International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 6, December 2022, pp. 6496~6505
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i6.pp6496-6505

Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen

Shihab A. Shawkat[1], Bilal A. Tuama[2], Israa Al_Barazanchi[3,4]
[1]Department of Quality Assurance and Academic Performance, University of Samarra, Samarra, Iraq
[2]Department of Pathological Analysis, College of Applied Sciences, Samarra University, Samarra, Iraq
[3]College of Computing and Informatics, Tenaga Nasional University, Kajang, Malaysia
[4]Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq

Article Info

Article history:

Received Sep 20, 2021
Revised Jun 21, 2022
Accepted Jul 18, 2022

Keywords:

3kRSA algorithm
Cloud security
Information security
Triple data encryption standard algorithm

ABSTRACT

Cloud computing is considered a distributed computing paradigm in which resources are provided as services. In cloud computing, the applications do not run from a user's personal computer but are run and stored on distributed servers on the Internet. The resources of the cloud infrastructures are shared on cloud computing on the Internet in the open environment. This increases the security problems in security such as data confidentiality, data integrity and data availability, so the solution of such problems are conducted by adopting data encryption is very important for securing users data. In this paper, a comparative study is done between the two security algorithms on a cloud platform called eyeOS. From the comparative study it was found that the Rivest Shamir Adlemen (3kRSA) algorithm outperforms that triple data encryption standard (3DES) algorithm with respect to the complexity, and output bytes. The main drawback of the 3kRSA algorithm is its computation time, while 3DES is faster than that 3kRSA. This is useful for storing large amounts of data used in the cloud computing, the key distribution and authentication of the asymmetric encryption, speed, data integrity and data confidentiality of the symmetric encryption are also important also it enables to execute required computations on this encrypted data.

Corresponding Author:

Shihab A. Shawkat
Department of Quality Assurance and Academic Performance, University of Samarra
Samarra, Iraq
Email: shahab84ahmed@gmail.com

1. INTRODUCTION

The distributed computing has quickly arisen as an acknowledged figuring worldview in which the resources of the registering frameworks are given as administrations of the web cloud processing is a hot examination region in the scholarly community, the development of distributed computing, equal processing and lattice figuring. Because of the consequences of such hybrid evolution, the applications can be expanded by means of the web security in the cloud computing [1]. Distributed computing shares disseminated assets in the open climate through the organization, so it makes security issues. Likewise, when the information is in plaintext, it is helpless against different sorts of assaults, on different words, the distributed computing is possible experiencing a number of known weaknesses, empowering aggressors to either get figuring administrations for nothing or take data from cloud clients. In the world of processing, security and protection issues are significant concern and the cloud computing is no exemption for these issues.

Cryptographic instruments applied to information offer the best answer for information insurance. Information ought to be scrambled locally preceding uploading to the cloud, and that information proprietor holds the encryption keys. The objective of encoded stockpiling in the cloud is to make a virtual stockpiling framework that maintains the cryptography objectives which are: confidentiality ,information uprightness on the other words, the encryption calculations were utilized to secure the information so it cannot be perused by a third-party while on the way [2], [3]. The main scholastic utilization of the cloud computing has all the earmarks of being who initially characterized it as a figuring worldview where the limits of processing will be controlled by monetary reasoning as opposed as far as possible definition for the cloud computing as: "A way of computing in which versatile and flexible IT-empowered capacities are conveyed as a support of outside clients utilizing Internet innovations" or "A normalized IT ability (administrations, programming, or framework) conveyed through internet advances in a compensation for every utilization, self-administration way" [4], [5]. Distributed computing is a model to empower on-request network admittance to a typical arrangement of the most configurable distributed computing assets (workers, organizations, administrations, stockpiling, and applications). The cloud model comprises of (five-fundamental provisions, three administration models and four-sending models) [6], [7]. Distributed computing has seen the improvement of innovations and business strategies that have arisen over the previous years. The fundamental squares range through (web innovation to cloud specialist organizations), as displayed plainly in Figure 1 [8].

