AN INTEGRATED SECURITY MODEL USING AES AND RSA FOR THE CLOUD COMPUTING SYSTEM

Nairouz Alzin[1], Zakria Mahrousa[2], Mahmoud Rahhal[3]

[1]Postgraduate Student (Ph.D.) Dept. of Computer Engineering, Faculty of Electrical & Electronic Engineering, University of Aleppo, Syria
[2]Dept. of Computer Engineering, Faculty of Electrical & Electronic Engineering, University of Aleppo, Syria
[3]Dept. of Computer Engineering, Faculty of Electrical & Electronic Engineering, University of Aleppo, Syria

---***---

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.

Key Words: **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.
The researchers concluded that these hybrid encryption algorithms optimize the encryption efficiency, key management, and data security in file encryption, but they have demonstrated there are still some deficiencies in their study, such as data tampering and forgery.

Also, Dixit and Gandhi (2017), have suggested securing the data before storing it in the cloud through a multi-level encryption model by increasing the protection of the encryption key, as they have suggested splitting the secret key of the AES algorithm into (n) part and then compressing it with Huffman's coding algorithm and then encrypting it with the RSA algorithm and the reverse process is done. at decryption, the researchers have indicated that they were able to secure the data by securing the encryption key.

Tyagi et al. (2019) have proposed a hybrid model that achieves the confidentiality of data stored in cloud computing and a mechanism that guarantees the privacy of the keys, by making use of most of the advantages of the AES and RSA algorithms. For instance, the AES algorithm has a high speed, but the main disadvantage is that the secret key is present for all cloud-computing users. The RSA algorithm eliminates this disadvantage because only one user has a private key. The main disadvantage in the RSA, however, it's being slow. Therefore, the researchers proposed encrypting data using the AES algorithm by a dynamic key, and then this key is encrypted with the RSA algorithm by the public key. Thus, they were able to secure the confidentiality and privacy of the data without achieving the rest of the security requirements of cloud computing.

Other researchers, such as Chavan et al (2019) have achieved another requirement of security requirements for cloud computing which is that the unauthorized user does not have access to the data stored on the cloud. This is coupled with securing the confidentiality and privacy of data by proposing a hybrid model that combines the RSA and AES algorithms with the OTP (One-time password) technology used to generate a one-time text password. It is characterized by being dynamic so that one new password is generated each time. that is usually used as an additional layer of security; thus, their proposed model achieved strong authentication through OTP technology because the one-time password provides privacy and confidentiality by preventing the unauthorized user from accessing the data stored on the cloud. On the other hand, their proposed model has also achieved stronger data security against attacks through hybrid encryption.

Singh and Sharma (2019) have proposed a new method for storing data securely in the cloud computing system via using encryption, decryption, and partitioning data algorithms. They have divided the file into (N files) to be stored, and then each part of this file is encrypted by using one of the encryption algorithms used in their research. Then, they collected the encrypted texts to get the total encrypted text at the stage of storing data, but the opposite process has been done when retrieving data at the decryption. Therefore, they have been able to improve the security of cloud computing, but their proposed model has not been able to achieve all security requirements in cloud computing.

Sharma et al. (2019) proposed a hybrid model combining RSA and AES algorithms through multilevel encryption to enhance data security, integrity, and authentication in cloud computing. They have encrypted the file with the RSA algorithm as the first level of encryption and then with the AES algorithm as the second level of encryption at the sending side before sending it to the cloud. However, the decryption process at the receiving side has been carried out with the AES algorithm and then with the RSA algorithm to get the file, so their proposed model has been able to enhance data security and privacy without achieving all the security requirements of the cloud computing.

Saeed et al. (2018) have endeavored to enhance data security in cloud computing, by proposing a hybrid model that combines RSA, AES, and ECC algorithms. They encrypted the text data with the AES algorithm and used the ECC algorithm to encrypt the key of the AES algorithm, and then both the encrypted text and the encrypted key are encrypted with the RSA algorithm. Then, they have applied their proposed model with the various sizes of text files, and their results have proved that their hybrid proposed model has achieved higher secrecy, but has not achieved all security requirements in cloud computing.

