International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Storage Security in Cloud Computing

Mamta Shinde[1], Anjali Jaiswal[2], Asmita Shinde[3], Mr. Rushikesh R. Nikam[4]

[1,2,3]Student, Department of Computer Engineering, New Horizon Institute of Technology and Management (Thane) Mumbai, Maharashtra.
[4]Professor, Department of Computer Engineering, New Horizon Institute of Technology and Management (Thane) Mumbai, Maharashtra.

Abstract – *Nowdays, the security is most concerned issue in the world. Because of less security and confidentiality the hackers will be easily capture the sensitive data or information through the internet. In this system we are providing security to a data in cloud computing. The cloud computing gives us better scalability, availability and confidentiality which provides data safety and security over the internet. Thus, the system implements a dual level of encryption algorithm for data file. The data file first converted into ciphertext-1 using AES algorithm of 256 bits which is symmetric encryption method then ciphertext-1 is again encrypted into ciphertext-2 using BLOWFISH algorithm which is randomly generated asymmetric encryption method. If anyone gets the cipher text, he could not extract the encryption key to recover the data contents. The proposed algorithm protects the information from the hackers to capture the data into the cloud. Thus, the data is safe in the cloud. Low complexity and easy implementation make the proposed algorithm widely applicable safeguard in the cloud computing.*

Key Words: Cloud Computing, Cryptography, Encryption, Decryption

1. INTRODUCTION

Cloud computing is used for processing and storing data of the consumers over the Internet. Cloud computing provides a computer user access to Information Technology (IT) services i.e., applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure. The consumers need no concern where the hardware and software or the application is operating; they only need to have a simple device that can simply operate with the cloud.

The three key cloud services are termed as: Infrastructure-as a-Service (IaaS), Platform-as-a-Service (PaaS) and Software As-a-Service (SaaS).Where (IaaS) provide us with Virtual machine, (PaaS) third party services like operating system, programming environments and web servers, and (SaaS) provide us with different software programs. There are Four deployment model: Private cloud, public cloud hybrid cloud and community cloud. Public cloud environments are accessible by multiple users. Whereas the private clouds are protected by organization. Since the Private cloud is protected but the rest have high risk of data leak. As the third party manages the data. And also the rising issue in cloud computing is its security measure as side channel attack is possible in cloud computing. Hence affecting the privacy of the user .The most dealing issue is the security of the cloud, especially the data and multimedia contents such as image, audio and video. Several studies have been done on the security of the multimedia contents in the cloud and decrease the side channel attack.

So to overcome this situation the combination of two different encryption algorithms are used .That is it implements a double stage encryption algorithm for the security of multimedia contents using a randomly generated key and the 94 bit converter. The randomly generated key makes the second stage encrypted data unbreakable. This is not only for the attackers but also for the system administrator. Thus, the paper provides more security of the multimedia content in the cloud.

In this paper, as said the system has double level of encryption the data is first encrypted using the AES algorithm giving result to Cipher text -1 and then then this cipher text acts as a input to second algorithm that is Blowfish algorithm hence the data is encrypted twice which results to cipher text 2 and third cipher text 2 is stored in the cloud .Similarly the the same procedure is repeated in reverse for the decryption process

2. LITERATURE SURVEY

In cloud computing, since it is a new area, the developers are concentrating more on computation speed and storage issue. Users going for unreliable networks without their knowledge to share the data content even though there are availability of more promising streaming technology and increased broadband speed. At present, the security of the data contents becomes a rising issue.

Have concerned some security issues based on the data contents in cloud for the next century. The [5] paper represented a survey on recently performed research activities on multimedia security and intersected four burning questions such as data integrity, data confidentiality, access control and data manipulation . The

paper showed various vulnerabilities, threats and attacks that hindered the more adoption of emerging cloud and identified some future challenges. Another study proposed taxonomy of security in the cloud layers and represented the current status of security in the rising cloud computing [IS].[6] He describe that a known-plaintext attack which can be used to successfully access the encryption key with the preknowledge of only one arbitrary pair of known plaintext-cipher text. A phase retrieval algorithm has been employed in this attack and also Computer simulations are made to demonstrate the effectiveness. The results have been showing that even after implementing only one round of iteration in the phase retrieval, an attacker can obtain a clear decoded plaintext from an intercepted cipher text.

