Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing

Mohammad Ubaidullah Bokhari
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, India

Qahtan Makki Shallal
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, India

ABSTRACT

The technology of Cloud computing is permit the subscribers to store their own data in its infrastructure. The subscribers will be able to use their stored data whenever they required. Since the data are stored outside their boundary, it needs to use a strong encryption during transmission process to be protected well. Thus, in this paper we have proposed a model to use a hybrid encryption and decryption process based on AES-128 and RSA algorithm. Furthermore, we used HMAC algorithm to ensure the integrity and authenticity of data. Our experiment work has been done to explain the time required, throughput and memory utilization for encryption and decryption based on different size of files.

Keywords

Advanced Encryption Standard (AES-128), RSA, hash based message authentication code (HMAC).

1. INTRODUCTION

The cloud computing security has become the most important problems in its growth. It has a huge interactions number of data between the platform of cloud computing and user [1]. In the process of data transmission, the data which transfer between the users and cloud computing could possibly be intercepted [2], it may lead in to leaked of secret data for the enterprise. Data leakage or loss will have a destructive impact on the enterprise. It is not impact on the reputation of enterprise only, but it is cause the customers and partners to lose trust and confidence on the enterprise. Actually the security in cloud have two major aspects: First, the user's data are not going to be leaked to prevent unnecessary losses. Second, it make sure that the user can get his data accurately whenever he required [2][3]. Therefore, we must focus on data in storage and in transmission. When the users are willing to transfer their sensitive data to the cloud, the first step is to encrypted the data, so even if the data interceptors steal the data, then they cannot retrieve the data content as it is encrypted. That is why it make sure that the security of user data during transmission in cloud computing [4].

There are three aspects threats for the data. 1) Security threats, the privacy information could possibly be intercepted by attackers; 2) Integrity threats, data could possibly be altered by attackers; 3) the authenticity of message, to help the cloud to detect whether the message have sent from attacker or authenticated user [5]. In view of such type of threats, we have proposed a strategy to secure the users' data during transmission. It use a technology of double encryption, and combines with the technology of hash-based message authentication code (HMAC) to ensure the data of users are transfer effective safely [6][7][8]. The client generates a value of HMAC and attach it behind the encrypted message by AES algorithm. It ensures the integrity and message authentication of user data. Then the proposed work will use the RSA algorithm to encrypt the secret key of AES to make sure that the secret key of AES is sent safely.

2. INFORMATION ENCRYPTION IN CLOUD COMPUTING

In order to ensure the security of data in entire technology of cloud computing, the service provider and client must encrypt the data. Furthermore, to avoid data leakage and loss the network between the client and cloud must be controlled and protected well. The cloud providers have started to enhance and improve this aspect [9]. The technology of encryption contains two elements: secret key and algorithms. Secret key is just an algorithm which use for encoding and decoding the data. Algorithm is the process of combining the common text with secret key (string of numbers) to produce ambiguous ciphertext. In the process of encryption, through the technology of suitable secret key encryption and proper mechanism of management we can guarantee the security in the communication and Information of the network [10][11]. The Cryptosystem can be divided into two types, which are asymmetric cipher and symmetric cipher. In symmetric encryption the secret key will be same in both processes of encryption and decryption. There are many algorithms of symmetric encryption such as DES, Blowfish, AES, 3DES, … etc. In asymmetric encryption the secret key of encryption will be different of the one which will be used to decrypt. There are many algorithms of asymmetric encryption such as RSA, Diffie-Hellman, …etc [12]. AES algorithm has many advantages such as available as a free for the users, fast processing speed, stronger than 3DES, it can also be used successfully in CPU and memory limited environment, supporting multi size of keys (128, 192, 256) and the entire life is not less than 20 -30 years [13] [14]. The algorithm of RSA does not require to confidential assign a secret key and the secret key security management is very easy [13]. To utilize the full advantage of RSA algorithm and AES algorithm, and avoiding the disadvantages of them, we have used a mix encryption of RSA and AES.