While Mahalle and Shahade (2014) have achieved data authentication by proposing hybrid encryption that combining RSA and AES algorithms, where the data have been encrypted with the AES algorithm and the secret key of the AES algorithm has been encrypted with the transmitter's public key, only the user has known the private key and secret key that as his. Therefore, user's private data has not been accessible to anyone, not even the cloud's administrator. Thus, they have achieved the main advantage is the confidentiality of data on the cloud without achieving all the security requirements of cloud computing.

Elgabbani and Shafie (2019) have proposed a hybrid model that combines the RSA and AES algorithms to secure data stored in iCloud, where the transmitter encrypts the AES key using the receiver's public key, while the receiver at the recipient side decrypts the AES key with the private key of the receiver. This is followed by decrypting the entire message using the AES algorithm. They have applied their study on iCloud technique namely dropbox, as they have used asymmetric encryption algorithm to encrypt a symmetric secret key. They have found that this hybrid model has given better data security by avoiding the defect of the AES algorithm in terms of managing the distribution of keys using RSA. This is in addition to avoiding the disadvantage of RSA being slow, by improving it by selecting two unpredictable large numbers randomly, for the public and private key, and then using them to encrypt the secret key of AES. Thus, they have taken advantage of both algorithms without fulfilling the rest of the security requirements of cloud computing.

As for Jintcharadze and Iavich (2020), they have implemented an analysis of new hybrid cryptosystems. They have compared the models so that each of them combines a symmetrical algorithm and an asymmetric algorithm, and their result has shown that their hybrid proposed model which combines the RSA and AES algorithms is significantly secure, which it has been based on encrypted the secret key of AES algorithm by RSA algorithm.

Other researchers Hussain et al. (2018) have pointed out the importance of using cryptography on both sides i.e. encrypting data at the transmitter's side later followed by decryption processes at the receiver's side, they have proposed a symmetric encryption algorithm based on XOR-ed and have shown that it's not quite viable cracking the encrypting/decrypting processes with no knowledge about the accurate secret key.

Many researchers have tended to the development of different hybrid encryption algorithms to protect data and increase confidentiality. Khan et al. (2015) have divided the message into three parts and encrypted them with one of three different techniques (Fibonacci series, XOR logic, PN sequence) respectively using two keys: segmenting key and encrypting key to provide further authentication and validation, and they have shown that their proposed hybrid model achieves authentication and validation.

As so for Biswas et al. (2017) have endeavored to protect data from unauthorized access by proposing a symmetric encryption algorithm that has been developed with a secret key that is generated from the plaintext based on XOR-ed. They relied on securing data by securing the secret key and they showed that their developed algorithm has the feature to fight against frequency analysis attacks.

On the other hand, Marqas et al. (2020) have demonstrated by the comparison between the RSA and AES algorithms that the AES is better and faster than the RSA algorithm in encrypting data.

We can summarize previous researchers' efforts in the strive to find a model that achieves higher data confidentiality, in addition to fulfilling most or all the security requirements in cloud computing. This is done through various proposals combining symmetric and asymmetric algorithms to achieve higher data confidentiality and get security requirements in cloud computing with the least possible execution time.

The main goal of this research is to get a model to protect cloud computing data, whether stored within the cloud or transferred between its users.
This model fulfills the requirements of cloud computing, which are:
1-Confidentiality, 2-Privacy, and integrity, 3- Authentication and verification, 4-Non-repudiation, 5- Acceptable execution time.
This model is based on the merge of the RSA and AES algorithms, to take advantage of the features of both of them.
This paper is organized as follows:

1. point out and summarize most important the reference models proposed by researchers to develop secure models in the cloud computing system.
2. point out and summarize security requirements in cloud computing.
3. demonstrate and present the proposed hybrid model and the manner of its work.
4. Discussing the results and comparing them with the studied reference models.