Several studies have been done on the security of the data contents in the cloud. [1] In this system it replaces the DES algorithm by the AES algorithm due to the inbuilt scarcity of strength and combined the AES with the RSA in order to apply security features. As soon as user tries to upload the data on cloud, the data is first stored in a temporary directory and after calling AES and RSA algorithm, requiring the user to enter the AES secret key the file will get stored into the database permanently corresponding to the user account and the temporary file get deleted.[2] Their was a system which proposed an advanced algorithm combining the RSA with two fish. These studies focused on the combination of two different algorithms and generated a security key for consumers as a key to access the cloud. The mitigation of the side channel attack was shown and the proposed algorithm focused only on the two prime numbers. The above study leads us to implement a double stage encryption algorithm for the security of data contents against a negligent third party and side channel attack. The proposed randomly generated key algorithm produces every time a unique symmetric key that lets the data be encrypted successfully.

A literature review was performed to find out an effective algorithm having minimum complexity and widely applicable cloud security for the multimedia contents against the side channel attack. Since it is more difficult to stop or identify the side channel attack, hence the double stage encryption allows cipher text to store on the cloud i.e. VM. For storage purpose we are using drop box tool as our virtual box which provide a personal cloud storage service. The double stage decryption transmits the original data from the VM. Based on the literature study the required languages, tools and hardware are selected to develop the proposed algorithm. C++ and Java are the chosen languages and Code Blocks and Net beans are the chosen compilers. At first, the data content is stored in a file. The file which is encrypted in cipher text-l after executing the Java code in Net beans and The cipher text-l is stored in another file. This second file is encrypted again using a randomly generated key and the 256 bit converter into the ciphertext-2 after executing and stored in the cloud or virtual machine. The decryption process is at the same but in reverse order that have done before for the encryption process.

3. PROPOSED METHODOLOGY

This section describes the implementation plan that performs the better security for multimedia data against side channel attack in cloud computing. The system represents a dual stage encryption of data using AES and Blowfish algorithm which provides the security to the data contents in the private cloud. The private cloud is developed using dropbox which is open source tool.

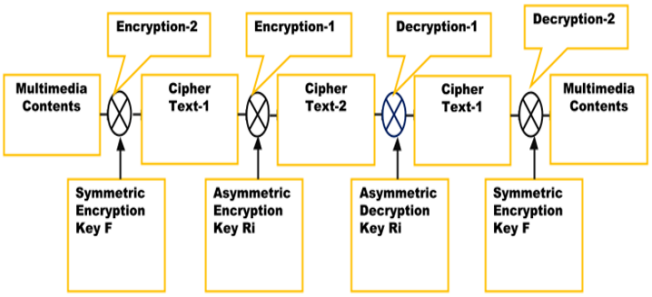

Fig -1: Block diagram

The proposed algorithm is crucial in the second stage randomly generated key provides more security than the conventional encryption system. The whole process is shown in the system architecture in Fig2.

At the first stage the multimedia contents are encrypted by the conventional encryption process using symmetric key. In the second stage, the encrypted cipher text-l is then again encrypted by the randomly generated asymmetric key thus produce ciphertext-2. In the decryption stage, the encrypted ciphertext-2 is decrypted by the asymmetric key in the first decryption process. Thus produced the cipher text-I. The cipher text-l is then decrypted by symmetric key method and regain the original data file content. Since the conventional encryption process the key is symmetric the attacker can easily be known the encryption key and retain original data content. In the proposed encryption method the key is generated randomly and the Key exposition possibility is low.

3.1 Proposed Design

The cloud is a server-client model and the server system consists of agent module, security module, analysis module and database. Though the conventional cloud model has single encryption and decryption process, the

proposed cloud security model has double encryption and decryption model (see Fig.1). In the security module, the content manager introduces the cloud contents double encryption processes (Encryption I and Encryption 2).

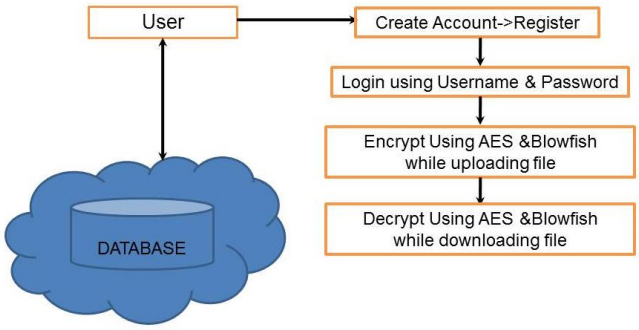

Fig -2: System Architecture

The Encryption-I is usually provided by all cloud architecture and produces cipher text-I, the proposed Encryption-2 is an attachment based on the architecture to secure the cloud data using randomly generated key and convert the cipher text-I into ciphertext-2. The randomly generated key is unknown to the content manager too. In the client, the decrypt processor has double decryption processes (Decryption-l and Decryption-2) and content player. The proposed Decryption-I is decrypted by random key and converts the ciphertext-2 into cipher text-I. The Decryption-2 finally converts the cipher text-I to data contents using symmetric key. Without the randomly generated key, the Decryption-I process is difficult and thus the proposed architecture gives efficient security.