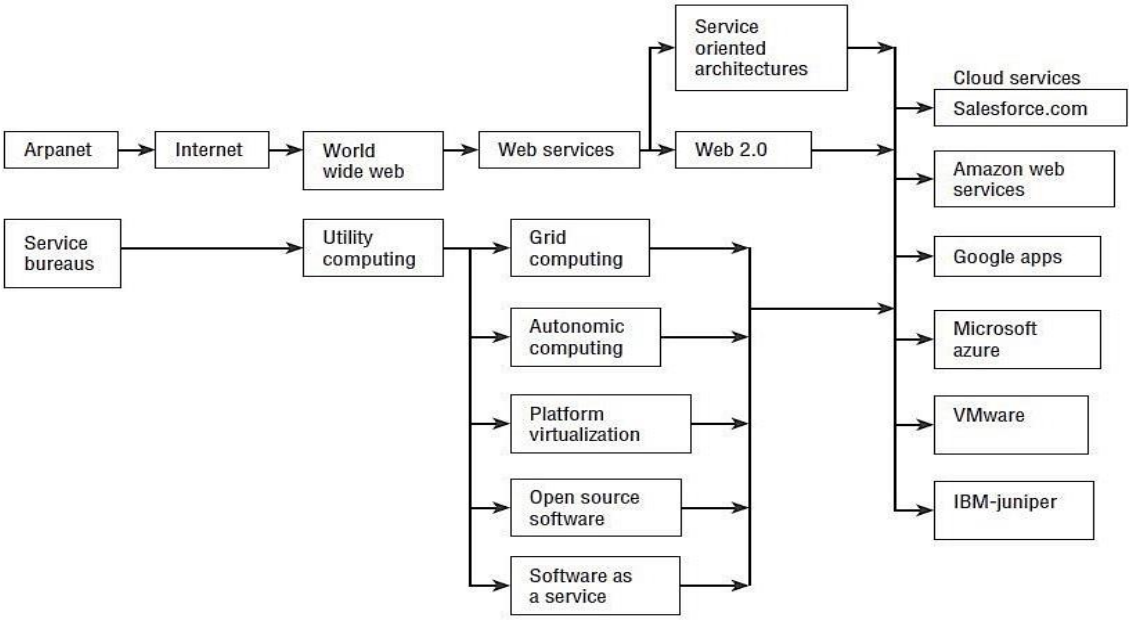

Figure 1. The main blocks of internet technology available to cloud service providers

The distributed computing separates itself from other registering standards like lattice processing, worldwide figuring, internet figuring in the different perspectives, for example, on-demand service provision, user centric interfaces, ensured quality of service (QoS), autonomous system [9], [10]. The distributed computing conveyance models, arrangement models, characterizing characteristic, assets, and association of the foundation examined in this part. There are three cloud conveyance models: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS), sent as open, private, local area, and half and half clouds. The parts of distributed computing are displayed in Figure 2 [11].

When settling on choices to take on cloud administrations, protection or security has consistently been a significant issue. To manage these issues, the cloud supplier should develop adequate controls to give such degree of safety than the association would have if the cloud was not utilized. It is discovered that security positioned first as the best test of distributed computing that ensure classification and credibility over an uncertain correspondence channel. The eyeOS is picked due to its components are: cloud based, easy-to-utilize interface, collaboration, compatibility ensured and flexibility [12], [13]. Rest of this paper is coordinated: section 2 presents the scientific classification dependent on foundation and related work in the concerned exploration region, section 3 verbalizes the key ideas proposed work, section 4 presents the outcomes and conversations, and section 5 presents end and future work.

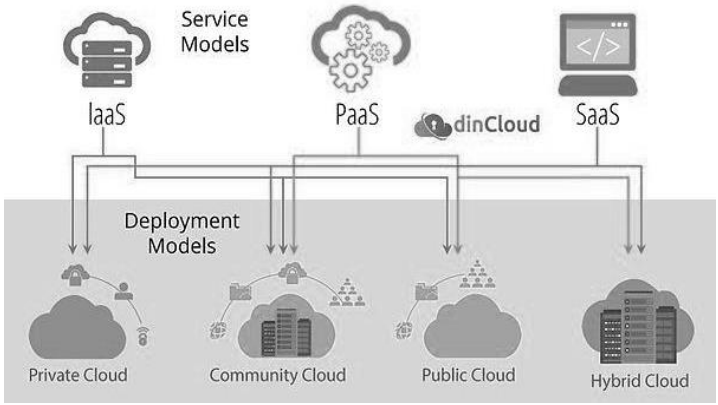

Figure 2. The cloud computing

2. BACKGROUND AND RELATED WORK

There are various studies done to compare the performance of these algorithms based on multiple parameters; some of which are related to encryption and decryption. Users need to keep their information safe and secure while in storage and/or transmission. The service providers ensure security through data encryption and decryption. There are a variety of encryption and decryption algorithms to protect the data. This section is categorized into four sub sections presenting a brief background of the main topics used in this paper through shedding light on a number of related works in the area of text document classification. This section reviews the literature in cryptography algorithms.

