International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Multimedia Security on Cloud Computing Using Cryptography

Avdhoot V. Mane[1], Ankita Kumari[2], Aditi R. Mhaskar[3], Supriya P. Joshi[4]

[1,2,3]Student, Dept of Information Technology Engineering, A.C. Patil College of Engineering, Maharashtra, India
[4]Asst.Professor, Dept of Information Technology Engineering, A.C. Patil College of Engineering, Maharashtra, India

---

Abstract - *Cloud computing is raising field due to its performance, high availability, cost efficiency and lots of others. The data storage is provided by service providers. Due to lack of proper security control policy and weakness, which cause many vulnerability in cloud computing so still many business companies aren't willing to adopt these cloud computing technology. This exclusive pattern brings many new security challenges, which haven't been well implicit. The cloud computing offers high scalability, confidentiality and therefore the easy accessibility of the knowledge over the web. The major issues within the cloud computing are data integrity, data theft, privacy issues, infected application, data loss, data location, security on vendor level, security on user level.*

As the traditional encryption system provides security, the most important issue is that of regular side channel attack for capturing ones sensitive and confidential image, audio and video. A malicious Virtual Machine (VM) kept besides a targeted VM which can extract all information. Thus, this paper implements a two stage encryption algorithm for multimedia content security which use a randomly generation key method.

The first stage encrypted multimedia content into ciphertext-l using an asymmetric private key which is randomly generated. The ciphertext-l is again encrypted in the cloud using a symmetric public key. If anyone gets the cipher text, he couldn't extract the encryption key to recover the multimedia contents. Low complexity and straightforward implementation make the proposed algorithm widely applicable safeguard within the cloud computing.

Key Words: **Cloud Computing, Multimedia Security, Cryptography, Encryption, Decryption.**

1. INTRODUCTION

Cloud computing is the freedom of processing and storing data of the consumers in a third party data centre using the remote computing resources over the Internet. The cloud is really a well-equipped universal network structure. It allows access to a shared pool of computing resources over the web and permits online consumers to perform various tasks with the info. The cloud is that the combination of three potential services. The three key cloud services are termed as: Infrastructure-as a- Service (IaaS), Platform-as-a-Service (PaaS) and Software as- a-Service (SaaS).

Though the private cloud is protected by that specific organization, the remainder have data risk and security issues. Moreover, cloud preserves these data and multimedia contents to a large data centre. A third party manages the info and multimedia contents and has the liabilities to form certain security for the protection of the info and multimedia contents and supply uninterrupted services. Unless there may arise a security question and trustworthiness of third party. Besides the third party deliberately or inadvertently discloses the info. The side channel attacker extracts the info or multimedia contents after placing a malicious VM beside the targeted VM.

At present, the foremost dealing issue is that the security of the cloud, especially the info and multimedia contents like image, audio and video. Several studies have been done on the security of the multimedia contents within the cloud and reduce the side channel attack. These studies focused on the mixture of two different algorithms and generate a security key for consumers as a key to access the cloud. These drawback allow us to to implement a double stage encryption algorithm for the safety of multimedia contents against a negligent third party and side channel attack.

This paper implements a double stage secret writing rule for the protection of multimedia system contents employing a randomly generated key and therefore the sixty-four bit convertor. The randomly generated secret's the outstanding feature that creates the second stage encrypted information unbreakable. These studies focus on the mixture of 2 totally different algorithms which generates a random security key for customers as a key to access the cloud. Cloud computing offers totally different services in commonplace models like Infrastructure as a service (IaaS), Platform as a service (PaaS) and code as a service (SaaS). This paper uses commonplace service module as IaaS.

The structure of this paper is as follows. Section II includes the related work based on the cloud computing research activities that held recently. Section III is described the research methodology. Section IV is illustrated the proposed algorithm. Section V evaluates the performance of the results and Section VI concludes the paper with future work.