2.STUDY THE MOST IMPORTANT PROPOSED REFERENCE MODELS FOR THE CLOUD COMPUTING SYSTEM

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.

2.3. The third studied reference model (Liang et al., 2017)

The researchers have enhanced the confidentiality of data in the cloud by proposing a hybrid encryption model based on improving the RSA algorithm by increasing the length of the key and then using it to encrypt the secret key of the AES algorithm at the transmitter's side before sending the data to the cloud, and the reverse operation is done at the receiving side. Their proposed hybrid model has got higher data secrecy in the cloud storage system without fulfilling the rest of the security requirements of cloud computing.

3. SECURITY REQUIREMENTS IN THE CLOUD COMPUTING

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):

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:

- Non-users of cloud computing should not tamper with cloud computing data.
- Not to have tampered one of the users of the cloud computing with the data of one or more users from the cloud computing users.

The first approach can be achieved by using the AES algorithm, but it is not able to achieve the second approach. While the asymmetric RSA algorithm can achieve the previous two approaches, it has a slower implementation rate when compared to AES.

3-Authentication and verification: The concept of authentication includes the ability of the data transmitter to authenticate his data so that others can know that this data belongs to this user alone and that this data cannot be for others. As for the concept of verification, it includes two basic concepts:

- The receiver checks the sending side and has the ability to know the transmitter.
- The transmitter has verified the recipient's side; and that only the recipient can see this data.

Asymmetric algorithms are often used to achieve the two properties of verification and authentication, through different models that differ among themselves in how the encryption is performed in terms of private and public keys.

4-Non-repudiation: The concept of non-repudiation includes the following two approaches:

- The transmitter has not to deny that he has sent this data.
- The receiver has not to deny that he received this data.

These two properties can be achieved using an asymmetric algorithm such as the RSA algorithm, where the first concept is achieved when the transmitter encrypts his data by his private key. However, the second concept is fulfilled (the receiver cannot deny) when the transmitter encrypts his data with the public key, because the private key cannot be possessed except by the transmitter in the first case or by the receiver in the second case.

4. THE HYBRID PROPOSED MODEL BY COMBINING RSA AND AES ALGORITHMS

Figure1 demonstrates the hybrid proposed model which combines the RSA and AES algorithms in the transmitter's side, to achieve high confidentiality and to meet the security requirements of the cloud computing with the least possible execution time.

The proposed model is based on the idea of dividing the plain text M into (N) a block with a128bit length, and encrypting the message blocks $\{m_2, m_3, \ldots\ldots, m_N\}$ based on the key (K), the key (K) is the result of ciphering the first block (m_1) using AES algorithm with dynamic key (KS) (which is generated randomly each time), and then this key (KS) has protected with two stages of encryption by using the RSA algorithm, firstly by using the private key of the transmitter (E_{RSAPrT}) and secondly with the public key of the receiver ((CK) E_{RSAPuR}). Then the m_i blocks where (i = 2, 3,...., N) are encrypted based on the key (K) and then this key is protected with the same mechanism of protection of the dynamic key (KS), and then the encrypted text (C) has been combined with the encrypted key (CCKS) which has been encrypted previously with two levels of encryption. Then, the message is sent along to the cloud, whether the process is messaging or storing, and the reverse operation is done on the receiver's side, as shown in Figure 2.