2.1. Cloud computing security

Cloud computing has become a known and important thing nowadays. However, privacy and security remain a powerful barrier of problems for users for the purpose of adapting to cloud computing systems. Note that these fears are not enough, and we must also add more in terms of five aspects (such as confidentiality, availability, data integrity, control and review) to avoid security problems. Cryptography is a technique used to make secure correspondence by controlling sent messages during the correspondence happened so just expected party that can know the substance of that message. The absolute most ordinarily utilized cryptography strategies to secure sent messages, particularly as message [14], [15]. Normal strategies for ensuring client information incorporate encryption before capacity, client validation methods preceding capacity or recovery, and building secure channels for information transmission. Normal information encryption strategies incorporate symmetric and symmetric. This sort of encryption and unscrambling measure utilizes a mysterious key. Awry cryptography, then again, utilizes two distinctive keys: a "public key" for encryption and a "private key" for decoding. Symmetric cryptography is more effective, and is reasonable for scrambling enormous volumes of information. Uneven cryptography requires more calculation time and is utilized for the decoding keys which are needed for symmetric cryptography [16].

2.1.1. Triple data encryption standard (3DES)

3DES was made in light of the fact that DES calculation, concocted in the mid-1970s utilizing 56-bit key. 3DES gives powerful security to me just 112-bits because of the midterm assaults it gets in the center. 3DES runs multiple times more slowly than DES, yet is considered more secure whenever utilized effectively. The unscrambling methodology is exactly the same thing as the decoding system; however then again, actually it is acted the other way. In information encryption and unscrambling (DES) is done in 64-bit segments as the info key length of DES is 64-bit and the actual key that DES utilizes is just 56-bit genuine length [17]. The most un-significant bit (extreme solidly) in every bite is the equality of the pieces, it should be worked out and there must consistently be an odd number of 1 s in every byte and these equality pieces are overlooked, so the utilization of the seven most significant pieces is just per bit, which prompts be 56-bits in length. This demonstrates that the force of the compelling key for 3DES is really 168-bits in light of the fact that every one of the three keys has 8 equality bits that are not utilized during the necessary encryption measure [18], [19]. 3DES encryption measure block graph is displayed in Figure 3.

New block cipher algorithm. The main principles of 3DES algorithm are [20]: i) 3DES uses a "Key Package" consisting of three keys (K1, K2, and K3) for every 56-bit; ii) the coding equation is *Cipher-text=EK3 (Dk2 (Ek1 (plain text)))*, DES encoding using "K1", decoding DES using "K2", and then encoding DES using "K3"; and iii) the decoding equation is *Plaintext=DK1 (Ek2 (Dk3 (Cipher text)))*, which will be

decoded using K3, encoded using K2, and then decoded using K). It enjoys the benefit of each triple encoding that scrambles one square of 64-pieces of information. In every exemplification, the center cycle is rather than the first and last, which works on the strength of the calculation when utilizing the lock choice 2, and gives the contrary similarity the DES with the lock alternative 3. The principles characterize three fundamental keying choices:

- Main keying alternatives 1: all three keys are separate,
- Main keying alternatives 2: (K1 and K2) are free and (K3=K1),
- Main keying alternatives 3: all 3 keys are indistinguishable (K1=K2=K3).

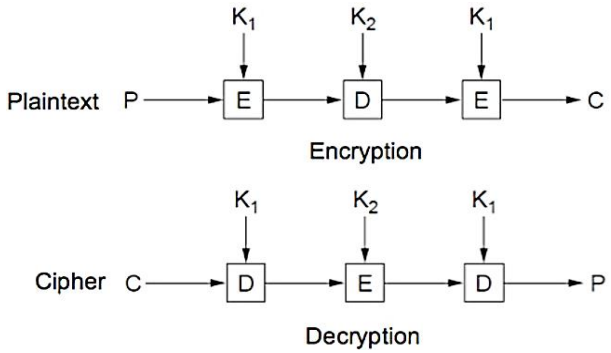

Figure 3. Flowchart of 3DES encryption and decryption algorithm

2.1.2. Rivest Shamir Adlemen

The calculation was created by Rivest, Shamir and Adlemen in 1977. It is a public key calculation since it utilizes two keys one to encode and other to unscramble the message. Public key is utilized by the sender to the private key (simply known to beneficiary) is utilized by the recipient to unscramble the message. This private key, as the name proposes is known distinctly to the recipient. The RSA comprises of some numerical tasks through which it can work out the encryption and unscrambling keys (R and T), after that one can without much of a stretch compute the code text and the plain text by the accompanying formula [21]:

$$C = MR \bmod (n) \quad (1)$$

$$P = MT \bmod (n) \quad (2)$$

where R and T are public and private keys and n is a worth acquired from numerical activities in RSA. To complete execution investigation RSA was altered. 3kRSA is a protected algorithm, a third key was proposed to be added to the RSA algorithm was proposed to twofold the security of the calculation. The RSA has been utilized in different applications like in e-com which guarantee message trustworthiness, security; verification and non-disavowal [22]. There are two types of encryption algorithms, symmetric and asymmetric now see Table 1 represents the comparison among 3DES and RSA algorithms.

