Multimedia Content Security with Random Key Generation Approach in Cloud Computing

Chandan Thakur[1], Rashmita Pandey[2], Nusrat Parveen[3]

[1,2]*Student, Computer Department, Datta Meghe College of Engineering, Maharashtra, India*

[3]*Professor, Computer Department, Datta Meghe College of Engineering, Maharashtra, India*

---***---

Abstract - *The cloud computing offers high scalability, confidentiality and easy accessibility of information over the internet. Though the conventional encryption system provides security, the most concerned issue is the regular side channel attack for capturing ones sensitive and confidential image, audio and video. A malicious Virtual Machine (VM) beside targeted VM can extract all information. Thus, this paper implements double stage encryption algorithm for multimedia content security using random key generation. The first stage encrypts multimedia content into ciphertext-1 using a symmetric public key. The ciphertext-1 is again encrypted in the cloud using a randomly generated symmetric private key. If anyone gets the cipher text, he could not extract the encryption key to recover multimedia contents. Low complexity and easy implementations make the proposed algorithm widely applicable safeguard in cloud computing.*

Keyword: *Cipher text, Encryption, Multimedia, Virtual Machine, random Key generation*

1.INTRODUCTION

1.1 Cloud Computing:

Cloud computing is freedom of processing and storing data of consumers in the third-party data center using remote computing resources over the Internet. The cloud is the combination of three services. The goal of cloud computing is to allow users to take benefit from all these technologies, without the need for deep knowledge. The cloud computing aims to cut costs, and helps the users to focus on their core business instead of being impeded by IT obstacles. Cloud computing and storage solutions provides services to users and enterprises with various capabilities to store and process their data in third party data centers that may be located far from user-ranging in distance from across a city to across the world. A third party manages the data and multimedia contents and has the liabilities to make certain security for the protection of data and multimedia contents and provide uninterrupted services. Unless there may be arise in security question and trustworthiness of third party.Beside the third party deliberately or inadvertently discloses the data.

1.2 Security issues in Cloud:

While it is generally agreed that encryption is necessary to protect data security, working with encrypted data proves to be challenging in cloud. The problem of using public cloud is the cloud owner can't be trusted with the data. to be challenging in cloud. The problem of using public cloud is the cloud owner can't be trusted with the data. Hence a solution is required to safeguard the data. A solution would be to download and decrypt all the documents to extract the relevant information.

1.2.1 Data Integrity:

A secured system ensures that the data it contains is valid. Data integrity implies that knowledge is protected against deletion and corruption each once it's among the information, and whereas it's being transmitted over the network.

1.2.2 Data Confidentiality:

A secure system ensures the confidentiality of data. This means that it allows users to see only those data which they are supposed to see. Whenever possible, confidential data should be encrypted and decrypted during on-premises or end-point processing before it is transferred to the cloud. The key concern is protecting data confidentiality in end-to-end fashion.

1.2.3 Access Control:

Access control states that information shared over cloud must be accessible to authorized users. Access should be given to only those users who have authority to gain the access to the shared data.

1.2.4 Data Manipulation:

It is an effort to make data more easier to read or to be more organized.

2. LITERATURE SURVEY

In cloud computing, since it is a new area, the developers are concentrating more on computation speed and storage issue. Users are going for unreliable networks without their knowledge to share the media content even though there are availability of more promising streaming technology and increased broadband speed. At present, the security of the multimedia contents such as image, audio and video become a rising issue. A survey on recently performed analysis activities on multimedia system security and intersected four burning queries like knowledge integrity, data confidentiality, access control and data manipulation.

Several studies are done on the protection of the multimedia system contents within the cloud. The paper replaces the DES algorithm by the AES algorithm due to the inbuilt scarcity of strength and combined the AES with the RSA. Gupta et al. also projected a sophisticated algorithmic rule combining the RSA with 2 fish. These studies targeted on the mix of 2 totally different algorithms and generated a security key for shoppers as a key to access the cloud. The mitigation of the facet channel attack was shown and also the projected algorithmic rule targeted solely on the 2 prime numbers. The on top of study leads USA to implement a double stage encoding algorithmic rule for the protection of multimedia system contents against a negligent third party and facet channel attack. The projected every which way generated key algorithmic rule produces when a novel isosceles key that lets the information be encrypted with success. A literature review is performed to search out a good algorithmic rule having minimum complexne**ss** and wide applicable cloud security for the multimedia system contents against the facet 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 in the VM. The double stage decryption transmits the original data from the VM. Based on the literature study the specified languages, tools and hardware area unit chosen to develop the projected algorithm.