2. RELATED WORK

2.1. Associate in Nursing Approach to increased Security of multimedia system information Model Technology supported Cloud Computing Er. Mandeep Singh Sandhu Er. Sunny Singla [1]

Cloud computing is rising field attributable to its performance, high convenience, least price and plenty of others. In cloud computing, the info is hold on in storage provided by service suppliers. However, still several business corporations don't seem to be willing to adopt cloud computing technology thanks to lack of correct security management policy and weakness in safeguard that cause several vulnerabilities in cloud computing. This paper has been written to focus on the matter of information security. Service suppliers should have a viable thanks to shielding their clients' information, particularly to stop the info from speech act by unauthorized insiders.

2.2. An Enhanced Security Technique for storage of multimedia content over the cloud [2].

P. Gupta and A. K. Brar. This paper implements security on data such as audio, Video, text file and image stored in a cloud. This Security is provided using a combination of two Algorithms such as RSA and two fish algorithm. Storage of data files with the signature and an encryption algorithm based on a combination of RSA and Twofish (to have better security than RSA or Twofish alone) on Microsoft azure cloud.

2.3. To strengthen multimedia security in cloud computing surroundings exploitation Crossbreed rule. Sonal Guleria and DR. Sonia Vatta [3]

This paper implements framework for access management during a cloud to facilitate style the design |the look} of the safety system and reduce the complexness of system design and implementation. This will exploit the likelihood of RSA to support public-key cryptosystem and digital signatures. On the other hand, RSA and DES well outlined additionally as policy templet in his specific domain are provided for reference. To style Associate in nursing secret writing rule supported combination on RSA and DES to have higher security than RSA or DES alone to write down within the code the data files before storage on the cloud. It increased security and forestall replay attacks so, the results of this MI is delivered to the service model, and perform actions according to this security checking method.

At present, the safety of the multimedia contents like image, audio and video becomes a rising issue. Delp [4] and Huang et al. [5] have concerned some security issues supported the multimedia contents in cloud for subsequent century. These paper represented a survey on recently performed research activities on multimedia security and intersected four burning questions like data integrity, data confidentiality, and access control and data manipulation.

The paper showed [6] various vulnerabilities, threats and attacks that hindered the more adoption of emerging cloud and identified some future challenges. Some other study proposed taxonomy of security within the cloud layers and represented the present status of security within the rising cloud computing. The proposed [7] known-plaintext attack can successfully access the encryption key and visualize the info stored within the cloud server. Several studies are done on the safety of the multimedia contents within the cloud.

The paper [8] replaces the DES algorithm by the AES algorithm thanks to the inbuilt scarcity of strength and combined the AES with the RSA. Gupta et al. also proposed a complicated algorithm combining the RSA with two fish. These studies focused on the mixture 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 therefore the proposed algorithm focused only on the 2 prime numbers.

The study above made us implement a two stage encryption algorithm for safety of multimedia contents against a negligent third party and side channel attack. The proposed randomly generated key algorithm produces whenever a singular symmetric key that lets the info be encrypted successfully.

3. RESEARCH METHOD

A literature review is performed to find an efficient algorithm which has less complexity and widely applicable cloud security for the contents of multimedia against the side channel attack. The aim is to implement a double stage secret writing rule for the protection of multimedia contents against a negligent third party and aspect channel attack. The planned willy-nilly generated key rule produces when a singular trigonal key that lets the data be encrypted successfully. It'll give high-level security to multimedia contents to be transmitted from owner to user. Within the planned theme, {the information|the info|the information} owner is in charge of generating change information and causing them to the cloud server.

Thus, the data owner has got to store the encrypted file. During this technique hybrid secret writing technique is applied to {the information|the info|the information} file exploitation AES and Blowfish rule to firmly store file data within the cloud. File sharing is possible exploitation this cloud computing information. The information of file shared between user and owner is a secure exploitation hybrid secret writing technique.