3. PROPOSED MODEL

The basic idea of our proposed model is before the data communication, we encrypt the plaintext by AES algorithm, and then we encrypt the secret key of AES by using RSA algorithm in order to send the secret key of AES safely. Thus, we can use the important advantages of these two algorithms such as the convenience and security of RSA secret key management, and AES high speed encryption [15][16]. Additionally, we have execute HMAC function using the secret key and produced cipher text to attach the produced value at the end of encrypted message in order to send them to cloud server to insure the integrity and authenticity of message [17].

3.1. Details Of Model To Ensuring The Confidentiality, Integrity, Authenticity Of Message In Encryption Process

3.1.1. Ensuring The Confidentiality

In figure.1, we represent the plaintext by P. we assume to use AES-128 algorithm to encrypt the plaintext, so the E_A is the encryption algorithm of AES and K is the secret key of AES. According to the figure.1 the C_P is the cipher text of original plaintext P. the attacker cannot obtain the plaintext without knowing the secret key of encryption algorithm [18]. If the unauthorized interceptors try to brute force the secret key which it is 128 bits, obviously the possible key combinations number is 3.4028237e+38 which will required 1021 years to be cracked using high performance computers which are available nowadays. So, it is impossible to break the key using brute force attack [19].

3.1.2. Transfer The Secret Key

To send the secret key through the internet channel will expose the key to be cracked. So, in our proposed model we suggest to encrypt the secret key by using RSA algorithm. To explain this process we used K_{Er} which is the cloud's RSA public key to encrypt the secret key of AES algorithm K to get the cipher text C_K of AES secret key in sender side to be safely send to receiver side. After that, permit the encrypted secret key of AES algorithm C_K and the encrypted plaintext C_P send to receiver through the internet channel [15].

3.1.3. Ensuring Integrity and Message Authentication

We have mentioned in previous section 3.1.2. that we will send the C_K and C_P through the internet channel just to explain the confidentiality. Furthermore, while we would like to ensure the integrity and message authentication, we suggest to apply HMAC algorithm on the cipher text C_P to produce M1 value and attach it at the end of cipher text C_P and send them as a one message to cloud server. The Hash function which been embedded is adopting the SHA-256 algorithm [18].

3.2. Details Of Model To Ensuring The Confidentiality, Integrity, Authenticity Of Message In Decryption Process

When the cloud server get the message, the first thing would be to use its own RSA private key K_{Es} to get the secret key of AES algorithm K, and then will obtain the new value M2 of HMAC using an obtained secret key and cipher text C_P to check the message authentication and integrity. Then compare the produced value of M2 with received value of M1, if they are identical then the plaintext is integrated and authenticated and must be process by the cloud server to be stored in its data center. Otherwise the plaintext shall be discarded [18] [15] [20].

After ensuring the message authentication and integrity, the process of decrypt the cipher text must be start. To do so, the secret key K and cipher text C_P must be feed into AES algorithm to produce the original plaintext P. Figure.1 is explain the process of encryption both the secret key and plaintext, also explain the process of decryption both the secret key and cipher text.

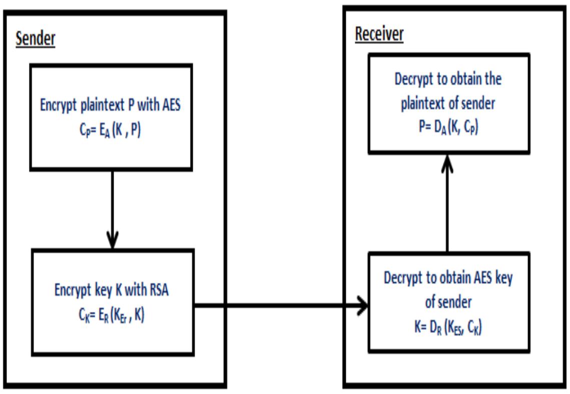
Sender
Encrypt plaintext P with AES
C_P= E_A (K , P)
Encrypt key K with RSA
C_K= E_R (K_{Er} , K)
Receiver
Decrypt to obtain the plaintext of sender
P= D_A(K, C_P)
Decrypt to obtain AES key of sender
K= D_R (K_{ES}, C_K)

Fig 1: Ensure the confidentiality of data

In figure.1 we have used ER, DR to refer for RSA encryption and decryption algorithm respectively, as well as DA to refer for AES decryption algorithm.