3.2 Encryption Process:-

While encrypting the multimedia data into cipher text, theciphertext-1 has been stored into a file. That has been used for the second pass encryption to generate the ciphertext-2. When the cipher text -1 generated, a randomly generated asymmetric key has been used for the encryption. Then the encrypted data stored in the cloud. In cloud computing, grabbing the user data from attackers is a difficult task.

In encryption process, first the data file is converted into cihertext-1 using public symmetric key. Then for the second encryption process, a random prime number (p) is chosen. The cipher texts are read character by character. In each pass a single character (n) is multiplied with the prime and converted the result into (m) to the 256-bit format. The converted value is then stored in the cloud. A separator is then added with that value. The 256-bit format is the set of printable character having the ASCII value from 33 to 126. To prevent from generating the next prime location from out of range, the prime number (p) is mod by the character (n) and stored the result as (s). The location of the next random prime is the lower index of the mod result (s). A prime array is used to generate the random prime. On the second pass the Prime array is rearranged by moving the prime number onto the first location of the array. The procedure ensures that selected prime is always random. With every pass of the encryption process the separators are programmatically generated that will help to find the random prime at the time of decryption. Until Remaining the ciphertext-2 the procedure is continued. The entire procedure of the proposed encryption algorithm is described in the pseudo code. The pseudo code takes a string as input and processes the string according to the encryption algorithm. Then the string is converted into ciphertext-2 and stored in the cloud.

The pseudo code for encryption operation is:

```
ENCRYPTION-PROCEDURE (String str)
1 len := str.length
2 p := Random (prime)
3 for i=1 to len
4 n := str [i]
5 k := 94-bit-converter (p*n)
6 PRINT "k" II k as a ciper text
7 s := p mod n
8 p := s-1
9 end
```

After completing the whole encryption process of the ciphertext-1 into the ciphertext-2 the encrypted data is stored in the cloud.

3.3 Decryption Process

In the decryption process at first, the each character of a cipher text is read sequentially one after another and add them to the temp (temporary variable) until found the separator. A character out of 256-bit converter is treated as a separator. By using the separator the random prime (p) is regenerated using at the time of encryption. Then the temp is converted into a decimal value (v). The value is then divided by the prime (p) and regained the desired ciphertext-1 (n). The ciphertext-1 is then stored in the temporary string until the ciphertext-2 remains. The desired output strings are then written to the targeted file and stop the decryption process. Again decrypting the ciphertext-1 for the second step the data is finally recovered.

The pseudo code for decryption operation:

```
DECRYPTION-PROCEDURE (string cp)
1 len := cp.length
2 t := charValue (cp [0])
3 p := prime [t-l]
4 for i= 0 to len - 1
```

```
5 set k := cp [i]
6 if separtor == false
7 temString := temString + k
8 else v := temString
9 n := vip;
10 str := str + n
11 temsSring := NULL
12 t := upperPos (p mod n)
13 p := prime [t-l]
14 end
15 return str
```

4. RESULT

This section analyzes the performance of the proposed approach through the appropriate setup to secure the data content in the cloud server. The different size of data content takes different time to generate different ciphertext -1 and then ciphertext-2. The comparative analysis shows that the performance of this setup. The algorithm gives hopeful result to secure data contents tested in various formats and sizes.

Section	Convential Encryption System	Proposed Encryption System
Encryption Method	Singular Symmetric key	Double symmetric and asymmetric key
Key Type	Fixed	Random
Key expansion possibility	High	Low

Fig -3: SECURITY COMPARISON WITH CONVENTIONAL ALGORITHM

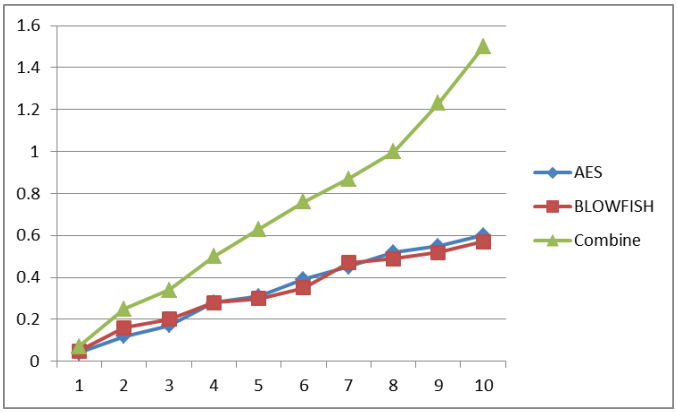

Fig -4: Encryption of file using AES ,BLOWFISH and Both Algorithm

Fig.4 illustrate that the execution time of AES, BLOWFISH and combination of both algorithm for data content is similar to the small data size. With increasing data rate, there is small difference between encryption times for the content using each algorithm.