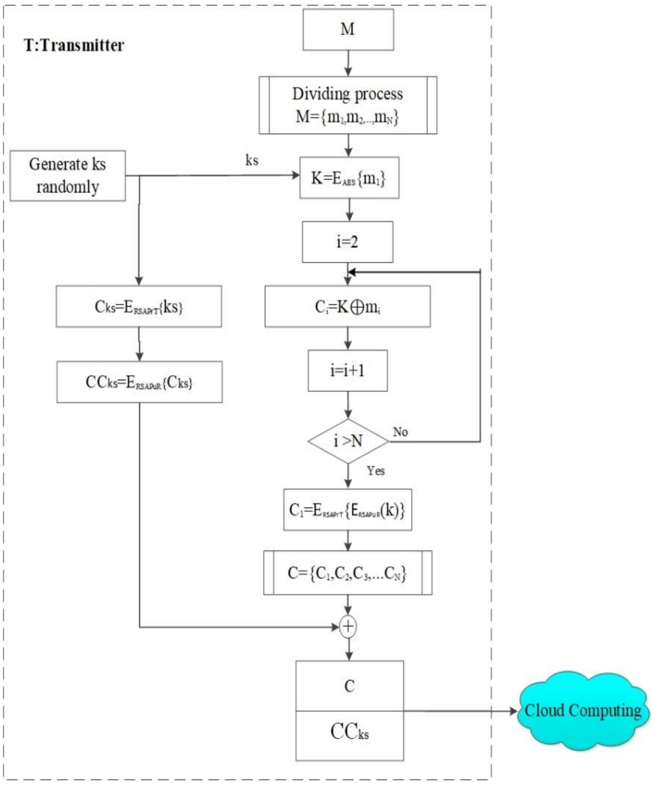

Figure -1: The hybrid proposed model by combining RSA and AES in the transmitter's side

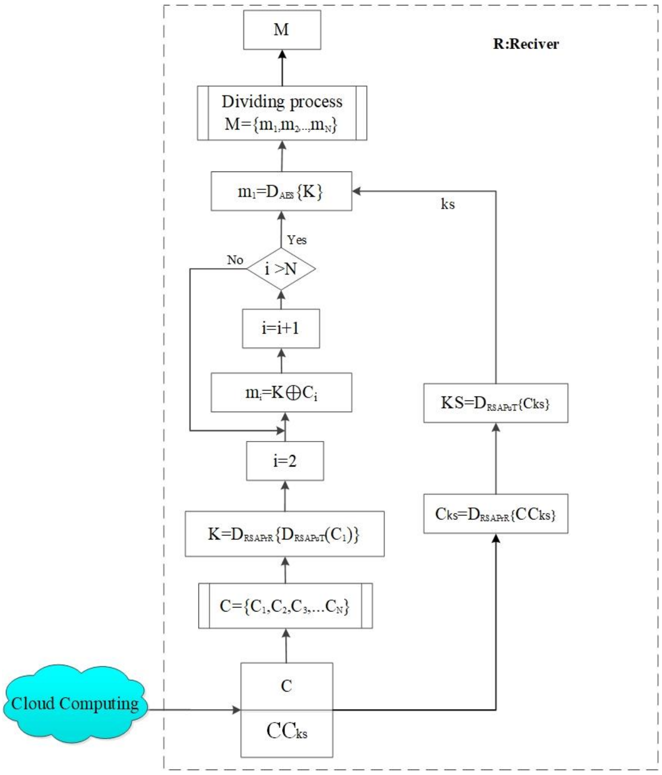

Figure -2: The hybrid proposed model by combining RSA and AES at the receiver's side

5.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 (m_1), which can be only obtained by a decryption (C_1) 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 (m_1), 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 with128bit length and for the encryption of the first block from the message that which it is the key (K). This means the RSA algorithm is used to encrypt text with a length of 16 Byte twice only and is not used to encrypt a relatively large message whether that compared it with this length. Also, the AES algorithm has been used only to encrypt the first block m_1 which is also 128bit long. This ensures the reduction of the other times necessary to encrypt the rest of the message blocks, as they are encrypted by relying on the XOR factor. This process takes place in the transmission and reception, which ensures shortening the execution time, whether on the transmitter or receiver's side. Table1 shows the execution times for the proposed model and each of RSA and AES algorithms separately on the transmitter's side for various file sizes.

Table -1: The execution times of the proposed model and each of RSA and AES algorithms separately on the transmitter's side for various file sizes.

