IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-6 E-ISSN: 2347-2693

Securing Data Transmission in Cloud using Encryption Algorithms

Anjali Nigam[1*], Vineet Singh[2]

[1,2]*Department of Computer Science and Engineering, Amity University, U.P., India*

www.ijcseonline.org

Received: May/26/2016 Revised: Jun/06/2016 Accepted: Jun/18/2016 Published: Jun/30/ 2016

***Abstract*—** Cloud computing provides an overwhelmingly versatile and flexible processing to associations that is accessible on interest. It lets enterprises to be fast, adaptable and ready to react quickly to the dynamic business situations. As cloud computing offers many advantages, it also has numerous security issues. The quantity of information exchanged over cloud is quite unsafe. The encryption specifications such as AES (Advanced Encryption Scheme), DES (Data Encryption Scheme), and 3DES (Triple Data Encryption Scheme) are widely used to solve such issues. But with the advancement in tools, these algorithms do not seem to be speedy and secure enough. In this paper we propose an encryption technique using two symmetric cryptography algorithms which supplies security to both the original file and the secret pass-code. The message to be sent is encrypted and decrypted using the AES algorithm. 3DES is used for encrypting and decrypting the secret key which encrypts the actual data to be transmitted.

***Keywords*—** AES; 3DES; Cloud Security; Data Transmission; Encryption; Decryption.

I. INTRODUCTION

Cloud computing is the deliverance of on-demand computing resources on a pay-for-use basis over the Internet. It furnishes clients with various capacities to store and process their information in third party data centers. Internet is the correspondence system for cloud clients to exchange their information. A crucial part of cloud computing is to give secure and effective transmission of information [1]. This correspondence between the client and server goes through the network where it can be misused [2]. To secure the transmission several encryption techniques are available. Encryption is one of the primary ways to promise the safekeeping of delicate data. An encryption algorithm applies a variety of operations on the plaintext and re-constructs it into cipher text.

Encryption techniques can be divided into two categories: Symmetric key and Asymmetric key. In Symmetric key, encryption and decryption are accomplished by using the identical key (secret key encryption). Whereas in Asymmetric key, encryption and decryption are accomplished by using two dissimilar keys – first is a public key and second is a private key (public key encryption) [3]. A Key can be constructed by the mixture of alpha numeric, numeric or special symbols. It is applied when encryption happens on the plain text and decryption happens on the cipher text.

Asymmetric algorithms are around 1000 times slower than the symmetric ones. That is why instead of using one symmetric and other asymmetric or both asymmetric algorithms, a technique using two symmetric cryptography algorithms has been proposed. They provide security to both the message and the secret key. The actual message to be transmitted is encrypted and decrypted using the AES algorithm. The secret key used in the encryption of the actual data, is encrypted and decrypted using 3DES.

By bringing together these techniques, this approach offers a solution for various weaknesses including:

- Key encryption management: key generator and key transmission.
- Data confidentiality: using Advanced Encryption Standard (AES). It has the fastest speed than other techniques and provides an excellent security.

Section 2 of this paper gives a brief about the theoretical background of the proposed framework. In section 3, the works of other scholars are summarised. In section 4 and section 5, we have explained our proposed framework and its simulation and results in detail respectively. Finally, section 6 concludes this paper.

The figure below shows the categorization of the cryptographic techniques and the type of keys they use.

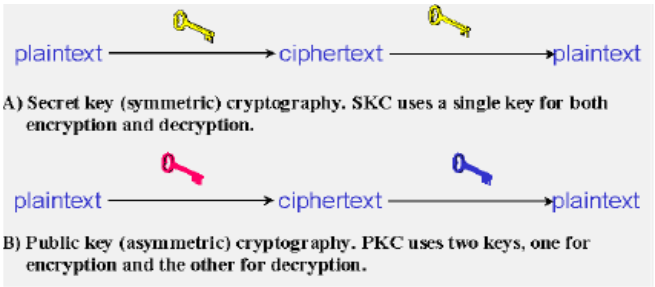

Fig. 1: Cryptographic Techniques based on the types of Keys Used [3]

II. THEORETICAL BACKGROUND

A. *Advanced Encryption Standard*

After the name of its two cryptographers, Vincent Rijmen and Joan Daeman, AES is also known as Rijndael. It is a symmetric key algorithm and was first published in 1998.