The most important things here, when the process of data encryption and decryption has been done successfully, both user and cloud have to remove the trial secret key in order to avoid illegal stealing secret key. Figure.2 is explain the whole process of encryption as well as decryption in our proposed model in both user and cloud server sides. The internet media is refer to the internet channel which may have unauthorized users trying to hack or alter our transferred data.

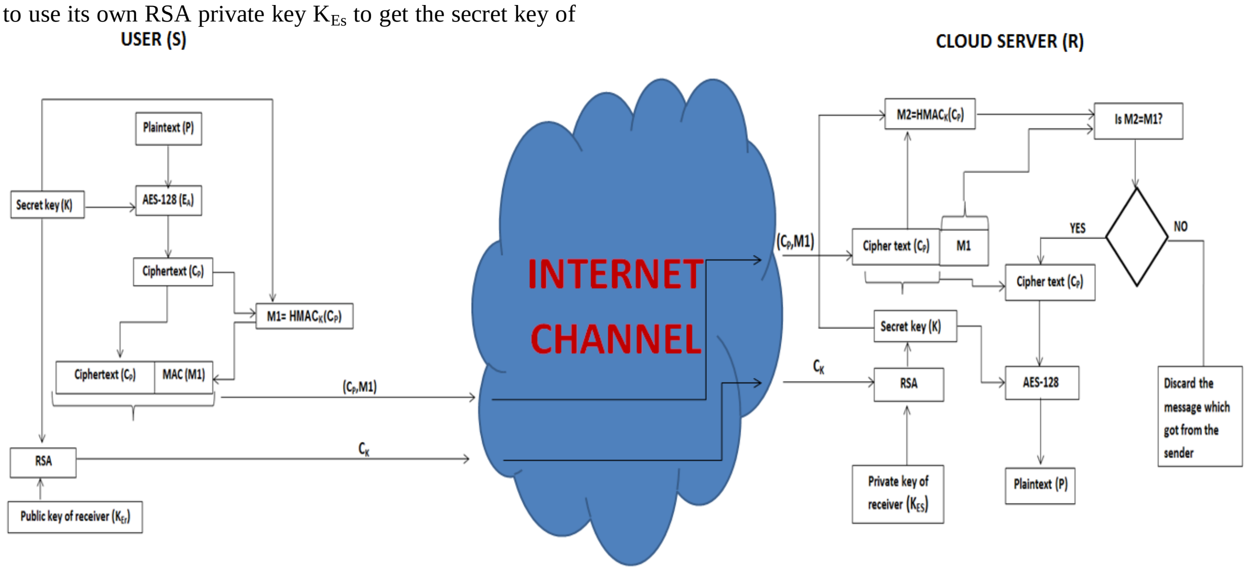

Fig 2: Proposed model which ensure confidentiality, integrity and authentication

4. TEST AND ANALYSIS

All the algorithms has been programmed with MATLAB 7 programming language. The experiment has been done using Dell laptop which having windows 8 as operating system, processor type is Intel Core i7 5th Gen, the speed of processor is 3.00GHz and RAM is 8 GB.

4.1. The Encryption And Decryption Time

The proposed model is implemented on the different size of data ranging from 100 KB to 50 MB. The table below is showing the required time for the process of encryption as well as decryption.

