International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174 Volume 7, Number 7 (2014), pp. 669-675

http://www.irphouse.com

A Hybrid Approach and Implementation of a New Encryption Algorithm for Data Security in Cloud Computing

Md Asif Mushtaque[1]' Harsh Dhiman[2], Shahnawaz Hussain[3]

[1,2,3]M.Tech (CS&E), Galgotias University, U.P., India

Abstract

Cloud Computing offers dynamic allocation of resources for guaranteed and reliable services. Users store their data on a single virtual server, when user wants to access any data that data might be changed or modified by unauthorized people for malicious purpose because user's do not have direct control of data So security is a big challenge for cloud computing and it is necessary to increase the security level in the cloud where the user should free from modification of data. We proposed a new encryption algorithm (ASIF Encryption Algorithm) for data security in cloud computing. This Algorithm performs multiple rounds based on the length of the key. The main feature of this algorithm is that it generates a random key in each round and also selects the key randomly in each round to encrypt the data. There are three main advantages of this model (i) it reduces the size of data and requires less storage space taken by existing encryption techniques (ii) reduce the congestion between server and user by fast transmission and (iii) provides better security because of random key selection. Many authors have given their ideas on data security in cloud but no one gives the full control to the user. This approach gives the full control to the user on their data and they can protect their data from unauthorized people. In Cloud Computing several organizations store their data on a single server so there is a very huge amount of data stored on a server. This approach is a hybrid approach and uses a data compression method to reduce the size of original data then encrypt data using ASIF Encryption Algorithm. So, this model is beneficial for users as well as a service provider.

Keywords: Cloud Computing, ASIF Algorithm, Encryption, Compression, Cloud Security, Data Privacy, Data Security, Integrity, Confidentiality, Reliability.

1. INTRODUCTION

Cloud computing is a type of computing which provides the facility to use resources available on cloud system, in other word we can say that it is a model where resources are retrieved through network, it allows user to use technology enabled services through the internet [1, 8]. Cloud computing is an internet based service where the user can easily use storage, services without knowing how it is actually working internally. Cloud computing is a collection of virtual machines in which user only uses the services provided by the virtual machines they don't have a control on virtual machines. In cloud computing several organizations store their data on a single virtual server sometimes multiple operating systems are executed on a single virtual server, in this case there is chances of threat from other machine. So there is a need of high level security especially in public cloud system.

There are some main characteristics of cloud computing:

- Location Independence: it means location of device is not necessary for the user where it is located; the user only uses the services through internet. They don't need to know what kind of device is used by user or cloud; they only know how to use it [8].
- Multitenancy: it means a single piece of resource is used by multiple users. A single user is known as the tenant. So cloud provides a facility to use a single instance of resource across a large pool of users.
- Reliability: uses multiple redundant (copied) sites which make it well suitable for business and disaster recovery.
- Measured service: it means cloud automatically measures about services, resources used by users and providing transparency from users.
- Scalability: modification of services quickly according to user's requirement without any problem in existing services.
- Security: due to centralization of data security is the main characteristics of data. It provides better security but need to increase the security level [8].
- On demand self service: in which user can use the services according to their need without interference of the service provider.

2. RELATED WORK

In [1], the authors have proposed a model and where they discussed on the multi level sign agreement from a service provider for data security but there would be some problem. If a service provider sign on the agreement and data is accessed by hacker then service provider would be responsible, according to [1] data can be protected only from service provider not from outside hackers. So, this model is not very effective for user and service provider. In [2], the authors used a HMAC scheme to encrypt data and used two times encryption at the time uploading a file and distribution of file. Uses of two times encryption means it will take double time which increases the time complexity. Many authors have given their ideas some of them uses existing method and some authors have proposed their new ideas.