After the recommendation of NIST, it replaced DES in 2001 as the specification for the encryption of electronic information. AES can sustain lengths of key of 128, 192 and 256 bits and any permutation of 128 bits data. Depending on the key lengths, it is subjected to as AES-128, AES-192 and AES-256 respectively. For the cryptographic process, AES takes 10 rounds for I28-bit key, 12 rounds for I92-bit key and 14 rounds for 256-bit key for providing the resulting cipher-text or to recover the original plain-text. In AES, 128 bit data is separated into four procedural blocks which are structured as a 4×4 order of matrix called the state [4].

Every round of AES constitutes the subsequent transfigurations [5]:

- Substitute Byte transformation- Using an 8-bit Rijndael S-box, each byte of a data block is substituted into a new block.
- Shift Rows transformation- Cyclical shift is performed on the bytes of the state at the last three rows. For the 2^{nd}, 3^{rd} and 4^{th} row, 1 byte, 2 byte and 3 byte circular left shifts are applied correspondingly.
- Mix columns transformation- Matrix multiplication is done with every state column with a fixed matrix. Rather than numbers, the bytes are considered as polynomials.
- Add Round Key transformation- Bitwise XOR operation is done amid the 128 bits of the round key and 128 bits of the current state.

B. Triple Data Encryption Standard

3DES was created to remove the issues in DES with no requirement of having to design a new encryption system. DES uses a key of 56-bits which is not enough to encrypt delicate information. 3-DES enlarges the size of the key length used in DES by implementing the algorithm thrice with three unlike keys. The size of the key is therefore changed to 168 bits (3 times 56). It entails using DES keys (K1, K2 and K3) in Encrypt-Decrypt-Encrypt (EDE) mode. The plain text is encrypted with K1, then decrypted with K2 and then encrypted yet again with K3 [6]. There are three keying options:

- There could be three keys that are mutually independent ($K1 \neq K2 \neq K3 \neq K1$). It provides key size of $56 \times 3 = 168$ bits. This is the most preferred choice.
- There could be two mutually independent keys. The first and the third keys would be alike ($K3 = K1$ and $K1 \neq K2$). This provides key size of $56 \times 2 = 112$ bits.
- There could be three similar keys ($K1 = K2 = K3$). This alternative is the same as DES Algorithm.

The 3-times iteration increases the encryption level and average time. But it also makes 3DES slower than other encryption algorithms.

III. RELATED WORKS

Shaik et al proposed an algorithm in which they used AES for encrypting their data and RSA for encrypting AES' key [7]. RSA is an asymmetric block cipher encryption algorithm. It utilizes a changeable size encryption block and an inconsistent size key.

Georgiana and Marius use a technique which combines the use of Digital Signature, Hash Functions and AES [8]. They have used RSA for digital signature and MD5 for hash functions. Hash functions are one way cryptographic techniques. Digital signatures are digital codes that are used to authenticate the sender's identity.

Shadma Fazal and B.P.S. Sengar have proposed a way of combining encryption algorithms with steganographic algorithms [9]. Steganography is the study of hiding the data without leaving a remarkable trace in order to prevent hackers from detecting the presence of the data. This is done by camouflaging the secret message with a carrier data.

Mahavir and Arpit have proposed a hybrid cryptographic algorithm by using two block cipher encryptions namely Data Encryption Scheme (DES) and International Data Encryption Algorithm (IDEA) [10]. IDEA operates with 64-bits blocks and is controlled by a 128-bit key.

Nagendra e. al proposed a way to access and secure data storage in private cloud with the help of digital signature [11]. Digital signatures are generated and validated by asymmetric encryptions. They are enclosed with an electronically transmitted document.