2.1 Existing System:

The security of multimedia contents in the cloud. The replaces the DES algorithm by the AES algorithm due to the inbuilt scarcity of strength and combined the AES with the RSA. Also projected a sophisticated algorithmic rule combining the RSA with two fish. These studies focused on the combination of two completely different algorithms and generated security key for users as a key to access the cloud. The mitigation of aspect channel attack was shown and therefore the proposed algorithm focused solely on the two prime numbers.

Disadvantages of existing system
I. Encryption Singular Symmetric Method key and asymmetric key.

II. Key Type Fixed.

III. Key exposition possibility high.

2.2 Proposed System:

This project double stage encryption algorithm that provides the security of multimedia contents such as image, audio and video in the cloud. In first stage data is encrypted using AES or Blow fish algorithm. Both AES and Blowfish algorithm is used in this system. AES algorithm is used as first encryption algorithm. The proposed algorithm is critical in the second stage. The randomly generated key provides additional security than the traditional encryption system. The 94-bit converter generates the multimedia contents into the cipher text. The cipher text is stored in the cloud instead of original multimedia content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protects the information from the side channel attacker to grab the multimedia data into the cloud. Thus, the multimedia is safe within the cloud.

Advantages of Proposed system:
I. Encryption Double Symmetric Method key and asymmetric key.

II. Key Type Random.

III. Key exposition possibility low.

3.METHODOLOGY & IMPLEMENTATIONS

3.1 System Architecture:

The system Architecture model involves three parties: the data owner, the cloud server and the user. The fig.1 illustrates the Architecture of System which includes encryption and decryption process flow.

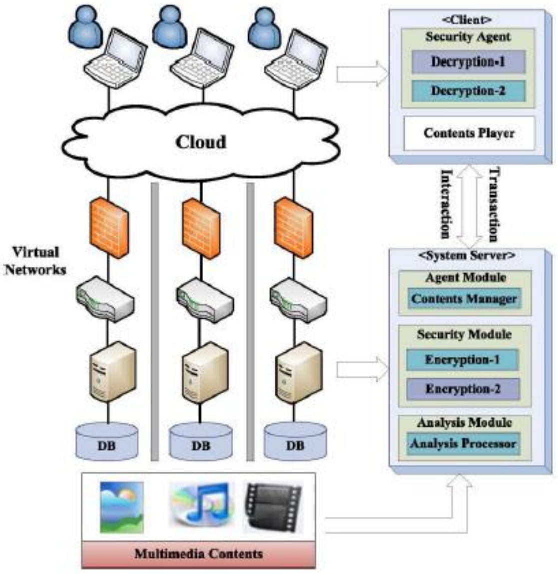

Fig - 1: System Architecture

3.2 Proposed Algorithm:

The proposed randomly generated key algorithm produces every time a unique symmetric key that lets the data be encrypted successfully. In this system hybrid encryption technique is apply on the data file using AES and Blowfish algorithm to securely store file data in cloud. File sharing is possible using this cloud computing database. File data share between user and owner is secure using hybrid encryption technique. In the first stage multimedia content is encrypted into ciphertext-1 using a AES symmetric key. The ciphertext-1 is again encrypted using a Blowfish algorithm. The decryption is done in reverse order as shown in fig. 2

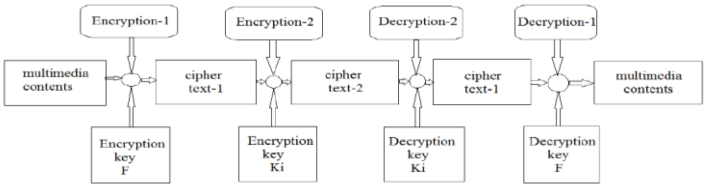

Fig - 2: Dual encryption and Decryption process

3.2.1 AES Algorithm:

The AES stands for Advanced Encryption Standard is a symmetric key algorithm. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, while maximum block size is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) network.

1. Key Expansion- each and every round keys are derived from the cipher key using AES key schedule. AES requires a separate 128-bit key block for each round plus one more.

2. Initial Round Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds a. Sub Bytes—

a. non-linear substitution step wherever every computer memory unit is replaced with another per a search table.

b. Shift Rows- a transposition step where last three rows of state are shifted cyclically in a certain number of steps.

c. Mixed Columns- a compound operation that operates on the columns of the state,

combining the four bytes in each column.

d. Add Round Key

4. Final Round (no Mix Columns)

a. Sub Bytes

b. Shift Rows

c. Add Round Key.

3.2.2 Blowfish Algorithm:

Blowfish is a symmetric block encryption algorithm designed in consideration with,

I. Fast: It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

II. Compact: It can run in less than 5K of memory.

III. Simple: It uses addition, XOR, lookup table with 32-bit operands.

IV. Secure: The key length is variable and it can be in the range of 32-448 bits. (Default 128 bits key length). Blowfish block cipher algorithm encrypts block data of 64-bits at a time.it will follows the festal network and this algorithm is divided into two parts.

