International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 2, Issue 10, pp 28-32, December-2018

The Secure Data Transmission in Cloud Computing By Using Encryption Techniques AES and RSA

Nampalli Radhika

Assistant Professor, Department of Computer Science And Engineering, Malla Reddy College of Engineering for Women, Hyderabad -500100, Telangana, India

Abstract - Security threats in cloud computing have still raised concerns for companies and individuals. So, most researches have raced to propose models that keep secure data transmission in cloud computing and have ensured stored data privacy by adopting appropriate encryption algorithms. This research presents a hybrid proposed scheme by combining the RSA and AES to get features of both of them. The encryption process is achieved by using a proposed algorithm depending on the XOR factor and AES algorithm. The AES algorithm security has been increased by generating a dynamic key and maintains the security of this key with two encryption levels using the RSA algorithm so that each level provides the authentication and verification requirements for both the transmitter and the receiver. The results of the implementation of this scheme have proved its ability to achieve the security requirements of cloud computing at the least possible execution times so that the execution time in the transmitter's side is (34.91, 36.1, 41.4, 43.26) ms for various file sizes (50,100,150,200) KB respectively. The results also showed superiority in terms of requirements of security, and execution time over well-studied reference models.

Keywords: Authentication and Verification, Data Security, Data Privacy, Data Confidentiality, Hybrid Encryption, Security Issues.

1. INTRODUCTION

There have been many means of networked computing, and the most prominent of these means is the cloud computing system that provides cloud storage, messaging between users, and access to numerous volumes of information in multiple fields. However, the issue of confidentiality and privacy of data storage remains the primary concern for any networked computer interaction, whether it is in the cloud computing system or other networked computer systems. Reference studies have diversified in the area of support confidentiality data, integrity, and authentication in cloud computing. Some of them discussed security requirements in cloud computing. For instance, Khan and Sharma (2019) have studied the security requirements in cloud computing and have proposed using symmetric and asymmetric encryption algorithms to keep data secure. In addition, they have assured the importance of using the symmetric AES (Advanced Encryption Standard) algorithm to encrypt data for its speed and flexibility.

Several reference studies have discussed the security challenges of cloud computing, and they have been defined security requirements for data transfer and storage in cloud computing to ensure its integrity, confidentiality, and authentication (Fatima and Ahmad, 2019; Ghaffari et al., 2019; San et al., 2019; Tabrizchi and Rafsanjani, 2020; Yahya et al., 2019; Sakharkar,2019). So to keep the data secure that are stored in the cloud, Sakharkar (2019) discussed security threats in cloud computing and compared the most effective algorithms for keep data secure at the cloud computing. It was found that it is necessary to apply multilevel security to ensure data security in cloud computing.

The most recent research has tended to combine the symmetric and asymmetric cryptographies to benefit from the rapidity of one and the security of the other to achieve an integrated security model for cloud computing. Such as Zou et al. (2020) have proposed a hybrid encryption algorithm AES and RSA (Rivest-Shamir-Adleman) that combining the advantages of the two algorithms, have made full use of the speed in encryption and decryption of the AES algorithm and key management advantage of the RSA algorithm.

2. PROPOSED REFERENCE MODELS FOR THE CLOUD COMPUTING

Many researchers have studied hybrid model AES and RSA in order to achieve higher data confidentiality and get security requirements in cloud computing. We have reviewed some of the above, but we will study the following studies for their modernity in order to compare their results with the results that we will get from our proposed model in this paper in terms of security requirements of cloud computing and execution time.

2.1. The first studied reference model (Khaing and Naung, 2019)

Researchers Khaing and Naung (2019) have proposed a system to protect data transferred to the cloud by combining the RSA and AES algorithms. They have proposed generating an AES key randomly, and then encrypting it using the RSA algorithm with the public key of the receiver, and then merging encrypted data file by the AES algorithm with the key file encrypted by RSA algorithm to get the output file that is sent to the receiver. Then, this file is separated into two files at the receiver's side. The first file is the encrypted data file and the second file is the encrypted key file. After that, the encrypted key file is decrypted using the RSA algorithm with the private key of the receiver to get the secret key for the AES algorithm, whereby the encrypted data is decrypted with the AES algorithm.

2.2. The second studied reference model (Malgari et al., 2020)

Malgari et al. (2020) have proposed a hybrid encryption model that combines the symmetric AES algorithm and the asymmetric RSA algorithm in order to take advantage of them. Thus, they have avoided the key management problem in the AES algorithm, where the AES secret key is decrypted using the private key of the recipient, and their model has achieved higher secrecy for sensitive data that requires higher secrecy but has taken a longer execution time.