Prof. S.N. Ghosh et al designed a hybrid AES-DES-RSA algorithm for securing information. The key exchange mechanism has been done using RSA [12]. AES and DES are symmetric algorithms whereas RSA is an asymmetric algorithm.

Aayasha and Deepti presented a way of securing data transmission by combining genetic algorithm, steganography technique and visual cryptography technique [13]. Genetic algorithms are evolutionary algorithms based on the concept of natural selection. It has proven to be a dependable and potent optimization technique. In visual cryptography a secret image is divided into several parts called shares. These shares separately do not reveal any information but only by stacking them together, secret image can be discovered.

Rachna Jain, Sushila Madan and Bindu Garg examined different techniques to secure data access in cloud environment and detected that security needs to be addressed for securing transaction in such a way that transaction should be encrypted and not be decrypted during access [14].

IV. PROPOSED FRAMEWORK

The file to be transmitted is encrypted using AES-256 along with a random Salt and IV generator. Former enhances the security of the key while the latter enhances the security of each message encrypted with that key. They both must be kept safe. Salt is a random value which is quite small in size

and used as an additional input that hashes a password. As people have a tendency to use the same passwords, salt's primary function is to guard against pre-computed rainbow table attacks and dictionary attacks. Salt makes the common passwords uncommon. A random new salt is originated every time for every password. Typically, the salt and the password are concatenated and the resultant output but not the original pass-code is saved along with the salt. Initialization Vector (IV) is a random fixed size input that makes the same plain text produce different cipher texts. An XOR operation is performed between the IV and the first 16 bytes of the file to be encrypted. IV hides the patterns in the messages.

A. The Encryption Process

The encryption process begins with the key generation process at the sender's side. The sender generates two keys (K1 and K2). K1 is used by the sender to encrypt the original file. The sender then uses K2 and encrypts K1+Salt+IV using 3DES. He then sends the encrypted file and K1 to the receiver. The receiver first decrypts K1 using 3DES with K2 and then decrypts the original file using AES with K1. K1 must be decrypted first because the encrypted data can only be decrypted with the original secret key. Once the secret key is decrypted it is then used in the AES algorithm to get back the original message.

In our proposed framework we are sending the original encrypted file, Salt and key to the receiver via different ports. So even if one port gets attacked and a particular data is lost, the attacker would not be able to decrypt the original file and make use of the sensitive information in an inappropriate or illegal way. In the below figure, it is shown how are our proposed framework works and how the data is sent from one client to another.

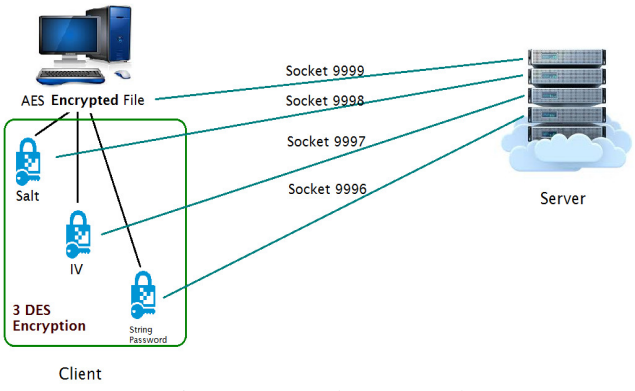

Fig. 2: Proposed Framework

B. Encryption Algorithm

Figure 3 shows the steps of the proposed encryption process. It involves the following:

Step 1: Select the file to be transmitted. It could be of any type i.e. audio, image, video, word, pdf, txt, etc.

Step 2: Enter the secret key for AES Encryption (K1) of the chosen file. This step results into the creation of Salt, IV and txt file of key of the encrypted file.

Step 3: Enter the secret key for 3DES (K2) encryption of the K1+Salt+IV.

Step 4: Send the encrypted files to the receiver.

Step 5: Receiver enters K2 for decrypting K1+Salt+IV.