Table 1. Comparison among 3DES and RSA [21], [22]

Factors	3DES	RSA
Cipher type	Symmetric block cipher	A symmetric block cipher
Security rate	One only weak which is exit in DES	Good
Key length	(kl, k2 and k3)168 bits (kl=k2) 112 bits	Based on No of bit in N=p*q
Rounds	48	Based on key length
Block Size	64 bits	variance
Execution time	Slow	Slow

2.2. EyeOS

Is one of the most used web operating system which only needs (Apache, PHP5, and (MySQL) to be installed, with eyeOS the user can build his private cloud desktop. Using eyeOS web runner the user can open his eyeOS files from his browser with his local applications and save them automatically on his Cloud.

Is free and open-source cloud OS software that can be installed on any Web server. It provides an interface that is similar to that of a Linux distribution, Therefore, eyeOS can be accessed from anywhere, and view, edit, share all of our documents that are stored remotely, by using the web applications available. The user can work collaboratively with other users simultaneously in the same document. The eyeOS can be hosted as a private cloud [23], [24]. The eyeOS will be used as a private platform to implement and evaluate our proposed encryption algorithms. According to the displayed screen see Figure 4, we will be able to login to our cloud OS [25].

Figure 4. The login of eyeOS

3. PROPOSED METHOD

The symmetric encryption algorithm called 3DES and the asymmetric encryption 3kRSA algorithm has been applied has been implemented on a cloud operating system (EyeOS) as cloud platform Also, a comparative study between 3DES and 3kRSA has been done. The similar outcomes tracked down that the 3kRSA calculation beats the calculation as for the intricacy, and yield bytes. The principal disadvantage of the 3kRSA calculation is its calculation time and algorithms will be executed to scramble the information in the distributed computing environment. According to the work in this paper, the eyeOS will be used as a private platform to implement and evaluate our proposed encryption algorithm. The 3DES is used rather than the others because of its effectiveness. The DES calculation plays out a great deal of bit handling in stages called "trade" switches in every one of the 16 rounds. DES calculation encodes information in 64-bit block size and uses successfully a 56-bit key. 3DES calculation is a development of applying DES three times in grouping. The 3DES calculation have three diverse keys (Kl, K2 and K3) has viable key length is 168-bits (The utilization of three particular keys is suggested of 3DES).

3.1. Experiment environment

The cloud operating system (CloudOS) an operating system designed to operate within cloud computing and virtualization environments. A cloud operating system manages the operation, execution and processes of virtual machines, virtual servers and virtual infrastructure, as well as the back-end hardware and software resources. A cloud operating system primarily manages the operation of one or more virtual machines within a virtualized environment. Depending on the virtual environment and cloud services in use, the functionality of cloud operating systems varies. Cloud operating system developed to be used within a computing-specific environment will manage the processes and threads of a single or cluster of virtual machines and servers.

3.2. Encryption plaintext

In the first place, the 3DES and 3kRSA calculation packed the sender's plaintext report to lessen its size and fortifying its cryptographic security. The calculation made a key and afterward the meeting key is handled utilizing symmetric encryption calculation 3DES or 3kRSA which creates a mysterious key, the meeting key is utilized by encryption calculation to scramble the plaintext; the outcome is cipher-text. The

meeting key is scrambled to the beneficiary's public key, utilizing encryption 3DES and 3kRSA. This public key-scrambled meeting key is communicated alongside the cipher-text to the beneficiary. The encryption algorithm is explained in more detail it as shown in Figure 5: i) create the session key, ii) compress the plaintext with Zip compression algorithm, iii) encrypt the plaintext with session key using 3DES and 3kRSA algorithm to produce cipher text, iv) the result is a single package combined from cipher text and encrypted session key that is transmitted to the receiver, v) The key generation (3KRSA) takes places:

- Two of the indivisible numbers are picked including *p, q* and *r*. Modulus by sub 2 can be determined utilizing these numbers, for example, *n=p*q*2*.
- While being the public type, the third number e which cannot partition similarly is chosen. It shows prime pertinence to result of (*p*-1*), (q*-1*), (r*-1*).*
- The whole number d is a private type which can be determined from quotient ((*ed*-1))/((*p*-1) (*q*-1) (*r*-1)).
- The *n* and *e* are number pair of public keys. However, these are publically recognized qualities yet bumbling for the assurance of *d* from *e* and *n* in any event, when *q* and *p* are sufficiently incredible.
- The figure message *C* is delivered through a public key for the production of scrambled message *M*. For this reason, condition $C=M^e$ Mod *n* is utilized.
- The ideal code text is decoded by recipient while using private key and condition $M=C^d$ Mod *n*.