4. PROPOSED ALGORITHM AND IMPLEMENTATION

This section describes the implementation plan that performs the higher security for multimedia data against side channel attack within the cloud computing. The entire process is shown within the diagram in Fig. 1. The double

stage encryption and decryption process was finished cloud security.

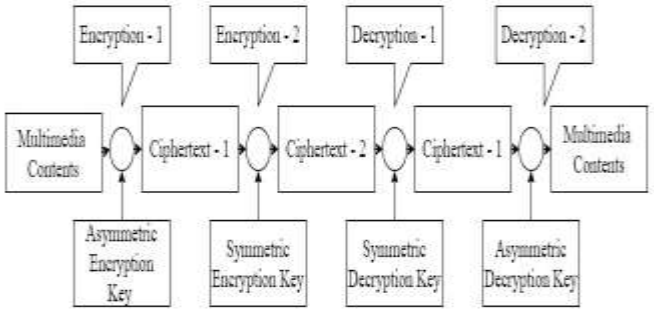


Figure 1: Block Diagram of Proposed Algorithm

At the primary stage the multimedia contents are encrypted by the traditional encryption process (DES, AES, RSA) using symmetric key.

In the second stage, the encrypted ciphertext-l is but 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 within the first decryption process. Thus produced the ciphertext-I.

The ciphertext-l is then decrypted by symmetric key method (DES, AES, RSA) and regain the first multimedia content. Since the traditional encryption process the key's symmetric the attacker can easily be known the encryption key and retain original multimedia content.

In the proposed encryption method the key's generated randomly and therefore the Key exposition possibility is low. Figure 2 shows the flow chart of the whole model.

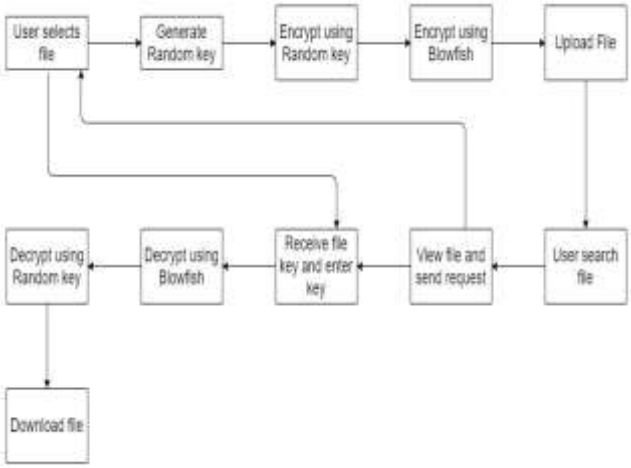


Figure 2: Block Diagram of Proposed System

4.1. Work Space Setup

In order to seek out out the multimedia content security in cloud computing an experimental setup was established having an Intel Core is predicated workstation for implementing the proposed algorithm. we've used Eclipse for Java and HTML programming and SQLyog for database respectively. Then the setup was tested severally.

4.2. Proposed Design

The cloud may be a server-client model and therefore the server system consists of agent module, security module, analysis module and database. Though the traditional cloud model has single encryption and decryption process, the proposed cloud security model has double encryption and decryption model (see Fig. 3). inside the security module, the content manager brings the cloud contents double encryption processes (Encryption I and Encryption II).

The Encryption-I is usually provided by all cloud architecture and produces Ciphertext-I, the proposed Encryption-2 is an attachment based on the architecture in paper [9] to secure the cloud data by generating a random key and convert the Ciphertext -1 into Ciphertext -2. The randomly generated key's unknown to the content manager too. In the client side, the decrypt processor has two decryption processes (Decryption-l and Decryption-2) and one content player. The proposed Decryption-I is decrypted by some random key and convert that ciphertext-2 into ciphertext-1. The Decryption-2 then finally converts the ciphertext-1 to multimedia contents using symmetric key. Without the randomly generated key, the Decryption-I process is difficult and thus the proposed architecture gives efficient security. The Encryption-2 and the Decryption-I process is based on the random key generation shown by the origin color in the system server and the client in Fig. 3.