Step 6: Receiver enters K1 for decrypting the original file.

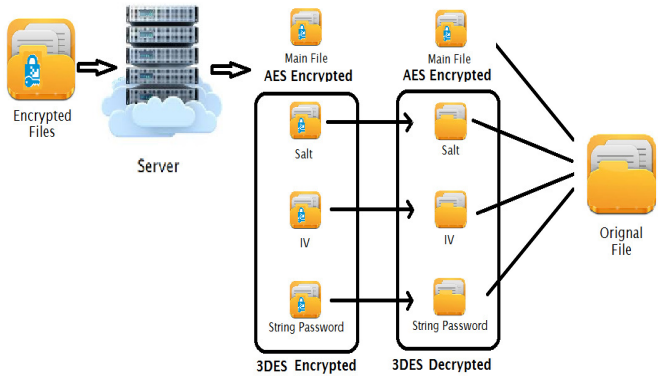

Fig. 3: Steps of the Encryption Process

V. SIMULATION AND RESULT

The proposed work was developed on Netbeans IDE 8.1. Language used is Java. Below is a table that shows the features of the AES and 3DES algorithms used in our framework:

	AES	DES
Block size	128	64
Key Size	256	168
Rounds	14	48

Table 1: Characteristics of AES and 3DES

Table 2 below records the encryption/decryption runtime of AES which is used in encrypting the actual file. Runtime is measured in milliseconds.

File Size in Bits	AES Encryption Runtime	AES Decryption Runtime
76432	0.329	0.295
181863	0.337	0.302
450560	0.345	0.309
851968	0.385	0.338
Average Time	0.349	0.311

Table 2: Performance Evaluation In terms of Runtime

Below are some of the screen shots of our project. Fig. 4 shows the main interface. The user can choose any file like

image, audio, video or text files. The main interface includes two tabs: one for AES encryption and the other for key wrapping i.e. 3DES encryption. The user can enter the secret keys for AES and 3DES according to his/her choice. After the encryption procedure is done, the sender then sends the encrypted main file, salt, IV and key to the receiver's side. The main interface also contains the drop down lists namely File, Help and About. In the file section options such as save file and select file are given. Help list assists the clients to use the framework in an easy manner. About list tells our users the details about this model such as language used, types of encryption algorithms used and their estimated output.

The files are then received by the receiver. He can then enter the secret keys for 3DES and AES and decrypt the AES' key and the original file respectively. Figure 5 and 6 below shows the screen shots at the receiver's side.