In AES algorithm it takes 4.5 seconds to encrypt the 7MB data and in BLOWFISH algorithm it takes 4 .7seconds to encrypt the 7MB data. That is both algorithm takes almost same time for the same data size. In combination of both algorithm AES and BLOWFISH it takes 8.7 seconds to encrypt the 7MB data. Its shows the combination of both algorithm is takes almost same time or less than the time required by individually time takes and we combining them than it is little bit high than the individual algorithm.

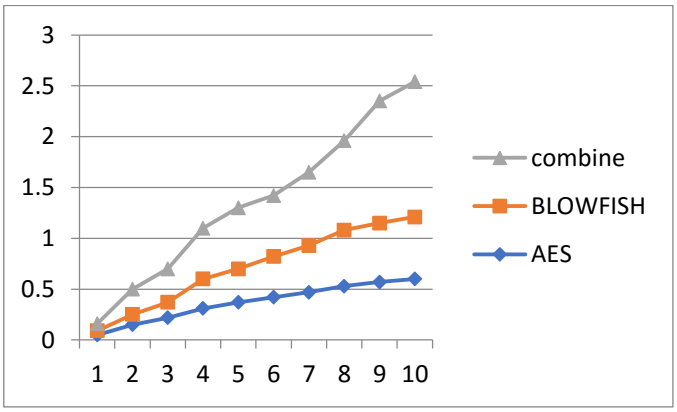

Fig -5: Decryption of file using AES ,BLOWFISH and Both Algorithm

Fig.5 illustrate that the execution time of AES, BLOWFISH and combination of both algorithm for data content is similar to the small data size. With increasing data rate, there is small difference between decryption time for the content using each algorithm.

In AES algorithm it takes 4.7 seconds to decrypt the 7MB data and in BLOWFISH algorithm it takes 4.6 seconds to decrypt the 7MB data. That is both algorithm takes almost same time for the same data size.In combination of both algorithm AES and BLOWFISH it takes 7.2 seconds to decrypt the 7MB data.

5. CONCLUSION

The system represents a double stage encryption algorithm that provides the security to data contents in the cloud. The proposed algorithm is crucial in the second stage. The randomly generated key provides more security than the conventional encryption system. The 256-bit converter generates the multimedia contents into the cipher text. The cipher text is stored in the cloud instead of original data content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protect

the information from the side channel attacker to grab the data from the cloud.

REFERENCES

1. 1.Rackspace Support, “Understanding the Cloud Computing Stack”, October 2013, http://www.rackspace.com/knowledge_center/whitepaper/understanding -the-cloud computing-stack-saas-paas-iaas

2. Webopedia.com, "What is Cloud Computing? A Webopedia Definition", 2015. [Online].Available: http://www.webopedia.com/TERM/C/cloud_computing.html "Why use clouds? - Cloud lounge", 2015. [Online]. Available: http://www.cloudlounge.org/why-use-clouds.html

3. V. S. Mahalle and A. K. Shahade, "Enhancing the data security in cloud by implementing hybrid (rsa&aes) encryption algorithm," in International Conference on Power, Automation and Communication (lNPAC), pp. 146-149, Amravati, India, October 2014.

4. P. Gupta and A. K. Brar, "An Enhanced Security Technique for Storageof Multimedia Content over Cloud Server," International Journal ofEngineering Research and Applications (lJERA), vol. 3, no. 4, pp.2273-2277, ACM, 2013

5. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "ASurvey on Security Issues and Solutions at Different Layers of CloudComputing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561-592, Springer, 2013

6. C.-T. Huang, Z. Qin, and c.-C. J. Kuo, "Multimedia storage security incloud computing: An overview;' in IEEE 13th International Workshopon Multimedia Signal Processing (MMSP), pp. 1-6, HNA Resort YunqiHangzhou, China, October 2011.

7. E. J. Delp, "Multimedia Security: The 22nd Century Approach," MultimediaSystems, vol. 11, no. 2, pp. 95-97, Springer, 2005.

8. W. Qin, X. Peng, X. Meng, and W. He, "Improved Known-PlaintextAttack on Optical Encryption Based on Double Random Phase Encoding,"in Symposium on Photonics and Optoelectronics, pp. 1-4, June201

9. Dropbox white paper:- https://www.dropbox.com/static/business/resources/Security_Whitepaper.pdf