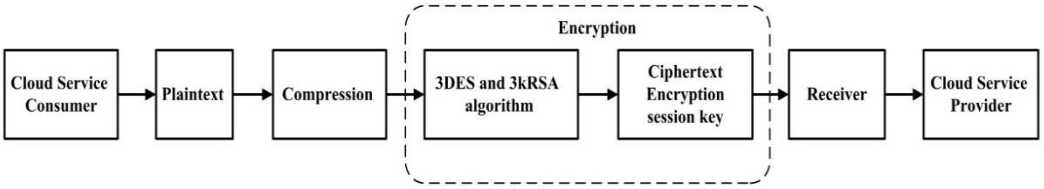

Figure 5. Flowchart of 3DES and 3kRSA encryption

3.3. Decryption cipher texts

The decryption phase is done in the reverse way of the encryption process. The recipient's copy of the proposed 3DES and 3kRSA algorithm uses his or her private key to recover the session key, and then the algorithm uses the session key to decrypt the encrypted cipher-text. The decryption algorithm is explained in more detail it as shown in Figure 6: i) decrypt the encrypted session key with private key of receiver using 3DES and 3kRSA decryption algorithm and ii) after the sent message the recipient will trail the steps given: i) private key *d* and *n* is used for the computation $M=C^d$ Mod *n*, ii) the integer descriptive *M* is extracted for plain text, and iii) decompress the decrypted text.

In this exploration, executed every one of the procedures are helpful for ongoing encryption. Every procedure is exceptional in its own way, which may be reasonable for various applications and has its own genius' and con's. According to explore in this exploration, executed every one of the procedures are valuable for ongoing encryption. Every strategy is interesting in its own way, which may be appropriate for various applications and has its own genius' and con's according to investigate.

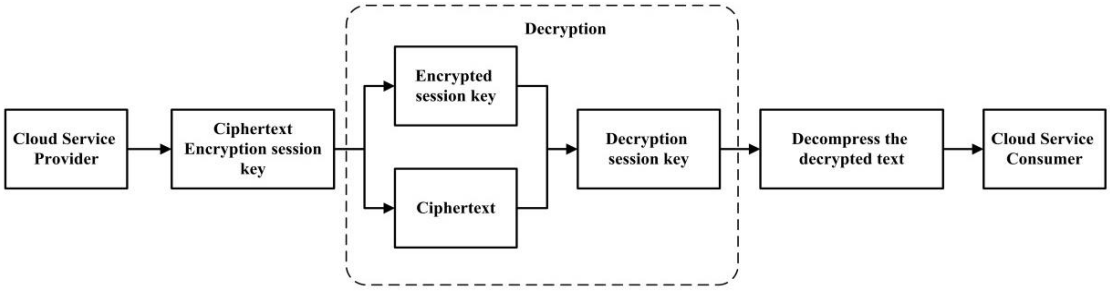

Figure 6. Flowchart of 3DES and 3kRSA decryption

4. RESULTS AND DISCUSSION

In this a comparative study between encryption algorithms 3DES and 3kRSA is done and implemented on the two types of the encryption algorithms have been implemented 3DES, and 3kRSA on the

eyeOS it is a private-cloud application stage with an electronic work area interface. Normally it is known as a cloud work area on account of its interesting graphical user interface (GUI). The interface was snappy "moving and switching apps", flawless. It is easy to upload and download files. The encryption processes have been done on the client side, so no passwords or content are transferred to the server. Sensitive data is saved into the eyeOS directories. According to 3DES and 3kRSA implementation, the performance of these symmetric encryption algorithms has been compared by encrypting input files with varying contents and sizes. The performance parameters and the performance evaluation of the proposed encryption algorithm are discussed, according to the comparative study results cloud OS. The performance parameters and the performance evaluation of the proposed encryption algorithm are discussed.

4.1. The simulator environment

EyeOS It is a private-cloud application stage with an electronic work area interface. Normally it is known as a cloud work area on account of its interesting UI. eyeOS conveys an entire work area from the cloud with document the executives, individual administration data instruments, and shared apparatuses and with the combination of the customer's applications. A standard WAMP/LAMP worker was utilized to introduce eyeOS, and code applications in PHP. That more applications will be available for the EyeOS platform in the long run eyeOS has a very interesting interface. The interface was snappy "moving and switching apps", flawless. It is easy to upload and download files.

4.2. The evaluating parameters

The performance of encryption algorithm is evaluated by considering the following parameters: i) computation time is the time that an encryption algorithm takes to produce a cipher-text from a plain text in case of encryption, also the time to produce plaintext from cipher-text in case of decryption; ii) output bytes is calculated by the size of output byte of cipher-text that is transformed from plaintext for each algorithm; and iii) time complexity used for the purpose of calculating the throughput of a cipher system and also indicates the speed of the cipher. The throughput of the coding scheme (*TE*) is calculated by dividing the total plain text in encrypted (megabytes) by the total output of the coding time and for each algorithm. Here, the higher the throughput, the higher the energy consumption of this coding technology.

$$TE=Tp/Et \quad (3)$$

Where *Tp* is total plain text (bytes), *Et* is encryption time (second). The time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the string representing the input.