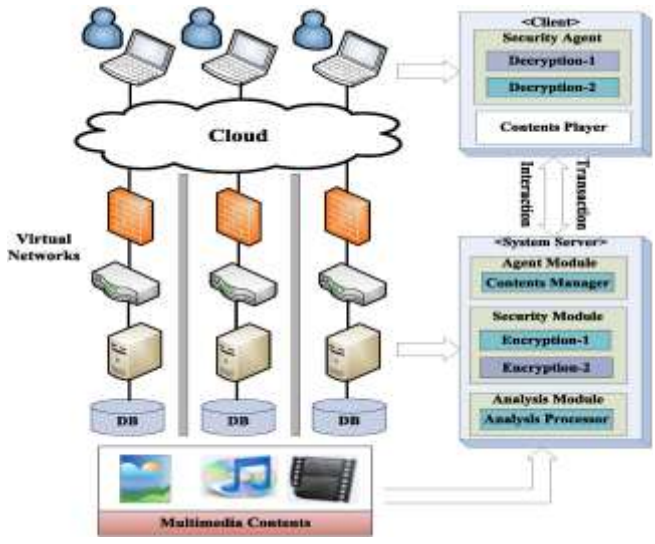


Figure 3: Proposed Architecture

4.3. Encryption and Decryption in RSA

While encrypting the multimedia data into ciphertext, the ciphertext-1 has been stored into a file. Second pass encryption is used to generate the ciphertext-2. When the ciphertext -1 is generated, a randomly generated asymmetric key has been used for the encryption. Then the encrypted data is stored in the cloud. In cloud computing, grabbing the user data from attackers may be a difficult task. This paper is to improve the security of the multimedia user data.

4.3.1. Encryption Process

In the first encryption process (see fig 4), the multimedia data is converted into ciphertext-1 using public asymmetric key and a random prime number (p) is chosen. The ciphertexts are read character by character. In each pass a single character (n) is multiplied with the prime and converted the result into (m) the 94-bit format. The converted value is then stored in the cloud. A separator is then added with that value. The 94-bit format is that the set of printable character having the ASCII value from 33 to 126. To prevent from generating subsequent prime location from out of range, the prime (p) is mod by the character (n) and stored the result as (s). The location of subsequent random prime is that the lower index of the mod result (s). A prime array is employed to get the random prime.

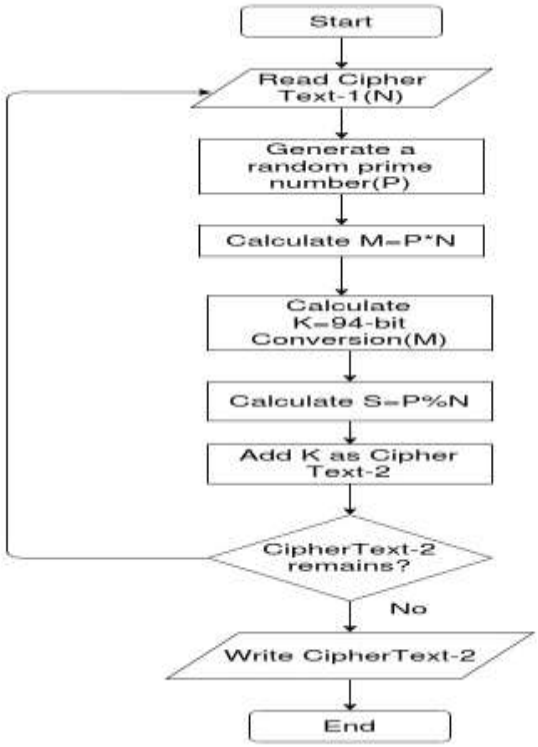


Figure 4: Flowchart of Encryption Process

On the second pass the prime array is rearranged by moving the prime onto the primary location of the array. The procedure ensures that selected prime is usually random. With every pass of the encryption process the separators are programmatically generated which will help to seek out 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 within the pseudo code. The pseudo code takes a string as input and processes the string consistent with the encryption algorithm. Then the string is converted into ciphertext-2 and stored within 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 cipertext

