International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Enhancing Security Mechanism to Sensitive Message and Data over Cloud

Neil Kamal[1], Mayur Rathi[2]

P.G. Student, Madhya Pradesh, India CSE, LNCTS (RIT), Indore, Madhya Pradesh, India[1]
Assistant Professor, Madhya Pradesh, India CSE, LNCTS (RIT), Indore, Madhya Pradesh, India[2]

ABSTRACT

Cloud computing is becoming very poplar due to its cost effectiveness. Because it provides large exposure area making prone to security threat. Shifts infrastructure costs to operational cost. In cloud computing data moves to and from in premises network to outside networks. This raises paradigm brings concerning several new security challenges, that haven't been well addressed. Securing essential cloud resources from the unauthorized access of the users is one amongst the most important problems that cause reduces the growth of this technology within the IT Industries. Encryption of message data is one way to secure highly sensitive data over cloud. Paper covers mechanism to enhance security of sensitive message over cloud by providing mechanism on honey encryption method and using AES with custom mechanism.

Keywords : Cloud Computing, Cryptography, Honey Encryption, Securing Data

I. INTRODUCTION

At the present world of networking system, Cloud computing [1] is one the most important and developing concept for both the developers and the users. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing.

The servers, users and individuals. As a result files or data stored in the cloud become open to all. Therefore, data or files of an individual can be handled by all other users of the cloud. [2, 3] Thus the data or files become more vulnerable to attack. As a result it is very easy for an intruder to access, misuse and destroy the original form of data. An intruder can also interrupt the communication. Besides, cloud service providers provide different types of applications which are of very critical nature. Hence, it is extremely essential for the cloud to be secure [4]. Another problem with the cloud system is that an individual may not have control over the place where the data needed to be stored. A cloud user has to use the resource allocation and scheduling, provided by the cloud service provider. Thus, it is also necessary to protect the data or files in the midst of unsecured processing.

In this paper we have proposed new security architecture for cloud computing platform. In this model high ranked security algorithms are used for giving secured communication process over network. Here messages are encrypted with custom honey algorithm in which keys are generated randomly by the system and then encryption on individual ciphers. In our proposed model distributive server concept is used, thus ensuring higher security. Our architecture is highly secure making impossible to intruder to crack it even if with every attempt to recover plain text from wrong and right key (even if intruder knows the key) yields a decoy (or honey) message that appears, to the attacker, to be a sample from the target distribution. An attacker that knows no further information about the true message will be unable to pick it out from the decoys.

II. RELATED WORK

Numerous research on security in cloud computing has already been proposed and done in recent times. Identification based cloud computing security model have been worked out by different researchers [1]. But only identifying the actual user does not all the time prevent data hacking or data intruding in the database of cloud environment. Yao's Garbled Circuit is used for secure data saving in cloud servers [4, 5]. It is also an identification based work. The flaw in this system is that it does not ensure security in whole cloud computing platform. Research related to ensuring security in whole cloud computing environments was already worked out in different structures and shaped. AES based file encryption system is used in some of these models [9, 10]. But these models keep both the encryption key and encrypted file in one database server. Only one successful malicious attack in the server may open the whole information files to the hacker, which is not desirable. Some other models and secured architectures are proposed for ensuring security in cloud computing environment [4, 7]. Although these models ensures secured communication between users and servers, but they do not encrypt the loaded information. For best security ensuring process, the uploaded information needs to be encrypted so that none can know about the information and its location. Recently some other secured models for cloud computing environment are also being researched [8, 9]. The approach of Splitting and encrypting enhanced the security but still could be breached, makes system algorithm for splitting and merging complex and must go through one more phase in process.

Partitioning of data performed at Third Party Auditor. Partitioning module accept user input file. Partitioning function has an important role in this work. It Splits (break up) larger files into smaller parts. It helps to store the data effectively in quick manner enhancing easy access to data also when there is need. But involvement of third party for Auditing not only possess trust issue but also increases the cost. Algorithm used for splitting and merging is not clear having their efficiency not tested for different customer requirements. These models also fail to ensure all criteria of cloud computing security issues [11, 12, 13, 14].

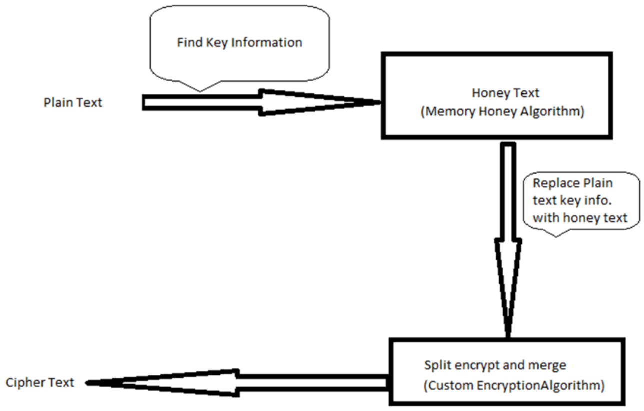

Figure 1. Architectural Diagram

In our method, we use custom encryption with AES and devised a memory based honey encryption algorithm for more sensitive messages. Method not only increases system security by many folds but also provides user trust due to custom algorithm and non-dependency on third party. Customer ease has been enhanced by enabling to use image to generate key.

III. PROPOSED ARCHITECTURE

Proposed architecture has been divided into three parts. Memory based honey encryption is applied to sensitive information in messages.

