International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.213-220
http://dx.doi.org/10.14257/ijgdc.2014.7.3.22

A New Innovation on User's level Security for Storage Data in Cloud Computing

Dr. Ritu Sindhu[1] and Md Asif Mushtaque[2]

[1]Assistant Professor, Galgotias University, U.P., India
[2]School of Computing Science and Engineering,
Galgotias University, U.P., India
[1]ritu.sindhu@galgotiasuniversity.edu.in, [2]asifmushtaque000@gmail.com

Abstract

In Cloud Computing data security as well as load balancing of cloud server is very important and most challenging issues. Cloud reduces cost by providing on demand access of resources, it provides guaranteed, reliable services and dynamic allocation of resources. In cloud a single server stores very huge amount of data so there is need to balance load and provide fast transmission on cloud. Many users store their information on a single server, so there are chances of threats by unauthorized user. As we know on cloud we don't have control over our data so security is a very important and challenging issue for cloud. If any algorithm provides fast transmission between user and server then there would be minimum chances for congestion and the data spend minimum time on transmission channel so it will give minimum time to attack on their data. In this paper, I proposed an ides and try to implement an algorithm through which cloud service provider can give the control to user itself. This algorithm uses a key and that key should be unknown from unauthorized person, the key may be user's password or any secret information then this algorithm will give control to user and provide better security for user's data where user would be free from authentication, correctness integrity or confidentiality. It is very important to .give control on user's hand for reliability of services.

Keywords: *Data Security, Cloud Computing, Cloud Security, Load Balancing, Integrity.*

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 [10, 11]. 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 [11].

ISSN: 2005-4262 IJGDC

- 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.
- 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 [10], 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 [10] 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 [12], 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. Secure Model

In this Section I discussed on proposed model how they would be beneficial for users and service provider.

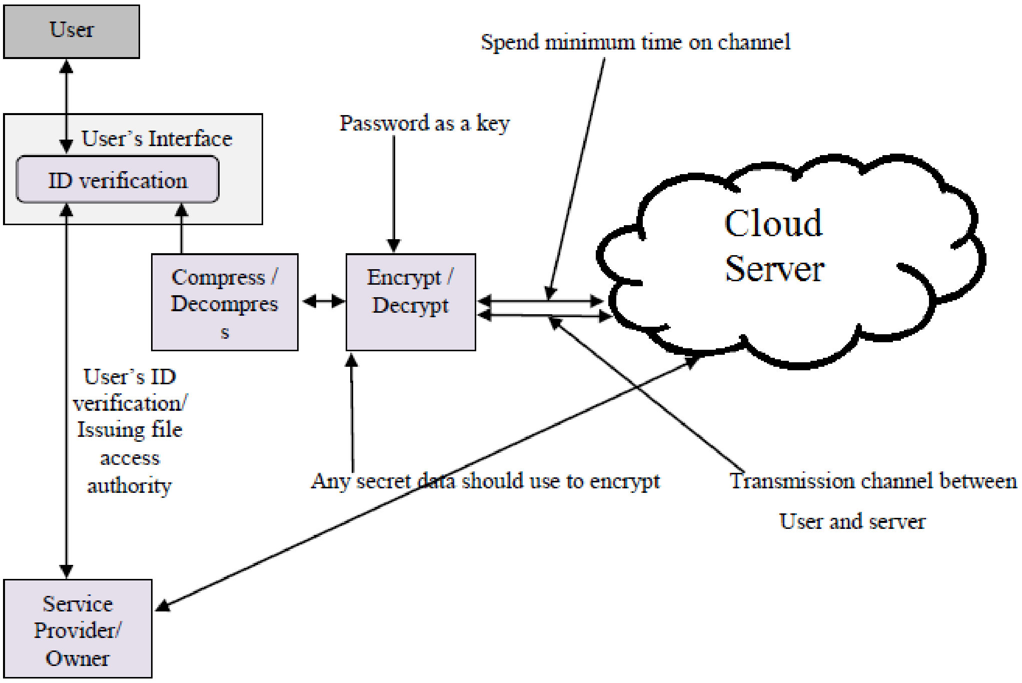

User
User's Interface
ID verification
Compress / Decompres s
Encrypt / Decrypt
Password as a key
Spend minimum time on channel
Cloud Server
User's ID verification/ Issuing file access authority
Any secret data should use to encrypt
Transmission channel between User and server
Service Provider/ Owner

Figure 1. Structure of Proposed Model

Figure 1 shows the complete structure of the secure 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. The encryption technique uses two different keys and to provide better security and give full control to user the key should be user's password or any secret information which is completely hidden from outside users. In this model I am compressing data by using existing method Arithmetic coding and to encrypt I used own encryption algorithm. The main objective of compression is that the data should be spending their minimum time on communication channel. The encryption technique also provides minimum space complexity so when we compress data both techniques (compression and encryption) then it'll reduce size up to 30-35% comparison to existing technique. For example: suppose the channel capacity is to transfer data 500 KBPS, the size of the original file is 2000KB then this file would be 4 seconds on transmission channel and will give 4 seconds to attacker to hack their data. After using this model, the size of the original file is 2000KB, size of the compressed file is 1200 KB, and now this file would 2-3 seconds on transmission channel, so it'll give 2-3 seconds to hack. 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.