4.3. Comparative study between 3DES and 3kRSA

First, the two types of the encryption algorithms have been implemented 3DES, and 3kRSA on the eyeOS. The encryption processes have been done on the client side, so no passwords or content are transferred to the server. Sensitive data is saved into the eyeOS directories. According to 3DES and 3kRSA implementation, the performance of these symmetric encryption algorithms has been compared by encrypting input files with varying contents and sizes (16.194, 24.933, 39.852, 44.904, 62.694, 71.395, 115.166, 135.065, 154.962, and 165.294 bytes). Table 2 represents the results of such experiments. According to the results of the comparative study, 3kRSA algorithm was found to outperform 3DES in encryption and decryption, it takes more time. According to the comparative study results, it is found that 3DES algorithm outperforms 3kRSA in terms of computation time by 56% but it is not outperformed by the level of encryption. The experimental results of implementing 3DES and 3kRSA algorithms are depicted in Figure 7.

Table 2. Comparative encryption time (milliseconds) of 3DES, and 3kRSA

No.	Input size	Time for 3DES	Time for 3kRSA	Percentage with respect to 3kRSA
1	16.194	18	45	52%
2	24.933	20	65	38%
3	39.852	28	75	42%
4	44.904	40	85	48%
5	62.694	48	95	52%
6	71.395	65	115	52%
7	115.166	68	125	50%
8	135.065	87	165	51%
9	154.962	89	185	53%
10	165.294	94	195	56%

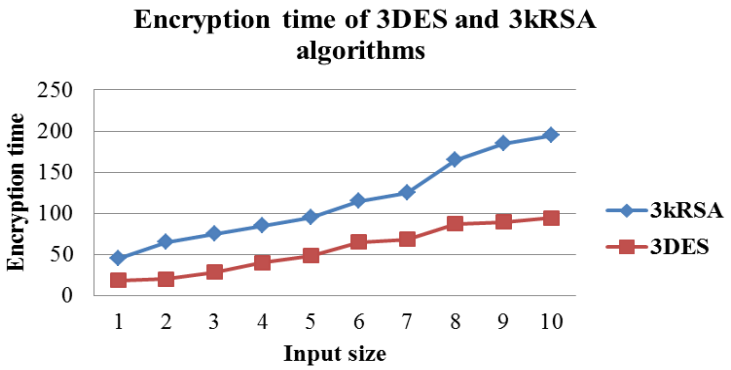

Figure 7. Encryption time of encryption algorithms 3DES, and 3kRSA

4.4. The comparative results

The security issues are a major issue for distributed computing advancement. To safeguard the protection of his information, the client should scramble information prior to being shipped off the cloud. Distributed computing security dependent on encryption, thought about productive plan to get information in distributed computing. This section describes the comparative results obtained after implementing the 3DES and 3kRSA encryption algorithms. The algorithms are implemented on cloud platform (eyeOS). It takes data input of size (25, 38, 66, 79, and 92 bytes). The algorithms are compared with each other using a set of parameters like computation time, output bytes and time complexity. Table 3 represents the computation time taken (encryption and decryption) and output bytes in the 3DES and 3kRSA algorithms respectively.

From Figure 8 which represents the computation time and output bytes of the two algorithms, it is noticed that 3kRSA consumes more time than 3DES. Output bytes in 3kRSA encryption are more than those bytes in 3DES encryption. 3DES algorithm is executed faster and with more throughput level as compared to the 3kRSA algorithm but 3kRSA is more Security efficiency algorithm than 3DES.

Table 3. Time taken (encryption and decryption) and output bytes in 3DES and 3kRSA algorithms

No.	Input Data Size(bytes)	Encryption		Decryption		Output bytes	
		Computation Time in 3DES	Computation Time in 3kRSA	Computation Time in 3DES	Computation Time in 3kRSA	In 3DES	In 3kRSA
1	25	8	10	4	35	36	65
2	38	4	8	6	51	52	97
3	66	15	35	17	75	92	161
4	79	20	43	22	88	115	180
5	92	28	49	25	102	140	195