Table I. The required time for encryption and decryption

File Size	Time required for encryption	Time required for decryption
100 KB	21 ms	16 ms
500 KB	73 ms	58 ms
1024 KB	150 ms	122 ms
2048 KB	173 ms	151 ms
5120 KB	210 ms	193 ms
10240 KB	421 ms	394 ms
51200 KB	1220 ms	1110 ms
Avarage data rate KB/ms	17.278	19.353
Throughput KB/ms	30.966	34.360

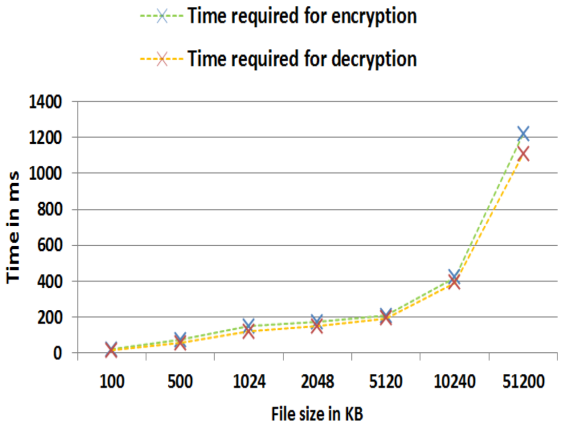

Fig 3: Encryption and decryption time consumption

The value of throughput for encryption as well as decryption in KB/ms has been calculated according to the following formula [21][22]:

$$Throughput = \frac{Total\ size\ of\ plaintext\ in\ KB}{Total\ encryption\ or\ decryption\ time\ in\ ms}$$

Also, average data rate for encryption and decryption process in KB/ms has been calculated according to the following formula [21][22]:

$$Average\ data\ rate\ of\ encryption/decryption = \frac{1}{Nf}\sum_{n=1}^{Nf}\frac{Mi}{TMi}$$

Where, Nf is the number of file which we used to encrypt or decrypt, Mi is the file size in KB, TMi is the time required to do encryption or decryption in millisecond.

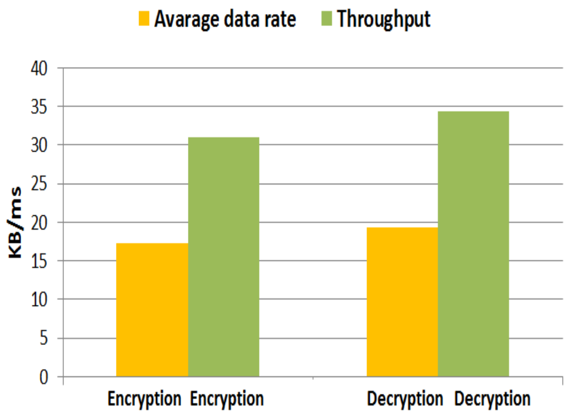

Fig 4: Throughput and average data rate for both encryption and decryption

4.2. The Memory Utilization

The memory utilization is an important parameter for the performance. The figure.5 and table II. below is showing the parameter of memory utilization in our proposed model based on different size of files.

Table II. The memory utilization in encryption and decryption process.

File Size in KB	Memory utilization in MB for encryption	Memory utilization in MB for decryption
100	4.1	3.5
500	10.05	8.9
1024	21.3	19.6
2048	32.5	29.7
5120	46.1	42.2
10240	73.7	66.02
51200	284.2	251.3

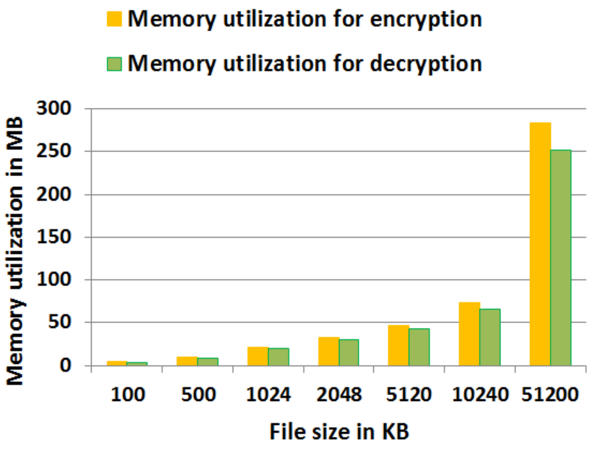

Fig 5: Memory utilization for encryption and decryption

It is easily to observe that whenever the size of file is increased, it will result to increase the memory utilization. That mean we will need a good memory to be attached to our system in case we have a large size of files.