3. HYBRID MODEL

Figure1 shows the complete structure of the proposed model, in this model when the user is allowed to upload/download file to or from cloud server, if the user wants to upload their data then that data will be compressed first then encryption is performed. In this model I am compressing data by using existing method Arithmetic coding and to encrypt I proposed own encryption algorithm (ASIF Encryption Algorithm) when we compress data then it'll reduce size up to 20-25%. The advantages of using compression technique is that after reducing the size of data it'll take 20-25% less storage space of cloud server, this technique saves the space of server another advantage is if we reduce the size then we can transfer data within less time in comparison to the original file because channel has the limited bandwidth. For example: suppose the channel capacity is to transfer data 1MBPS, the size of the original file is 10MB then this file would be transferred in 10 seconds. After using this model, the size of the original file is 10MB, size of the compressed file is 7MB, and now this file would be transferred in 7 seconds. When file would be transferred within 7 second then it reduces the congestion on channel or between cloud server and user because cloud server supports multitenancy feature where a single resource is used by multiple users. In existing method all encryption techniques require same of maximum storage space for encrypted data in comparison to the original data. This model keeps more effect on larger file where it can reduce maximum size. If we use both approach then security becomes high then service provider can provide reliable service with high security.

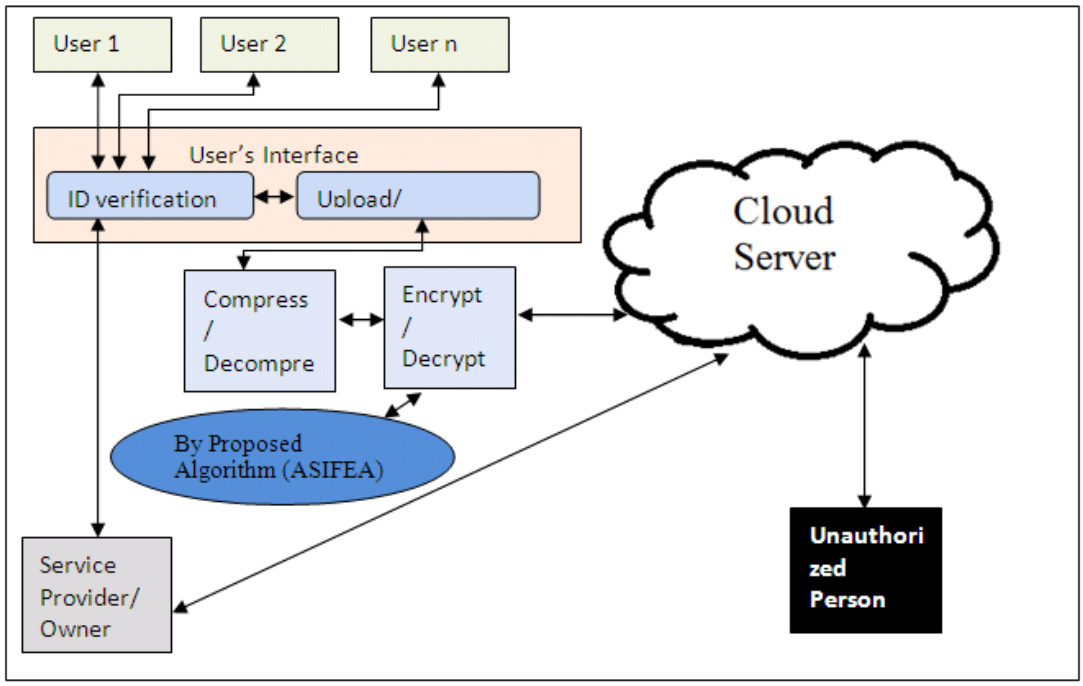

Figure1. Structure of Hybrid Model

3.1.PROPOSED ALGORITHM: ASIF ENCRYPTION ALGORITHM (ASIFEA)

❖ **Algorithm for Random Key Generation**:

1. Select key as key1 and initialize Round as 0.
2. Find the length of the key L.
3. Apply reverse function on key1 and store in rev_key.
4. Calculate random_number= ∑ASCII * pos^i. Where pos is the position of character in key1.
5. Find mod of random_number M= Mod(random_number)
6. Apply matrix on key1 and rev_key
7. Add 'M' to each bit of matrix _key1 and matrix_rev_key.
8. Perform Exclusive-Or operation between matrix_key1 and matrix_rev_key.
9. Obtained new matrix as new_matrix.
10. Convert each bit of new_matrix into its equivalent character to obtain new key.