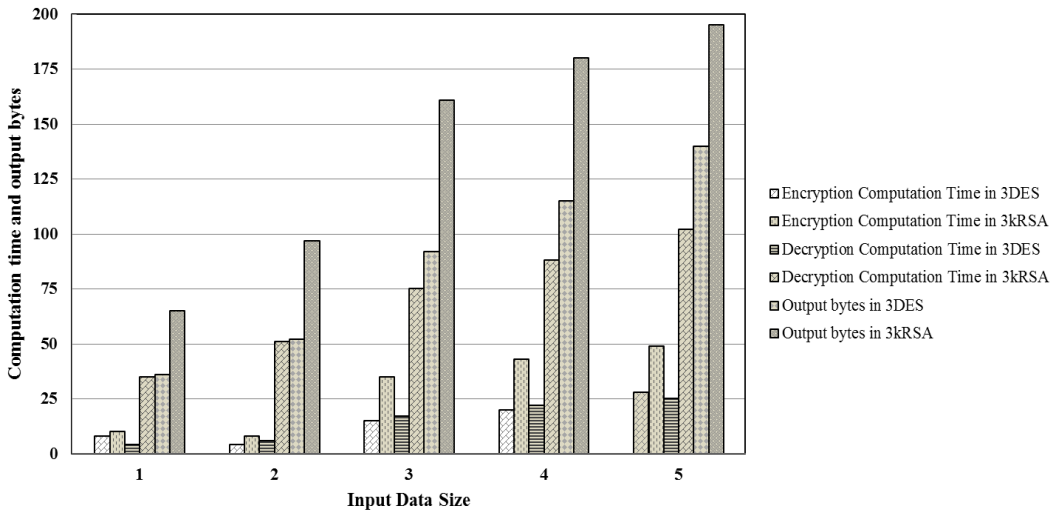

Figure 8. Computation time taken (encryption and decryption) and output bytes in 3DES and 3kRSA

5. CONCLUSION AND FUTURE WORK

The security issues are a major issue for distributed computing advancement. To protect the security of his information, the client should scramble information prior to being shipped off the cloud. Distributed computing security dependent on encryption, thought about effective plan to get information in distributed computing. This paper examined a portion of the current encryption plots and talked about the utilization of the most effective one, to get distributed computing information. Future work will focus on implementation and development of a method for data encryption that is important in the field of technology, where the principles of physics and quantum theories can be applied in place of mathematical equations in encoding and re-decoding data, since the "Q bit" units on which quantum physical theories depend are more capable and efficient in coding than the "Bit" units that depend on them. Mathematical equations, which in turn works to develop the results of actual use cases for the purpose of publishing them in all services (governmental, banking, military and security) to setup a more secure environment for data storage and retrieval.

REFERENCES

[1] S. Rani and A. Gangal, "Cloud security with encryption using hybrid algorithm and secured endpoints," *International journal of computer science and information technologies*, vol. 3, pp. 4302–4304, 2012.

[2] R. Buyya, "Cloud computing: the next revolution in information technology," in *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)*, Oct. 2010, pp. 2–3, doi: 10.1109/PDGC.2010.5679963.

[3] P. Guo, L. Ning, L. Su, and L. Bu, "A new strategy of resource management for cloud computing," *Information Technology Journal*, vol. 12, no. 17, pp. 3964–3969, Aug. 2013, doi: 10.3923/itj.2013.3964.3969.

[4] S. Pearson, "Privacy, security and trust in cloud computing," in *Computer Communications and Networks*, Springer London, 2013, pp. 3–42, doi: 10.1007/978-1-4471-4189-1_1.

[5] J. W. Rittinghouse and J. F. Ransome, *Cloud computing*. CRC Press, 2017., doi: 10.1201/9781439806814.

[6] A. Nayyar, *Handbook of cloud computing: basic to advance research on the concepts and design of cloud computing*, BPB Publications, 2019.

[7] A. Hameed *et al.*, "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems," *Computing*, vol. 98, no. 7, pp. 751–774, Jul. 2016, doi: 10.1007/s00607-014-0407-8.

[8] R. L. Krutz and R. D. Vines, *Cloud security: A comprehensive guide to secure cloud computing*, Wiley Publishing, 2010.

[9] S. S. Manvi and G. Krishna Shyam, "Resource management for infrastructure as a service (IaaS) in cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 41, pp. 424–440, May 2014, doi: 10.1016/j.jnca.2013.10.004.

[10] A. Shawish and M. Salama, "Cloud computing: paradigms and technologies," in *Inter-cooperative Collective Intelligence: Techniques and Applications*, Springer Berlin Heidelberg, 2014, pp. 39–67, doi: 10.1007/978-3-642-35016-0_2.

[11] M. B. C and K. B. Ramesh, "Novel holistic architecture for analytical operation on sensory data relayed as cloud services," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 4, pp. 4322–4330, Aug. 2020, doi: 10.11591/ijece.v10i4.pp4322-4330.

[12] R. L. Grossman, "The case for cloud computing," *IT Professional*, vol. 11, no. 2, pp. 23–27, Mar. 2009, doi: 10.1109/MITP.2009.40.

[13] R. F. Abdel-Kader, S. H. El-sherif, and R. Y. Rizk, "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3295–3306, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3295-3306.