➢ Algorithm

This is an encryption algorithm performed on the user side, when users are allowed to access the services of cloud the encryption algorithm will performed by clicking on upload or download button. The secret key should be entered by the user. In the existing encryption algorithm we use a reverse process of encryption to decrypt the file, the key feature of this Algorithm is that there is no need to implement/design a decryption algorithm it decrypts the data by the same process. This algorithm performs a variable number of rounds depend on the key length and in each round this algorithm generates a random key. It is impossible to predict the random key in each round so this algorithm provides a high security level. There are no any limitations of key length but the key size should be square of any number.

Encryption Algorithm:

```
Step 1: read file example.txt
Step 2: read two different keys of equal length (key1 and key2)
Step 3: find l = length of key1
Step 4: key1= {key1+ rand(l)} x key2
Step 5: initialize R=0 where R is the number of rounds
Step 6: rand_key_generation (key1)
        • Reverse kry1 and store as RevOfKey1
        • Convert each character into its ASCII value
        • Sum=  ∑ASCII * P. Where P is the position of character in key1.
        • Calculate mod (sum, l)
        • Arrange key1and RevOfKey1  into matrix form
        • Add mod value with each character in key1 matrix.
        • N1w key1⊕    RevOfKey1
        • Obtain NewKey
```

Step 7: Now Perform Exclusive-Or operation with example.txt and NewKey.

- Ciphertext= example.tx$\oplus$ NewKey

Step 8: now initialize key1= NewKey and R= R+1.

Step 9: Repeat step 6, 7 & 8 until R<= Length of the key

Step 10: Stop.

Decryption is the same process of encryption.

Example: Suppose key1= aw23e45t6 and key2= fd34eft56 then key1= key1 + rand(l) x key2, where rand() is the random function.

Now, Key1= aszxwdefy

L=9

RevOfKey1= yfdewxzsa

a=97, s=115, z=122, x=120, w=119, d=100, e=101, f=102, y=121.

Sum= 97*1+115*2+122*3+120*4+119*5+100*6+101*7+102*8+121*9= 4980

mod= (4980, 9)= 3

a	s	z
x	w	d
e	f	y

97	115	122
120	119	100
101	102	121

Key1 _matrix

y	f	e
d	w	x
z	s	a

122	102	101
100	119	120
122	115	97

RevOfKey1_matrix

100	118	125
123	122	103
104	105	124

After adding mod value to key1_matrix

100	118	125
123	122	103
104	105	124

$\oplus$

122	102	101
100	119	120
122	115	97

Xoring between key1matrix after add mod value and RevOfKey1_matrix

30	16	24
31	13	31
18	26	29

ASCII value of key1= 97, 115, 122, 120, 119, 100, 101, 102, 121.

ASCII of newkey = 30, 16, 24, 31, 13, 31, 18, 26, 29.

The character for the ASCII value of newkey is not available on keyboard. These are the reserved notification symbol for system so it is impossible to crack the new key. This process is performed in each round of this algorithm so key1 and newkey would be change in each round.

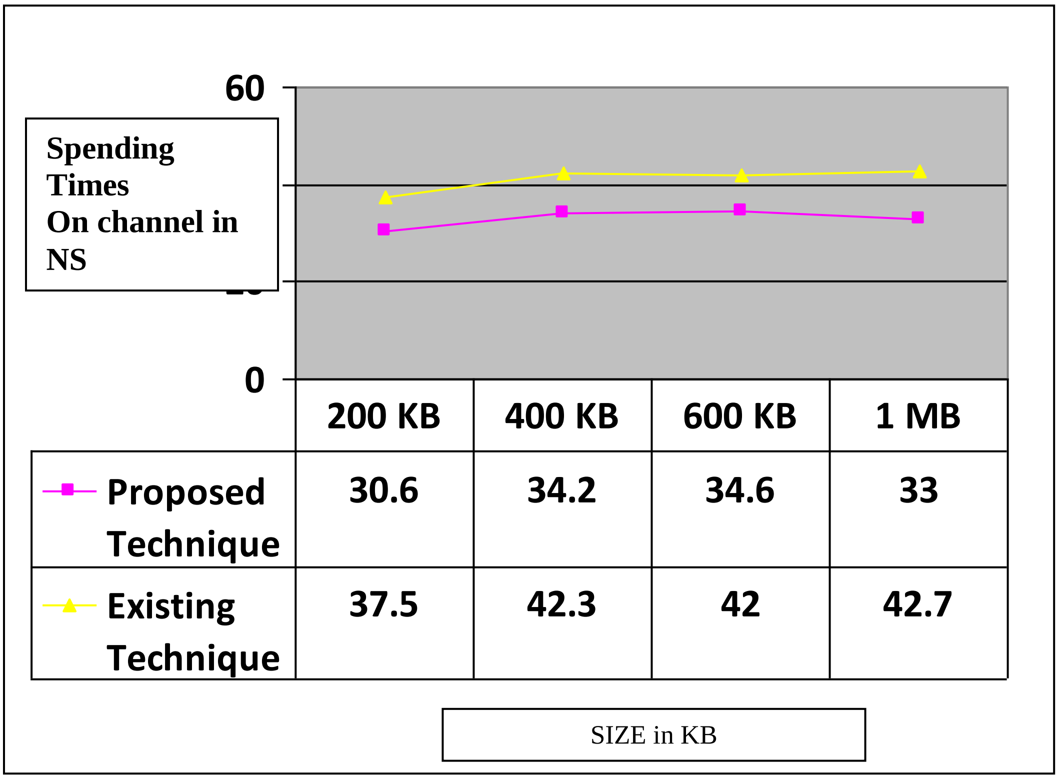
The first key is should be entered from user, it may be password of user or service provider can add extra button for a secret key but the key service provider should be unaware from secret key and providers have to cooperate their user to secure data.