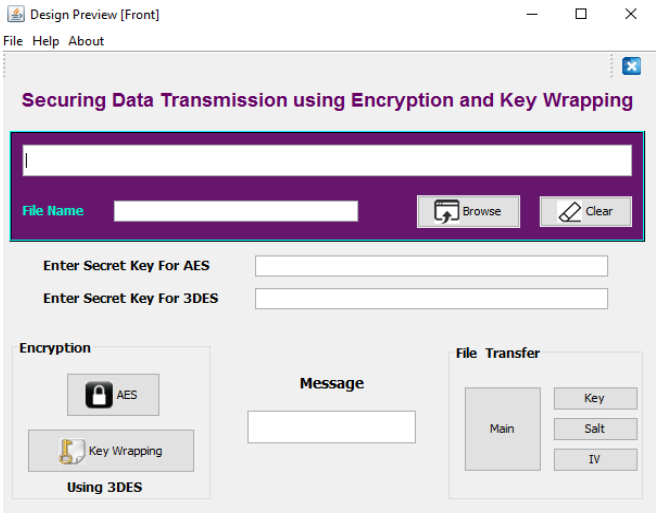

Fig. 4: Main Interface

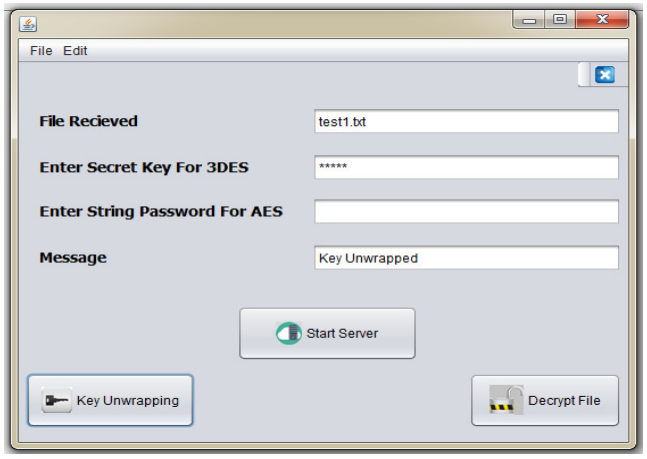

Fig. 5: Decrypting AES Secret Key

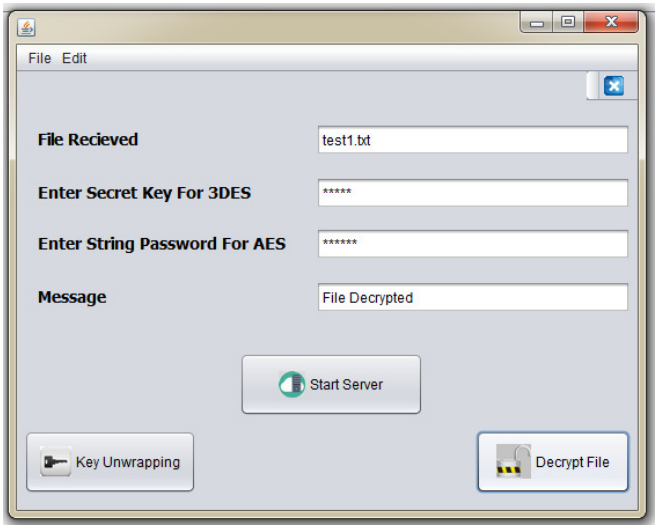

Fig. 6: Decrypting the original file

AES Key Used- 79DD1B81EA2A3C18C1695349491EB. Figure 7 and figure 8 below represents the AES key in Plain text and Cipher text respectively.

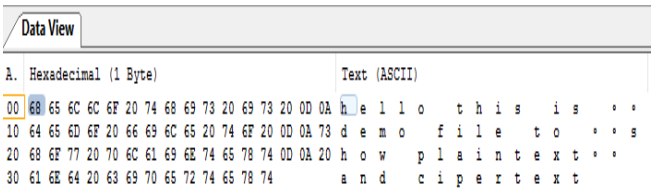

Fig. 7: AES Key in Plaintext

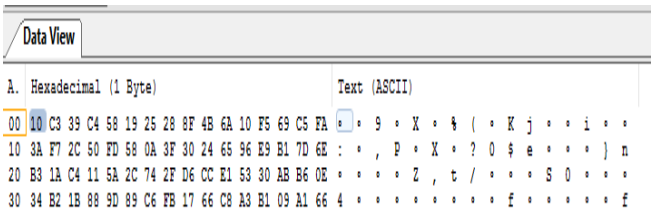

Fig. 8: AES Key in Cipher Text

3DES Key used for AES key's encryption- A64E58D45CE528B3197FFBCB11CBF

After 3DES Encryption, AES key turns into- "››xµ'©R†°ä{:ø_÷5"n‡_#{Áö9ÆÅõ^alb@g¶Õ"

VI. CONCLUSION

Cloud environment is a huge help to the IT world and also to singular customers. It is important to consider protection and anonymity when utilizing and planning for cloud computing services. The model proposed in this paper provides a way of defending the data by introducing an encryption technique. It achieves the availability, reliability and

integrity of data traversing through client to cloud and cloud to client. The data while in transmission over an internet network can be attacked by a variety of illegal interceptors. Using today's technology, it is not tricky to fracture this network by crunching large number combinations speedily in order to find out every feasible key. This attempt is known as a brute force attack. In the proposed model we are using 256 bit AES encryption and 168 bit 3DES encryption which is sufficient to make a brute force attack generally unsuccessful. The processing power required, among other things, would render most attacks futile. Hence, this approach not only defends the data where it resides, but also helps guarantee the customers that data is safe and sound while in transit.