File size (KB)	The execution time of the proposed model in the transmitter's side (ms)	The execution time of the RSA algorithm in the transmitter's side (ms)	The execution time of the AES algorithm in the transmitter's side (ms)
50KB	34.91	552	123
100KB	36.1	1112	239
150KB	41.4	1630	306
200KB	43.26	2063	499

Figure 3 shows the execution times graph of the proposed model in the transmitter's side.

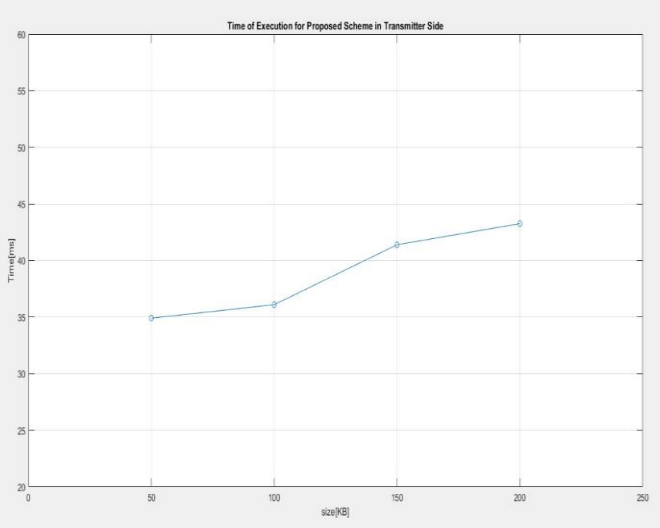

Figure -3: The execution time of the proposed model in the transmitter's side

Table 2 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.

Table -2: The execution times of the proposed model and each of RSA and AES algorithms separately on the receiver's side for various file sizes.

Filesize (KB)	The execution time of the proposed model in the receiver's side (ms)	The execution time of the RSA algorithm in the receiver's side (ms)	The execution time of the AES algorithm in the receiver's side (ms)
50KB	106.2	2103	470
100KB	110.1	4025	910
150KB	112.01	6440	1220
200KB	114.2	8200	1760

Figure 4 shows the execution times graph of the proposed model on the receiver's side.

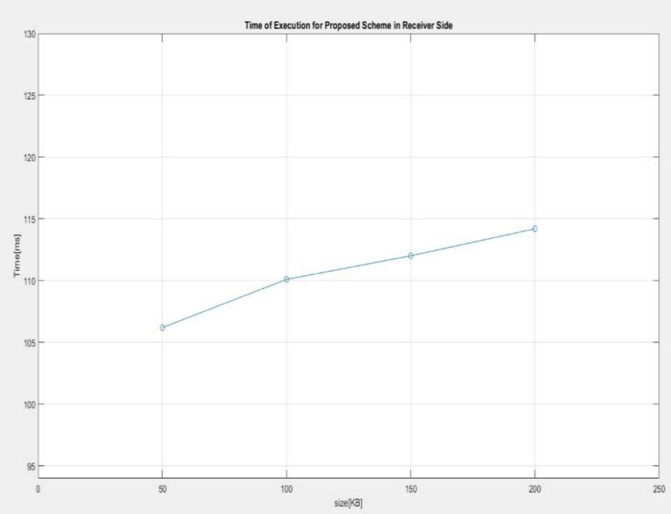

Figure -4: The execution time of the proposed model in the receiver's side.

6. COMPARISON

in order to perform the comparison between the proposed model and the studied reference models, we have to get the data that used in the studied reference models (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017) and then the procedure of implementing the proposed model on these data was carried out. The proposed model was compared with the studied reference models (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017) in terms of security requirements in cloud computing.

Table 3 shows a comparison of the execution times between the proposed model and the three reference models studied (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017) for the various file sizes, where it is noticed that the proposed model is superior to the reference models at the execution time. This is because in the proposed model the AES algorithm, with its iterative loops, is executed once and the RSA algorithm twice in order to protect the secret key of the AES algorithm and two more times for the protection of the (K) key only for a fixed text length of 128bit at both the transmitter and receiver side. We have considered the execution time to the comparison as the sum of the times at the transmitter and receiver sides. This is done for every model, separately.