7 s := p mod n

8 p := s-1

9 end

4.3.2. Decryption Process

In the decryption process (see Fig. 5) at first, the cipher text reads each character sequentially one after another and add them to the temp (temporary variable) until found the separator. A character out of 94-bit converter behave as a separator. By using that separator a random prime number (p) is regenerated at the time of encryption. After that temp is converted into a decimal value (v). The value is then divided by the prime (p) and regained the specified ciphertext-1 (n). The ciphertext-2 is then stored in the temporary string until the ciphertext- 1 remains.

The final output strings are then written into the targeted file and then the decryption process stops. One more time decryption of ciphertext-1 is done for the second step and the multimedia 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

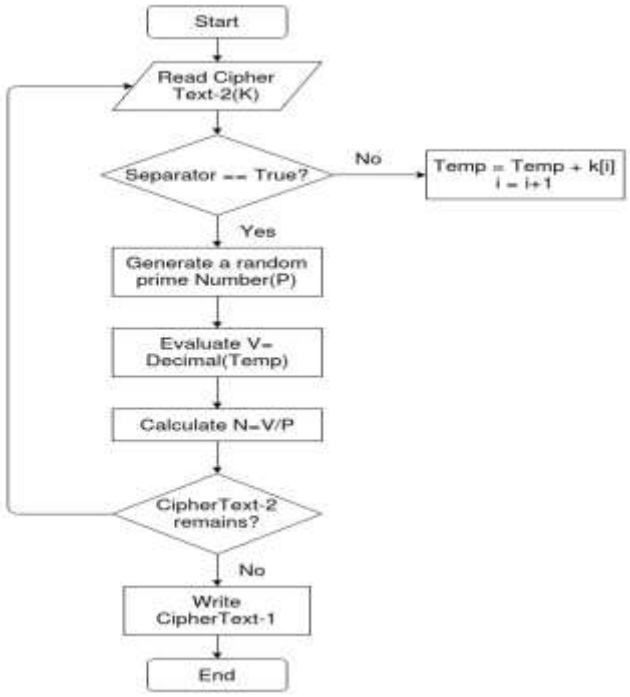


Fig 5: Flow Chart of Decryption Operation

4.4. Encryption and Decryption in Blowfish

The algorithm, Blow fish symmetric block cipher encrypts block data of 64-bits at a time. It will follows the feistel network and this algorithm is split into two parts.

1. Key-expansion

2. Data Encryption

1. 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 generate earlier to any encoding or decryption.