❖ **Algorithm for Random Key Selection**:

1. Read both keys as key1 and key2
2. Find LSB of both keys as L1 and L2.
3. If L1= = L2
   Call encryption function, Encrypt (key1), Round=Round+1
   Else
   Call encryption function, Encrypt (key2), Round=Round+1
4. Stop.

Perform random key generation and random key selection operation till Round<= l/2.

For Example: Let key1= ahc5i90w4 'and' Rev_key=4w09i5cha

L=9

Random_value= ∑ASCII * pos^i(key1)

97*1+104*2+99*3+53*4+105*5+57*6+48*7+119*8+52*9= 3437

M= Mod (random_value, L) = 8

Now representing key1 and rev_key in matrix form

Step (1) Apply_matrix

a	h	c
5	i	9
0	w	4

97	104	99
53	105	57
48	119	52

Mat_key1

Step (2) Reverse_Matrix

4	w	0
9	i	5
c	h	a

52	119	48
57	105	53
99	104	97

Rev_Mat_Key

Step (3) Add_ModValue to mat_key1

105	112	107
61	113	65
56	127	60

Step (4) Xor with mat_rev_key

105	112	107
61	113	65
56	127	60

⊕

52	119	48
57	105	53
99	104	97

Step (5) New_matrix after Xoring

93	7	91
4	24	116
91	23	93

Step (6) New_Key as key2

]	BEL	[
EOT	CAN	t
[	ETB	]

Now calling Key_Selection Function where

key1=

a	h	c	5	i	9	0	w	4

Key2=

]	BEL	]	EOT	CAN	t	[	ETB	]

Step (1) read key1 and key2

Step (2) Find the Least Significant Bit (LSB) of both key.

L1= LSB (key1) = 0, L2= LSB (key2) = 1

Step (3) if L1= =L2

Cipher = plaintext $\oplus$ key1, Round = Round+1

Else

Cipher = plaintext $\oplus$ key2, Round = Round+1

Step (4) perform random_key_generation and key_selection operation until round less than or equall to L/2.

Table 1: Encryption Process of ASIF- Encryption Algorithm (ASIFEA)

Rounds	**Key1**	**Key2**	**Plain Text/ Ciphertext**	**Selected Key**	**Cipher text**	
Round 1	A1sd5jy7v	n/oay7z33	Galgotias	n/oay7z33	aj&i(%l=y	C1
Round 2	n/oay7z33	l8w$]w01a	aj&i(%l=y	n/oay7z33	ol(q@;f-s	C2
Round 3	l8w$]w01a	S4)hb+il”	ol(q@;f-s	S4)hb+il”	sA[yN*3qc	C3
Round 4	S4)hb+il”	D5e/ 8^t!	sA[yN*3qc	D5e/ 8^t!	Pl\#f7,(h	Final Ciphertext

Table 1 shows that how encryption is done in propose algorithm. The above encryption performed by using key length of 9 bytes (72 bits) so it performs total 4 processing rounds. In Round 1 there are two different keys but after comparison of LSB of key1 and key2, algorithm decided to use key2 for encryption where C1 is the cipher text obtains from Round 1 and in round to C1 is used as an input. After processing of Round 4 we obtain the final ciphertext. In each round we can see that the changing in keys and the selection of key. So it is not possible to predict the next key and which key is used for encryption process. The main advantage of this algorithm is that the same algorithm is used for decryption. The existing algorithm decrypt data by performing reverse process of encryption or change the key into reverse order then decrypt but proposed algorithm provides the facility to use same

process, it does not require key in reverse order. This algorithm supports key size of 4 bytes, 9bytes, 16bytes and so on but the key length should be square of any number. The number of processing round is depend on the key if the key size is 4 bytes it performs 2 processing rounds, if key size is 9 bytes it performs 4 processing round means Rounds = length of the key/2.