[14] S. Shawkat, O. Abu-Elnasr, and T. Elarif, "Evolved algorithm to secure communication with steganography," *International Journal of Intelligent Computing and Information Science (IJICIS)*, vol. 17, no. 1, pp. 1–17, 2017.

[15] B. Bordel, R. Alcarria, T. Robles, and D. Martín, "Cyber-physical systems: Extending pervasive sensing from control theory to the internet of things," *Pervasive and Mobile Computing*, vol. 40, pp. 156–184, Sep. 2017, doi: 10.1016/j.pmcj.2017.06.011.

[16] S. Keelveedhi, M. Bellare, and T. Ristenpart, "DupLESS: Server-aided encryption for deduplicated storage," in *22nd USENIX security symposium (USENIX security 13)*, 2013, pp. 179–194.

[17] A. Gahan and G. D. Devanagavi, "A empirical study of security issues in encryption techniques," *International Journal of Applied Engineering Research*, vol. 14, no. 5, pp. 1049–1061, 2019.

[18] P. Kumar and N. Rajaanadan, "Data encryption and decryption using by triple DES performance efficiency analysis of cryptosystem," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 3, pp. 4030–4040, 2016.

[19] S. A. Shawkat and R. N. Ismail, "Biometric technologies in recognition systems: a survey," *Tikrit Journal of Pure Science*, vol. 24, no. 6, Nov. 2019, doi: 10.25130/j.v24i6.899.

[20] I. Al_Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. Lateef Al-badri, "Modified RSA-based algorithm: a double secure approach," *Telecommunication Computing Electronics and Control (TELKOMNIKA)*, vol. 17, no. 6, pp. 2818–2825, Dec. 2019, doi: 10.12928/telkomnika.v17i6.13201.

[21] S. H. Alibadi and S. B. Sadkhan, "A proposed security evaluation method for bluetooth E0 based on fuzzy logic," in *2018 International Conference on Advanced Science and Engineering (ICOASE)*, Oct. 2018, pp. 324–329, doi: 10.1109/ICOASE.2018.8548918.

[22] S. A. Shawkat, "Enhancing steganography techniques in digital images," *Faculty of Computers and Information, Mansoura University Egypt-2016*, 2007.

[23] D. G. Chandra and D. B. Malaya, "A study on cloud OS," in *2012 International Conference on Communication Systems and Network Technologies*, May 2012, pp. 692–697, doi: 10.1109/CSNT.2012.154.

[24] R. VidyaBanu, J. Preethi, and N. Dinesh, "Implementation of financial system using eyeOS in the cloud environment," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, Jun. 2011, pp. 656–660, doi: 10.1109/ICRTIT.2011.5972380.

[25] B. P. Rimal, A. Jukan, D. Katsaros, and Y. Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach," *Journal of Grid Computing*, vol. 9, no. 1, pp. 3–26, Mar. 2011, doi: 10.1007/s10723-010-9171-y.

BIOGRAPHIES OF AUTHORS

Shihab A. Shawkat received the B.Sc. degree in Computer Science from University of Tikrit in 2007 and M.Sc. Degree in Computer Science from Mansoura University in 2017. Mr. Shihab A. Shawkat worked as a teacher during the period from 2008 to 2019 in Directorate of Education in Salah Al-Din, Ministry of Education, Iraq. He has recently started working at the University of Samarra at the end of 2019 till now. His research interest lies in computer science, information security, image processing and AI. He can be contacted at email: shahab84ahmed@gmail.com.

Bilal A. Tuama M.Sc. computer science, University of Science USM (Malaysia). He is a Lecturer at the University of Samarra, College of Applied Sciences. His research interests include pattern recognition, software analysis, and design patterns. He can be contacted at email: Bilal.at@uosamarra.edu.iq.

Israa Al_Barazanchi received her Bachelor of Computer Science (BCS) from Department of Computer Science, Baghdad college of economic science university-Iraq-Baghdad in June 2002. In January 2010, she entered the master's program at the Faculty of Information and Communication Technology, Graduate School of Computer Science (Internetworking Technology), Universiti Teknikal Malaysia. She is Currently a student Doctor of Philosophy in Information and Communication Technology. She is a lecturer in Computer Engineering Techniques Department. Editor-in-chief for international union of universities journal. Member of editor board in many Scopus journals for computer science field. Head of researcher group. Member in many conferences panel and communications events. She is a Reviewer of various high impact factor journals. Her research activities are: WBAN, WSN, WiMAX, WiFi on vehicular ad-hoc networks (VANETs), communications, networking, signal processing, IoT, smart systems, and blockchain. She can be contacted at email: israa.albarazanchi@baghdadcollege.edu.iq; israa44444@gmail.com.