REFERENCES

[1] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, ISBN: **978-0-7695-4456-4**, October **2011**.

[2] Anjali Nigam and Vineet Singh, 'A Study on Data Transmission Security Threats in Cloud', International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): **2320-9798**, Volume **4**, Issue **5**, May **2016**.

[3] Sadiya Shakil and Vineet Singh, 'Security of Personal Data on Internet of Things using Cryptographic Algorithm', International Journal of Engineering Science and Computing, ISSN: **2321-3361**, Volume **6**, Issue **4**, April **2016**.

[4] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, 'Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System', International Journal of Multidisciplinary Research, pp. **143-151**, Volume **1**, Issue **4**, August **2011**.

[5] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, 'Performance Evaluation of Cryptographic Algorithms: DES and AES', Conference on Electrical, Electronics and Computer Science, ISBN: **978-1-4673-1516-6**, Page No. (**1-5**), March **1-2, 2012**.

[6] Supriya and Gurpreet Singh, 'A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security', International Journal of Computer Applications (**pp. 0975-8887**), Volume **67**, Issue **19**, April **2013**.

[7] Shaik Rasool, G. Sridhar, K. Hemanth Kumar and P. Ravi Kumar, 'Enhanced Secure Algorithm For Message Communication', International Journal of Network Security & Its Applications, Volume **3**, No. **5**, Sep **2011**.

[8] Georgiana Mateescu and Marius Vladescu, 'A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques', Proceedings of the Federated Conference on Computer Science and Information Systems, pp. **659–662**, **2013.**

[9] Shadma Fazal and B.P.S. Sengar, 'Data Transmission Security Technique Using Encryption/Decryption and Steganographic Algorithms', International Journal of Advanced Technology & Engineering Research, ISSN No: **2250-3536**, Volume **4**, Issue **4**, July **2014**.

[10] Mahavir Jain and Arpit Agarwal. 'Implementation Of Hybrid Cryptography Algorithm', International Journal Of Core Engineering & Management (IJCEM), ISSN: **2348 9510**, Volume **1**, Issue **3**, June **2014**.

[11] Nagendra Kumar, Ashok Verma and Ajay Lala, 'Access, Identity and Secure Data Storage in Private Cloud using Digital Signature', International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): **2320-9798**, Volume **2**, Issue **3**, March **2014**.

[12] Prof. S. N. Ghosh, Deepak T. Biradar, Ganesh C. Shinde, Sarika D. Bhojane and Manojkumar R. Shirapure, 'Performance Analysis of AES, DES, RSA And AES-DES-RSA Hybrid Algorithm for Data Security', International Journal of Innovative and Emerging Research in Engineering, ISSN: **2394-5494**, Volume **2**, Issue **5**, May **2015**.

[13] Aayasha Kausar and Deepty Dubey, 'Secure Data Transmission by Combining Genetic Algorithm and Steganography Techniques with Visual Cryptography Technique', International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Print): **2320-9798**, Volume **3**, Issue **11**, November **2015**.

[14] Rachna Jain, Sushila Madan and Bindu Garg, 'Analyzing Various Existing Security Techniques to Secure Data Access in Cloud Environment', International Journal of Computer Sciences and Engineering, E-ISSN: **2347-2693**, Volume **3**, Issue **1**, January **2015**.

Authors Profile

Anjali Nigam is an M.Tech Student in Amity University, Department of Computer Science and Engineering, Lucknow, Uttar Pradesh, India. She persued B.Tech in Information Technology from Amity University in 2013.

Vineet Singh is an Assistant Professor in the Department of Computer Science and Engineering in Amity University, Lucknow, Uttar Pradesh, India.