3. SECURITY REQUIREMENTS

There are many security requirements in cloud computing and they differ from one reference to another and from one organization to another, it can be summarized with the following requirements (Fatima according to Ahmad, 2019; Ghafari et al., 2019; San et al., 2019; Tabrizsch and Rafsanjani, 2020; Yahya et al., 2019):

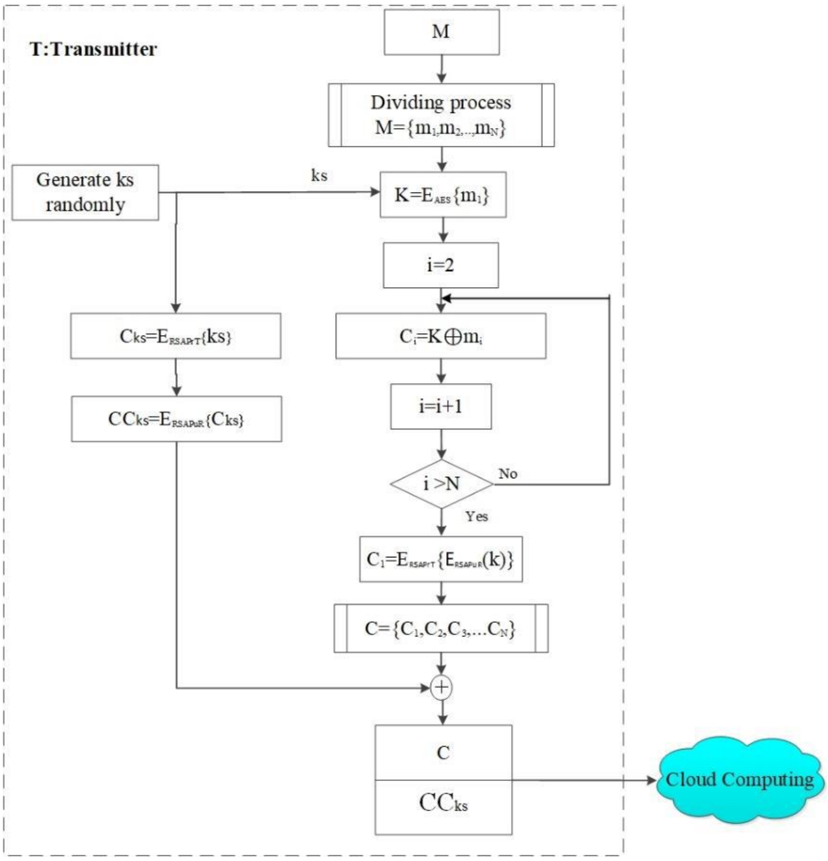

Figure -1: The hybrid proposed model by combining RSA and AES in the transmitter's side

1-Confidentiality: The concept of confidentiality includes more than one approach and can be summarized in the following three aspects:

- Cloud computing data, whether stored or transmitted, is not disclosed to non-cloud users.
- The correspondence between two particular cloud users is not disclosed to the other Cloud users.

- The data of any cloud user is only disclosed to him and not to anyone else.

The first concept of confidentiality can be achieved by using symmetric algorithms such as the AES algorithm, which has a high speed of implementation Mohan et al. (2020). However, these algorithms have fallen short of achieving the other two concepts because all users have shared a secret key, but asymmetric algorithms have achieved the other two concepts, such as the RSA except it has slow implementation when compared with symmetric algorithms Al- Kaabi, and Belhaouari (2019). 2-Privacy and Integrity: The concept of privacy data refers to the application of laws, standards, policies, and processes by which personal information is managed. On the other hand, integrity refers to protecting cloud data and software from unauthorized deletion, modification, theft, or fabrication. This ensures that data have not been tampered with or abused. Integrity includes data accuracy and completeness. The concept of data privacy and integrity includes two main aspects, namely:

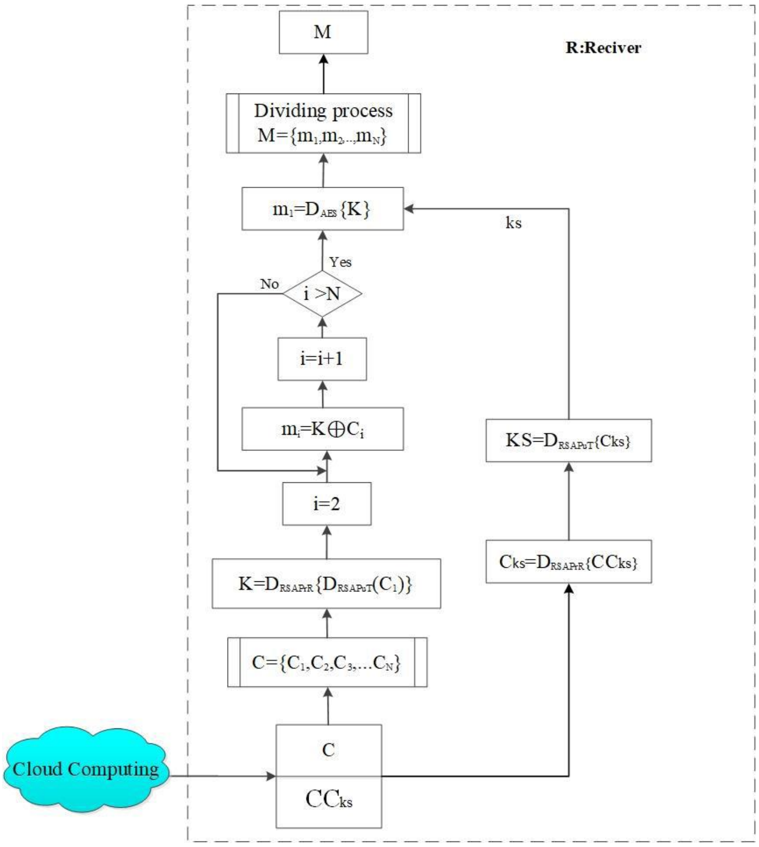

Figure -2: The hybrid proposed model by combining RSA and AES at the receiver's side

4. RESULTS AND DISCUSSION

We have discussed the security requirements of the cloud computing that the proposed model has achieved and whether the security requirements explained above have been met as follows:

1-Confidentiality: The proposed model has provided the confidentiality feature for non-users of cloud computing and for other cloud computing users, where the message can only be obtained by the recipient. This is because the message can only be obtained after getting (m1), which can be only obtained by a decryption (C1) using the AES algorithm with the key KS. This is because the owner of the private key of the receiver PrR can obtain this key, and this key is present only at the recipient of the message. Therefore, no one can see this message, which means that the confidentiality is secured by its three aspects described previously, in addition to protecting the first block (m1), which represents the key (K), with two levels of encryption with the same key protection mechanism (KS) for the AES algorithm, which increases the confidentiality and that the message is protected from unauthorized access.

2-Privacy and Integrity: Since the decryption key KS can be only obtained by decrypting CCKS twice, and the first time is exclusively associated with the private key, no one can tamper with it except by the recipient who is the owner of the message exclusively, as for key (K) the same procedure has applied to it.

3-Authentication and Verification: The proposed model provides the transmitter with the ability to authenticate his message by encrypting the KS session key using the RSA algorithm with his private key PrT, where we obtain CKS, which is the encryption of the secret key. This can be considered as the transmitter's authentication of his message, since the transmitter encrypts KS with his private key, allowing the receiver to verify the transmitter and know his identity. This is only the receiver can obtain the KS key by decrypting it using the RSA algorithm by the public key's transmitter. This cannot be done without his public key or by using one of the public keys of other users. The proposed model also allows the transmitter to verify that the message has reached the receiver exclusively by encrypting CKS by the receiver's public key, which ensures that the transmitter can only get CKS by the receiver (R) exclusively, as no one else has his private key, as for key (K) the same procedure has applied to it.

4-Non-repudiation: Once the plain text of the message (M) is known by the non-transmitter of the proposed model, the transmitter cannot deny that he sent this message, and the recipient cannot deny that it was he who opened this message exclusively. This is because only the transmitter and the receiver have their key, as for key (K) the same procedure has applied to it.

Execution time:

The proposed model has used only the RSA algorithm for the encryption of the secret key (KS) for the AES algorithm

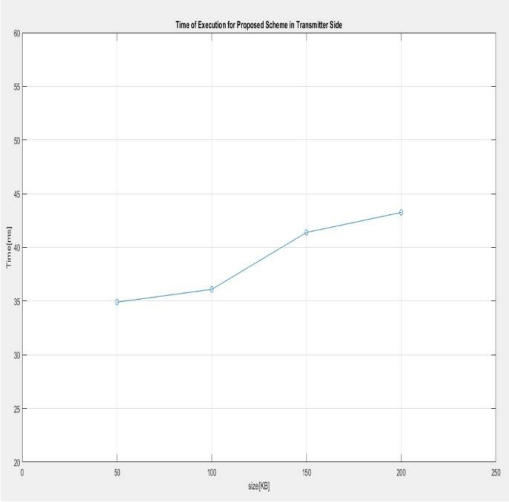

Figure -3: The execution time of the proposed model in the transmitter's side

Shows the execution times for the proposed model and each of RSA and AES algorithms separately on the receiver's side for various file sizes.