Key-expansion:

It will convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Blowfish uses large number of sub keys. These keys are generated earlier of any data encipherment or decipherment. The p-array consists of 18, 32-bit sub keys:

P1,P2,…………,P18

Four 32-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,………. S1,255

S2,0, S2,1,……….. S2,255

S3,0, S3,1,……….. S3,255

S4,0, S4,1,…………..S4,255

Generating the Sub keys:

The sub keys are calculated using the Blowfish algorithm:

i. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal representation of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

ii. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits till the whole P-array has been XORed with key bits. (For each and every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

iii. Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).

iv. Replace P1 and P2 with the output of step (3).

v. Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.

vi. Replace P3 and P4 with the output of step (5).

vii. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are needed to create all needed sub keys. Applications will store the sub keys instead of executing this derivation process multiple times.

It is having a function of 16 iterations of network. Each round consists of key-dependent permutation and data-dependent substitution. All operations are XORed and additions on 32-bit words. The only further operations are four indexed array data lookup tables for each round.

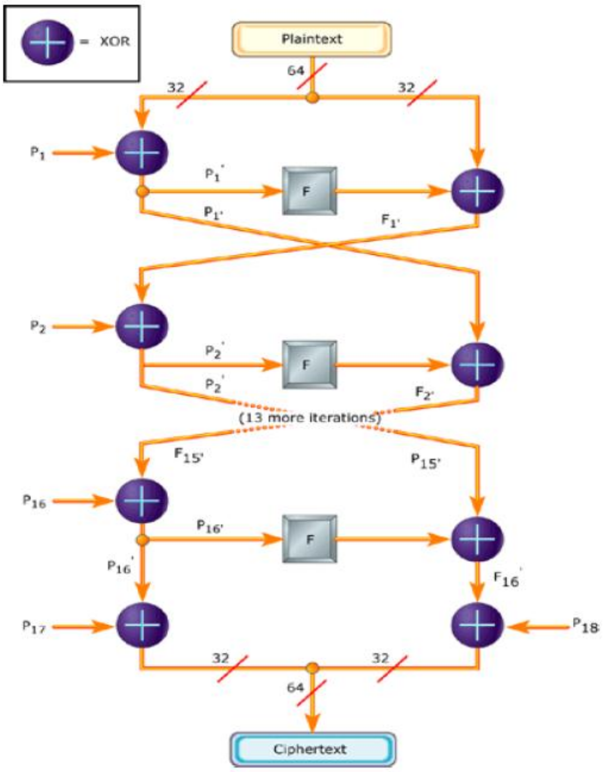

Fig - 3: Blowfish Encryption

Algorithm: Blowfish Encryption

```
Divide x into two 32-bit halves: xL, xR

For i = 1to 16

xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR
```

4. CONCLUSION

This project represents a double stage encryption algorithm that provides the security of multimedia contents such as image, audio and video in the cloud. The proposed algorithm is critical in the second stage. The randomly generated key provides additional security than the traditional encryption system. The 64-bit converter generates the multimedia contents into the ciphertext. The ciphertext is stored in the cloud rather than in original multimedia content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protects the information from the side channel attacker to grab the multimedia data into the cloud. Thus, the multimedia data is secure in the cloud.

But as we know many of us uses smartphones frequently to upload content on cloud as a fast backup option. Hence there should also be security for content while uploading or downloading using cloud storage via smartphones. So in future we will be expanding our domain to other systems such as android and ios. Because of this many user who don't use computers all the time or don't have computer access frequently can use cloud without fear of getting their stuff deleted or stolen. By using this system on a smartphone there will be more portability and safety for cloud consumers.

5. REFERENCES

[1] P. Gupta and A. K. Brar, "An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 4, pp. 2273-2277, ACM, 2013.

[2] Sonal Guleria and DR. Sonia vatta, "To enhance multimedia security in cloud computing environment using Crossbreed Algorithm." International Journal of

Application or Innovation in Engineering and Management, vol. 2, 6 June 2013.

[3] Md. Habibur Rahman, Nazrul Islam, Mehedy Hasan Rafsan Jany, Shariful and Mohammad Motiur Rahman, “Multimedia Content Security with Random Key Generation Approach in Cloud Computing.” IEEE cyber security and privacy,vol 4, may 2017.

[4] W. Kim, "Cloud Computing: Today and Tomorrow." Journal of object technology, vol. 8, no. 1, pp. 65-72, 2009.

[5] H. Takabi, 1. B. Joshi, and G.-J. Abn, "Security and Privacy Challenges in Cloud Computing Environments;' IEEE Security & Privacy, no. 6, pp. 24-31, IEEE, 2010.

[6] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud Computing-the Business Perspective," Decision support systems, vol. 51, no. 1, pp. 176-189, Elsevier, 2011.