PROPOSED ALGORITHM

1. **Login Phase:-**

Step 1:- User enters User ID & Password.

Step 2:- After user is granted, server provides key.

2. **Honey Encryption Phase:-**

Step 1:- Find the sensitive informations like Identify numbers, mobile numbers and key answer informations in plain text.

Step 2:- Separate identified texts and apply memory honey encryption algorithm on each texts.

Memory Honey Algorithm

Run the memory honey algorithm for each keys in plain texts.

Find the sample space of required keyword.

We have created Initial set of sample spaces for each keyword and assigned an initial weight to each word. Let say S (Nationality) = {India =0.3, USA =0.1, China =0.3, Russia =0.1, Japan=0.2}

Step 1:- With addition of words in every message will add new word in sample space for that keyword with weight average of all words in sample space. Let say plain text word is Germany, not on sample space for nationality so add it i.e. S (Nationality) = {India =0.3, USA =0.1, China =0.3, Russia =0.1, Japan=0.2, Germany=0.2}

Step 2:- With every malicious attempt, weight of that word in corresponding keyword will increase in multiple of 2. Let suppose there incident of malicious attach has happened with provided honey text Russia. So increase its weight (0.1 X 2 = 0.2) with) 0.2. I.e. S (Nationality) = {India =0.3, USA =0.1, China =0.3, Russia =0.2, Japan=0.2, Germany=0.2}

Step 3:- Remove the first word in sample space among words having lowest weight.

I.e. S (Nationality) = {India =0.3, China =0.3, Russia =0.2, Japan=0.2, Germany=0.2}

Step 4:- Transpose the word with word in sample space by random selection technique.

Replace Plain text word with cipher honey texts.

3. **Custom Encryption Phase:-**

Step 1:- Get numbers of characters in plain text.

Step 2:- Upload Image file, convert into bytes of characters, store it as key (K2).

Step 3:- Distribute root key K1 characters into key K2 to get key K3.

Step 5:-Encrypt P1, P2, P3… Pk using AES to get corresponding cipher text C1, C2, C3…Ck.

Step 6:- Choose random point in between 0 to k, let say m.

Step 7:- Choose C [m] as first Cipher.

Step 8:- Partition it into two sets, say C [0] to C [m-1] and sets C [m+1] to C[k].

Step 9:- Take C [m-1/2] as second cipher and C [(k)-(m+1)/2] as third cipher.

Step 10:- Repeat step 8 and 9 until get all ciphers.

IV. RESULT ANALYSIS

For result analysis we implement this proposed technique in .NET and SQL server. For performance analysis proposed technique is compared with previously proposed techniques. This comparison is based on various dependency parameters as mentioned on Table 1 & Table 2.

Parameter	Split and Merge	Third Part Auditor	Proposed Architecture
Internet	No	Yes	No
Dependency on third Party	No	Yes	No
Multi-Level	No	No	Yes

Security			
Forging Intruder	**No**	**No**	**Yes**
Layer for securing critical sensitive information.	**No**	**No**	**Yes**

Table 1: Comparison of Proposed Technique

Attacks	Status
Man-in the middle attack	YES
Eavesdropping	YES
Insider attack	YES
Outsider attack	YES
Identity Spoofing	YES
Identity disclosure attack	YES
Replay attack	YES
Password based attack	YES

Table 2 : Preventions from various attacks

V. CONCLUSION

This paper we have proposed a newer security structure for cloud computing environment which includes honey based encryption with custom algorithm through image for secure communication. This model ensures security for the data storage on cloud structure. Here, execution time is not subsequently high because implementation of each algorithm is done in different servers. In our proposed system, an intruder cannot decrypt stored data, we have provided extra layer of encryption on critical information in message, and every message has been fragmented and encrypted. The model, though it is developed in a cloud environment, individual servers' operation has got priority here. Memory Honey Encryption has been designed, however, the wrong guess will generate phony results that appear to be genuine. With each wrong attempt algorithm becomes more and more efficient. The brute force attack is the major problem which is eliminated, and the side channel attack and the difficulty in the field of the key management can be removed effectively.

In future we want to work with ensuring secure communication system between users and system, user to user. We also want to work with encryption algorithms to find out more light and secure encryption system for secured file information preserving system.

VI. REFERENCES

[1]. Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science Emerging Technology, Vol-2 No 5 October, 2011 , 316-322

[2]. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011

[3]. Mladen A. Vouk, "Cloud Computing - Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235-246

[4]. Ye Hu, Johnny Wong, Gabriel Iszlai, Marin Litoiu, "Resource Provisioning for Cloud Computing", IBM Canada Ltd., 2009

[5]. Daniele Catteddu, Giles Hogben, "Cloud Computing:- Benefits, risks and recommendations for information security", November, 2009

[6]. "Cloud Computing: Silver Lining or Storm Ahead?", Volume 13 Number 2, Spring 2010

[7]. NGONGANG GUY MOLLET, "CLOUD COMPUTING SECURITY" , Thesis Paper, April 11

[8]. Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", 1999

[9]. Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001

[10]. Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January 2010.

[11]. TCloud: A Trusted Architecture for Cloud, International Journal of Advanced Science and Technology Vol.63, 2014.

[12]. Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3), 2014

[13]. Using Cryptography Algorithms to Secure Cloud Computing Data and Services, American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-6, Issue-10, pp-334-337, 2017

[14]. Improving Data Integrity for Data Storage Security in Cloud Computing, IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.6, June 2015