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

Algorithm

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

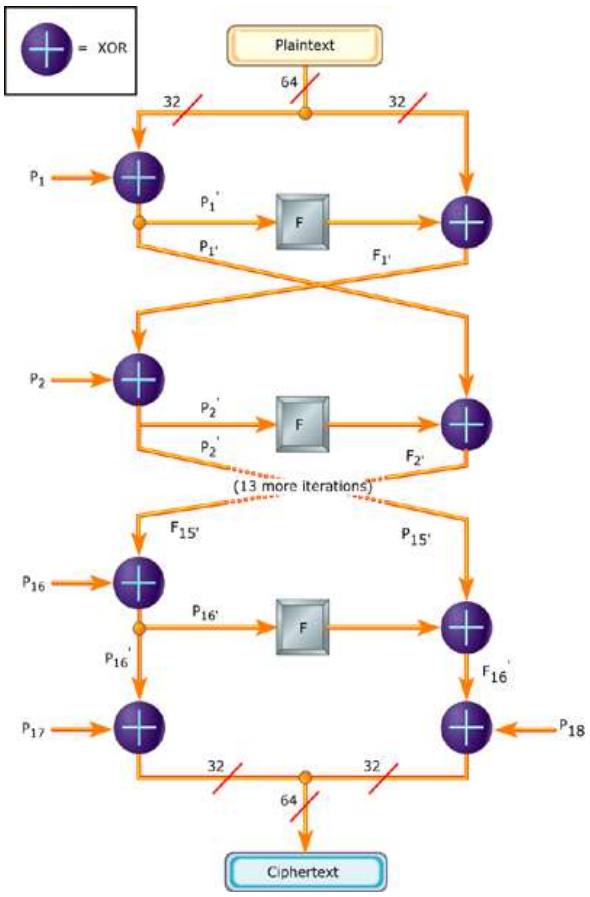
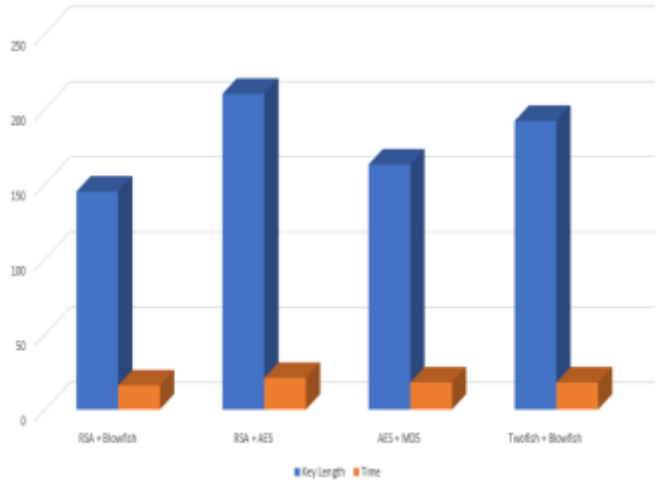


Figure 6: Blowfish Encryption

5. RESULT and ANALYSIS



By comparing the various hybrid algorithms, it is observed that RSA + Blowfish, has taken less time and key length to achieve the security. Hence the project accuracy is 73%.

6. CONCLUSION

This paper represents a double stage encryption algorithm that gives the safety of multimedia contents like image, audio and video within the cloud. The randomly generated key provides more security than the traditional encryption system. The ciphertext is stored within the cloud rather than original multimedia content. The cipher text is difficult to recover the original content for random asymmetric key. Thus, the multimedia content is safe within the cloud. Also, in future we can add a module called Deduplication, which will help in not storing same content files again.

REFERENCES

[1] Associate in Nursing Approach to increased Security of multimedia system information Model Technology supported Cloud Computing Er. Mandeep Singh Sandhu Er. Sunny Singla.

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

[3] Sonal Guleria and DR. Sonia vatta, "To enhance multimedia system security in cloud computing surroundings exploitation Crossbreed rule." International Journal of Application or Innovation in Engineering and Management, vol. 2, half dozen June 2013.

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

[5] C. T. . Huang, Z. Qin, and C. J. Kuo, "Multimedia Storage Security in Cloud Computing: An Overview;" in IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), pp. 1-6, HNA Resort Yungi Hangzhou, China, October 2011.

[6] Modi, D. Patel, B. Borisaniya, A. Patel,, and M. Rajranjan, "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing", The Journal of Supercomputing, vol. 63, no. 2, pp. 561-592, Springer, 2013.

[7] Qin, X. Peng, X. Meng, and W.He, "Improved Known-Plaintext Attack on Optical Encryption based on Double Random Phase Encoding", in Symposium on Photonics and Optoelectronics, pp. 1-4, June 2010.

[8] 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 (INPAC), pp. 146-149, Amravati, India, October 2014.

[9] Md. Habibur, Rahman, Nazrul Islam, Mehdev Hasan Rafsan Jany, Shariful and Mohammad Motiur Rahmant, "Multimedia Content Security with Random Key Generation Approach in Cloud Computing", in IEEE 2017.