4. EXPERIMENTAL RESULT COMPARISON TABLE

Table2. Experimental Result of ASIFEA

Sr. No	Original File Size	Ciphertext Size	Decrypted File Size
1	130 Kb	130 KB	130 KB
2	240 KB	240 KB	240 KB
3	350 KB	350 KB	350 KB
4	970 KB	970 KB	970 KB

Table 3. Comparison of ASIFEA with most common Symmetric key Encryption Algorithms.

Algorithms	Plain text	After Encryption	After Decryption
AES	240 KB	847KB	240 KB
TDES	240 KB	614KB	240 KB
Blowfish	240 KB	955KB	240 KB
AMEA (Proposed Algorithm)	240 KB	240 KB	240 KB

5. CONCLUSION AND FUTURE WORK

We used ASIF Encryption Algorithm on different files of different size but after result from Table2. We found that this algorithm takes same space for their cipher text in comparison to plain text, while in Table3 we compare our proposed algorithm with some most common encryption algorithm based on space complexity we analyze that all these existing algorithms require extra space for encrypted data but ASIFEA does not require any extra space. After experiment result of proposed algorithm and according to [4] we found that ASIF Encryption Algorithm is best because it provides better security and reduce space complexity in comparison to related algorithms. ASIF Encryption Algorithm would be more beneficial for Cloud computing for data security and control the congestion between users and sever because a single server is used by multiple users. The most important feature of this encryption algorithm is that it is impossible to crack this algorithm without knowledge of original key value because the internal key generation function is based on key entered by user. This paper also presents the hybrid model for cloud in this model two different techniques are used compression and encryption. For compression I used the existing method and to encrypt we used our own encryption algorithm. We know that cloud server contains

very huge amount of data and multiple user accesses a cloud server at the same time so this hybrid model reduce the size of data that saves the storage space of cloud server and increase throughput of cloud computing. Finally after all experiment we found that ASIF Encryption Algorithm provides better security.

REFRENCES

[1] Ashutosh Satapathy, J. Chandrakant Badajena and Chinmayee Rout," *A Secure Model and Algorithms for Cloud Computing Based on Multicloud Service Providers*", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 12, December – 2013.

[2] G. Rahul Reddy and N. J. Subashini, "*Secure Storage Services and Erasure Code Implementation in Cloud Servers*", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 1, January – 2014.

[3] Md Asif Mushtaque, H, Dhiman, S. Hussain and S. Maheshwari, "*Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm: Based on Space Complexity*", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[4] http://en.wikipedia.org/wiki/Disk_encryption_theory accessed on 24th April 2014.

[5] Abhishek Patel and Mayank Kumar, "*A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

[6] Kangchan Lee, "*Security Threats in Cloud Computing Environments*", International Journal of Security and Its Applications, Vol. 6, No. 4, October, 2012.

[7] Rohit Maheshwari and Sunil Pathak, "*A Proposed Secure Framework for Safe Data Transmission in Private Cloud*", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-1, Issue-1, April 2012.

[8] http://en.wikipedia.org/wiki/Cloud_computing accessed on 25th April 2014.

[9] Md Asif Mushtaque, "*Comparative Analysis on Different parameters of Encryption Algorithms for Information Security*", International Journal of Computer Sciences and Engineering, Volume-02, Issue-04, Page No (76-82), Apr -2014.

[10] Md Asif Mushtaque and Mr. Khushal Singh, "*Feasibility Evaluation of Symmetric Key Encryption Techniques for Wireless Channel and Disk Storage*", International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol. 2 Issue V, May 2014.