5. CONCLUSION

In this paper, we have suggested a mechanism of hybrid encryption and decryption based on AES-128 bits algorithm to encrypt the original plaintext and then encrypt the secret key of AES by RSA algorithm. Furthermore, we used the value which produced by HMAC algorithm and attached in the end of encrypted plaintext to check the integrity and authenticity of message. The results of experiment shows the time required for encryption and decryption different size of data started from 100 KB up to 51200 KB. Moreover, the memory utilization has been measured for different size of files.

6. REFERENCES

[1] Hashem, Ibrahim Abaker Targio, et al. "The rise of “big data” on cloud computing: Review and open research issues." Information Systems 47 (2015): 98-115.

[2] Alneyadi, Sultan, Elankayer Sithirasenan, and Vallipuram Muthukkumarasamy. "A Survey on Data Leakage Prevention Systems."Journal of Network and Computer Applications (2016).

[3] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on 62.2 (2013): 362-375.

[4] Mulazzani, Martin. New challenges in digital forensics: online storage and anonymous communication. Diss. Vienna University of Technology, 2014.

[5] Ahmed, Usama, et al. "Modelling cyber security for software-defined networks those grow strong when exposed to threats." Journal of Reliable Intelligent Environments 1.2-4 (2015): 123-146.

[6] Liu, Bin, and Bevan M. Baas. "Parallel AES encryption engines for many-core processor arrays." Computers, IEEE Transactions on 62.3 (2013): 536-547.

[7] Goshwe, Nentawe Y. "Data encryption and decryption using RSA Algorithm in a Network Environment." International Journal of Computer Science and Network Security (IJCSNS) 13.7 (2013): 9.

[8] Arasu, S. Ezhil, B. Gowri, and S. Ananthi. "Privacy-preserving public auditing in cloud using HMAC algorithm." International Journal of Recent Technology and Engineering (IJRTE) ISSN (2013): 2277-3878.

[9] Mu, Shuai, et al. "Cloud Storage over Multiple Data Centers." Handbook on Data Centers. Springer New York, 2015. 691-725.

[10] Basu, Sanjay. Modified Playfair Cipher with Rectangular Matrix. Diss. JADAVPUR UNIVERSITY, 2012.

[11] Schreck, Jörg. Security and privacy in user modeling. Vol. 2. Springer Science & Business Media, 2013.

[12] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications 67.19 (2013).

[13] Kapur, Raj Kamal, and Sunil Kumar Khatri. "Secure data transfer in MANET using symmetric and asymmetric cryptography." Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on. IEEE, 2015.

[14] Dubrawsky, Ido. How to cheat at securing your network. Syngress, 2011.

[15] Rege, Komal, et al. "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA." International Journal of Computer Applications 71.22 (2013).

[16] Chandra, Sourabh, et al. "A comparative survey of symmetric and asymmetric key cryptography." Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference on. IEEE, 2014.

[17] Crocker, Paul, and Pedro Querido. "Two Factor Encryption in Cloud Storage Providers Using Hardware Tokens." 2015 IEEE Globecom Workshops (GC Wkshps). IEEE, 2015.

[18] C. Xue-zhou, “Network Data Encryption Strategy for Cloud Computing,” 2015.

[19] Rajput, Somesh Kumar, and Anuradha Konidena. "PERFORMANCE ENHANCEMENT IN IMAGE ENCRYPTION USING AES." (2015).

[20] Zhu, Xiaoyan, et al. "Efficient privacy-preserving authentication for vehicular ad hoc networks." Vehicular Technology, IEEE Transactions on 63.2 (2014): 907-919.

[21] K. M. Anand and S. Karthikeyan, “Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms”, International Journal of Computer Networks and Information Security, vol. 2, pp. 22-28, 2012.

[22] A. K. B and P. A. A, “A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development,” vol. 5, no. 10, pp. 804–811, 2014.