Table -3: The Comparison of the execution time between the proposed model and the three studied reference models (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017)

Filesize (KB)	Execution time for the proposed model	Execution time for the first studied reference model (Khaing and Naung, 2019)	Execution time for the second studied reference model (Malgari et al., 2020)	Execution time for the third studied reference model (Liang et al.,2017)
40KB	140.92 ms	-	670.06ms	-
104KB	146.86 ms	-	697.23ms	-
Database file db1.mdb 560KB	205.24 ms	1355ms	-	-
1024KB	312.33ms	-	-	1426.25ms
Image file image.jpg 3255KB	982.79 ms	8047ms	-	-

Table 4 shows a comparison between the security requirements in the cloud computing that the proposed model fulfills and each of the three studied references (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017).

Table -4: The comparison of the security requirements achieved by each of the proposed model and the three studied reference models (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017)

The proposed model and the reference models Security requirements of the cloud computing		The proposed model	The first studied reference model (Khaing and Naung, 2019)	The second studied reference model (Malgari et al., 2020)	The third studied reference model (Liang et al.,2017)
Confidentiality	Not a cloud user	√	√	√	√
	Cloud user	√	√	√	√
	Anyone	√	√	√	√
Privacy and Integrity	Not a cloud user	√	√	√	√
	Cloud user	√	√	√	√
Authentication		√	×	×	×
Verification	From the transmitter	√	×	×	×
	From the receiver	√	√	√	√
Non-repudiation	From the transmitter	√	×	×	×
	From the receiver	√	√	√	√

Table 4 provides a comparison in terms of the possibility of meeting the security requirements of the cloud computing for the proposed model and the three studied reference models (Malgari et al., 2020; Khaing and Naung, 2019; Liang et al., 2017). It can be noted that the proposed model is superior over the three reference models in the subject of authentication and verification of the transmitter and non-repudiation of sending the message. This is due to an additional encryption phase for both of the key (KS) and the key (K) by the private key of the transmitter (E_{RSAPrT}) on the transmitter's side.

7.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] 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

[2] 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

[3] 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.

[4] 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

[5] 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.

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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.

[11] 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

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

[13] 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

[14] 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

[15] 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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] San, M. M. and Win, K. M. (2019). Risk management of secure cloud in higher educational institution. International Journal of Trend in Scientific Research and Development, 3(5), 1314-1319.

[21] Sharma, Y., Gupta, H. and Khatri, S. K. (2019). A security model for the enhancement of data privacy in cloud computing. In: IEEE Amity International Conference on Artificial Intelligence, Dubai, United Arab Emirates, United Arab Emirates, 4-6/02/ 2019. DOI:10.1109/AICAI.2019. 8701398

[22] Singh, B. and Sharma, S. (2019). Enhancing data security using encryption and splitting technique over multi-cloud environment. International Journal of Scientific Research & Engineering Trends, 5(3),1041-1047.

[23] Tabrizchi, H. and Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(n/a), 9493– 9532.

[24] Tyagi, M., Manoria, M. and Mishra, B. (2019). Analysis and implementation of AES and RSA for cloud. International Journal of Applied Engineering Research, 14(20), 3918-3923.

[25] Yahya, F., Chang, V., Walters, R.J. and Wills, G.B. (2019). A security framework to protect data in cloud storage. In: Proceedings of the 4th International Conference on Internet of Things, Big Data and Security, Heraklion, Crete, Greece, 2–4/05/2019. DOI: 10.5220/ 0007737603070314

[26] Zou, L., Ni, M., Huang, Y., Shi, W. and Li, X. (2020). Hybrid encryption algorithm based on AES and RSA in file encryption. Springer Nature Singapore Pte Ltd, n/a(n/a),541–551. DOI:10.1007/978-981-15-3250-4_68