5. CONCLUSION

This paper proposes an integrated secure model for the cloud computing system. The proposed model achieves the security requirements of cloud computing on higher data confidentiality and gets security requirements in the cloud computing with the least possible execution time, the hybrid proposed model of RSA and AES algorithms makes full use of the advantages of both of them. This is accomplished by using them twice to encrypt a fixed text block of 128bit, additionally, the AES algorithm is using a dynamic cipher key that is generated randomly in each session. The proposed model achieved a lower execution time than the three studied references (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017).

REFERENCES

[1] Malgari, V., Dugyala, R and Kumar. A. (2020). A novel data security framework in distributed cloud computing. In: IEEE Fifth International Conference on Image Information Processing , Shimla, India, India, 15-17 /11/ 2019. DOI: 10.1109/ICIIP47207.2019.8985941

[2] Marqas, R. B., Almufti. S. M. and Ihsan, R.R. (2020). Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. Journal of Xi'an University of Architecture & Technology, 12(3), 3110-3116.

[3] Mohan, D. N., Kumar, V. H. and Shashank, N. (2020). Enhancement of cloud computing security with secure data storage using AES. International Journal of Research in Engineering, Science and Management, 3(1), 586–587.

[4] Saeed, Z.R., Ayop, Z., Azma. N. and Baharon. M.R. (2018). improved cloud storage security of using three layers cryptography algorithms. International Journal of Computer Science and Information Security, 16(10),34-39.

[5] Sakharkar, N. (2019). Survey of cryptographic techniques to certify sharing of information in cloud computing. International Research Journal of Engineering and Technology, 6(8), 397-400.

[6] Al-Kaabi, S.S. and Belhaouari, S.B. (2019). Methods toward enhancing RSA algorithm: A survey. International Journal of Network Security & Its Applications, 11(3), 53–70. DOI: 10.5121/ijnsa.2019.11305

[7] Biswas, C., Gupta, U.D. and Haque, M. (2017). A hierarchical key derivative symmetric key algorithm using digital logic. In: IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh. 16-18/02/ 2017 DOI: 10.1109/ECACE. 2017.7912976

[8] Chavan, A., Jadhav, A., Kumbhar, S., and Joshi, I. (2019). Data transmission using RSA algorithm. International Research Journal of Engineering and Technology, 6(3), 34-36.

[9] Dixit, A. K. and Gandhi, C. (2017). Multilevel security framework for cloud data. In: IEEE International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 12-14 /10/ 2017. DOI: 10.1109/IC3TSN.2017.8284478

[10] Elgabbani, B.O. S. and Shafie, E.A. (2019). Securing iClouds storage based on combination of RSA and AES crypto system. International Journal of Computer Science and Security, 13(5), 201-210.

[11] Fatima, S. and Ahmad, S. 2019. An exhaustive review on security issues in cloud computing. International Journal of Scientific and Research Publications, 13(6), 3219-3237. DOI: 10.3837/tiis.2019.06.025

[12] Ghaffari, F., Gharaee, H. and Arabsorkhi, A. (2019). Cloud security issues based on people, process and technology model: A survey. In: IEEE 5th International Conference on Web Research, Tehran, Iran, Iran, 24-25 /04/2019. DOI: 10.1109/ICWR.2019.8765295

[13] Hussain, I., Negi, M. C. and Nitin Pandey. N. (2018). Proposing an encryption/ decryption scheme for IoT communications using binary-bit sequence and multistage encryption. In: IEEE 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 29-31 /08/ 2018. DOI: 10.1109/ ICRITO. 2018.8748293

[14] Jintcharadze, E. and Iavich, M. (2020). Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems. In: IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria, 4-7/09/2020. DOI: 10.1109/EWDTS 50664.2020.9224901

[15] Khaing, K. K. and, Naung, Y. (2019). Encryption data measurement and data security of hybrid AES and RSA algorithm. International Journal of Trend in Scientific Research and Development, 3(6), 834-838.

[16] Khan, A., Mishra, K.K., Santhi, N. and Jayakumari. J. (2015). A new hybrid technique for data encryption. In: IEEE 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, India, 23-24 /04/ 2015. DOI: 10.1109/GCCT.2015.7342801

[17] Khan, S. and Sharma, S. (2019). Analysis of cloud computing for security issues and approaches. International Journal on Emerging Technologies, 10(1), 68-73.

[18] Liang, C., Ye, N., Malekian, R. and Wang. R. (2017). The hybrid encryption algorithm of lightweight data in cloud storage, In: IEEE 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR), Bangi, Malaysia, 23-24 /08/ 2016. DOI: 10.1109/ISAMSR. 2016.7810021

[19] Mahalle, V. S. and Shahade. A. K. (2014). Enhancing the data security in cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In: IEEE International Conference on Power, Automation and Communication, Amravati, India, 6-8 /10/ 2014. DOI: 10.1109/INPAC.2014.6981152.

****