4. Result

Table 1. Result of Algorithm

# Rounds		**Key1**	**Newkey**	**Plaintext**	**ciphertext**
Initial Stage	**Key1=** aw23e45t6, Key2= fd34eft56				
1		12qwaszx3	-;a#4d&k9	security	Cd5%l*ku
2		-;a#4d&k9	/>e@t*)!l	Cd5%l*ku	-<i7b2'{
3		/>e@t*)!l	Ax+.0se\p	-<i7b2'{	]yi&by()
4		Ax+.0se\p	V([ty^"$e	]yi&by()	Ju?:[]0@ **Encrypted Data**

In Table 1 we can see that how the key is changing and it is unexpected key, sometimes it may be happen new key would be invisible symbol that's why I am showing all these characters because character of each ASCII is not available on the keyboard but in the above example we can see that how invisible character means the system notification symbol is used as a new key. This algorithm is not only for key length of 9 bytes it supports variable key length but length should be square of any integer. If we use the maximum length of the key then it is more secure because for maximum key length there would be the maximum number of rounds which keeps user's data secure from unauthorized user. Like existing encryption algorithm this Algorithm doesn't require



	200 KB	400 KB	600 KB	1 MB
Proposed Technique	30.6	34.2	34.6	33
Existing Technique	37.5	42.3	42	42.7

Figure 2. Transmission Time of Existing Technique and Proposed Technique

5. Conclusion / Future Work

Security of stored data is a very big challenge for cloud service provider, on cloud computing users only access their data and use the service provided by the service provider, users don’t know anything about its security and don’t have any control on their data. So, in this paper we proposed our new algorithm to give control to users for their data security. From the above example and Table1 we analyzed that this algorithm provides better security and also gives full control to users. 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 I used 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 proposed technique provides better security which is controlled by the users itself.

Acknowledgment

I want to say thank to my Respected Faculty Dr. Ritu Sindhu for their support and guidance throughout my course here. To me, she has been more than a research advisor, his advice have benefited and enriched me in several ways. Thank also goes to all fellow students, proof readers, respected faculties and my supportive friend. Especially to those friends they continually and persuasively convey a spirit of adventure in regard to my work.

References

[1] K. Khajehei, “Secure Communication in Cloud by Using ECC Algorithm”, International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 1, **(2014)** January.

[2] P. Bhisikar and A. Sahu, “Security in Data Storage and Transmission in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, **(2013)** March.

[3] A. Patel and M. 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, vol. 3, no. 4, **(2013)** April.

[4] K. Lee, “Security Threats in Cloud Computing Environments”, International Journal of Security and Its Applications, vol. 6, no. 4, **(2012)** October.

[5] R. Maheshwari and S. Pathak, “A Proposed Secure Framework for Safe Data Transmission in Private Cloud”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, vol. 1, no. 1, **(2012)** April.

[6] A. T. Velte, “Cloud Computing A Practical Approach 1st Edition”, Tata Mcgraw Hill, ISBN-13-9780070683518, **(2009)**.

[7] 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, no. 4, **(2014)** April.

[8] M. Ebrahim, S. Khan and U. Bin Khalid, “Symmetric Algorithm Survey: A Comparative Analysis”, International Journal of Computer Applications (0975 – 8887), vol. 61, no. 20, **(2013)** January.

[9] Md A. Mushtaque and Mr. K. 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, no. V, **(2014)** May.

[10] A. Satapathy, J. Chandrakant Badajena and C. Rout, “A Secure Model and Algorithms for Cloud Computing Based on Multicloud Service Providers”, International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 12, **(2013)** December.

[11] http://en.wikipedia.org/wiki/Cloud_computing accessed on 25th April **(2014)**.

[12] 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, no. 1, **(2014)** January.

Authors

Dr. Ritu Sindhu, Assitant Professor of Galgotias University, Greater Noida, U.P., India. Her research interest include Operating System, MANET, Network Security, Failure Handling and Distributed System.

MD Asif Mushtaque, Student of M.Tech in Computer Science and Engineering of Galgotias University, Greater Noida, U.P., India. My research interest include Network Security, Failure Handling and cloud computing.