], is fethed from the allocated address at the data center and with each quotient value of the array the following calculation is performed:

$Pi = Qi * 26 + Ci$

Where, Pi is the resultant numeric value (ASCII value)

Qi is the quotient value from the stored array

Ci is the Numeric value obtained from Step 2

Qi	Ci	Pi		Qi	Ci	Pi
5	12	142		5	0	130
4	25	129		2	6	58
2	6	58		5	14	144
2	6	58		0	0	0
3	25	77		0	0	0
6	12	168		0	0	0
0	15	15		0	0	0
3	25	77		0	0	0

4. ASCII characters corresponding to the ASCII values:

ASCII Value	Character		ASCII Value	Character
142	Ä		130	é
129	ü		58	:
58	:		144	É
58	:		0	NULL
77	M		0	NULL
168	¿		0	NULL
15	SI		0	NULL
77	M		0	NULL

5. The cipher text is thus formed and transmitted through the transmission media:
Ä ü : : M **¿** SI M **é** : **É** NULL NULLNULLNULLNULL
The cipher text obtained for the 1st layer decryption is transmitted from the data center end to the user end using the cloud network.

2nd Layer Decryption at user end:

1. ASCII values of the characters of the cipher text obtained from the transmission medium.

Character	ASCII Value		Character	ASCII Value
Ä	142		é	130
ü	129		:	58
:	58		É	144
:	58		NULL	0
M	77		NULL	0
¿	168		NULL	0
SI	15		NULL	0
M	77		NULL	0

2. 8-bit binary representation of the ASCII values:

Decimal Value	Binary Representation		Decimal Value	Binary Representation
142	10001110		130	10000010
129	10000001		58	00111010
58	00111010		144	10010000
58	00111010		0	00000000
77	01001101		0	00000000
168	10101000		0	00000000
15	00001111		0	00000000
77	01001101		0	00000000

3. 8*8 matrix formation:

1	0	0	0	1	1	1	0
1	0	0	0	0	0	0	1
0	0	1	1	1	0	1	0
0	0	1	1	1	0	1	0
0	1	0	0	1	1	0	1
1	0	1	0	1	0	0	0
0	0	0	0	1	1	1	1
0	1	0	0	1	1	0	1

1	0	0	0	0	0	1	0
0	0	1	1	1	0	1	0
1	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

4. Resultant matrix obtained from XOR operation of LF and RF:

0	1	1	0	1	1	1	0
1	0	0	1	0	0	0	1
1	0	0	1	1	0	1	0
1	0	0	1	1	0	1	0
1	0	0	1	1	1	0	1
0	0	1	0	1	0	0	0
1	1	1	1	1	1	1	1
1	0	0	1	1	1	0	1

1	0	1	0	0	0	1	0
1	0	0	1	1	0	1	0
1	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

5. Octal values of each row of the matrix (Ignoring the padding):

Binary Representation	**Octal Value**		**Binary Representation**	**Octal Value**
01101110	110		11111111	127
10010001	145		10011101	157
10011010	154		10100010	162
10011010	154		10011010	154
10011101	157		10010000	144
00101000	40			

6. ASCII characters corresponding to the octal values:

Octal Value	**Character**		**Octal Value**	**Character**
110	H		127	W
145	e		157	o
154	l		162	r
154	l		154	l
157	o		144	d
40	space			

7. The resultant plain text:
Hello World
Thus, the user receives the data stored in the cloud data center.

V. RESULT ANALYSIS

The proposed idea is to provide a Dual Layer Encryption to the data in the cloud in order to safeguard the data and thus, make cloud more secure. Several literature surveys reveal that data in cloud highly vulnerable to threats through network sources. Besides providing the security to data at the data centers of the cloud our proposed work provides security to the data while traveling from the client to the data center as well by providing encryption to the data at the client end. In comparison to the traditional process, this system provides more effective security to the data. From the following Fig. 2, we can see that time required is almost same for the input character string that shows the efficiency for our proposed work.

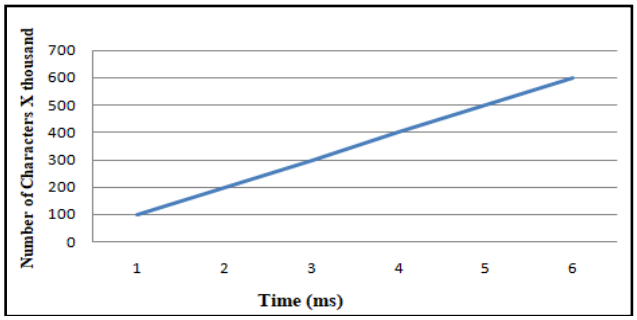

Fig. 2 – Number of Characters vs. Time

VI. CONCLUSION

Cloud Computing being the soul of the Technological world needs its data to be safeguarded by providing proper protection. Besides isolating its data and providing proper logical storage segregation, encrypting the data is a fruitful approach towards data security. In our proposed work we have implemented a dual layer encryption on the data from the user, one at the client end and other at the data center end.After the 1st Layer Encryption at the client end the data is safe to travel through the transmission media. Further, at the data center the 2nd Layer Encryption provides deeper encryption. The use of the XOR operations, Mode operation and Rail Fence Cipher technique along with substations makes the whole encryption strong. Thus, this Dual Layer Encryption system succeeds in safeguarding the data in cloud network.

REFERENCES

[1]. Rajiv Mishra, Meenaxi Kumari, "Need of Multi-Layer Security in Cloud Computing for on Demand Network Access", International Journal of Computer Science and Mobile Computing, A Monthly Journal of Computer Science and Information Technology, IJCSMC, Vol. 4, Issue. 6, June 2015, pg.398 – 404, ISSN 2320–088X.

[2]. Debabrata Sarddar, Rajesh Bose,Sudipta Sahana, "An Enhanced Cloud Network Load Balancing Approach Using Hierarchical Search Optimization Technique", International Journal of Hybrid Information Technology Vol.8, No.3 (2015), pp.9-20.

[3]. Aarti Singh, Manisha Malhotra, "Security Cconcerns at Various Levels of Cloud Computing Paradigm: A Review", International Journal of Computer Networks and Applications, Volume 2, Issue 2, March – April (2015).

[4]. Mahima Joshi, Yudhveer Singh Moudgil, "Secure Cloud Storage", International Journal of Computer Science & Communication Networks,Vol 1(2), 171-175, ISSN:2249-5789.

[5]. Ahmed Albugmi, Madini O. Alasssafi, "Data Security in Cloud Computing", Fifth International Conference on Future Generation Communication Technologies (FGCT 2016), DOI:10.1109/FGCT.2016.7605062.

[6]. Bhavna Makhija, VinitKumar Gupta, Indrajit Rajput, "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013, ISSN: 2277 128X.

[7]. Rajesh Bose, SudiptaSahana, Debabrata Sarddar, "An Efficient Model of Distribution and Storage of Big Data across Cloud-based Nodes using Billboard Manager", International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015, ISSN 2229-5518.

[8]. K.Govinda, V.Gurunathaprasad, H.Sathishkumar, "Third Party Auditing For Secure Data Storage In Cloud Through Digital Signature Using RSA", International Journal Of Advanced Scientific and Technical Research (ISSUE 2, VOLUME 4- August 2012), ISSN 2249-9954.
[9]. John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing",2009 IEEE CO Published by the IEEE Computer and Reliability Societies.
[10]. Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, "Cloud security Issues", 978-0-7695-38112/09 2009, IEEE computer society.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Sudipta Sahana. "Enhancing Data Safety Through Dual Layer Security Protection in Cloud Network." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 03, 2019, pp. 01-10.