An Efficient Hybrid Cryptographic Model for Securing Information over Communication Network

Konyeha Susan[1] and John-Otumu A. M[2]
[1]Department of Computer Science, University of Benin, Benin City, Nigeria
[2]Department of Information Technology, Federal University of Technology, Owerri, Nigeria
susan.konyeha@uniben.edu, macgregor.otumu@gmail.com

Abstract

The importance of data security is very crucial in information networks and there is an ongoing search for better encryption and decryption technique with the focus on hybridizing algorithms. In this research paper, we present the design and implementation of a hybrid method which combines the advantages of the Rivest Shamir Adleman (RSA) algorithms and Data Encryption Standard (DES) for securing data transmission across information networks. The proposed method was achieved using Microsoft Visual C# programming language. The rate of decryption of the hybrid method was evaluated based on the time for encrypting and decrypting data, and throughput for different input text and image data samples. The results obtained demonstrated that the throughput of the hybrid method for data encryption (0.391MB/sec), is lower than that of DES alone (0.399 MB/sec), this means that, memory and CPU resources will be conserved for the data samples. Also, the throughput of the hybrid method for data decryption (0.330 MB/sec), is remarkably lower than that of DES alone (0.674 MB/sec), this means that the hybrid method for decryption, is much more secure than that of DES. Therefore, it is recommended that the developed hybrid method can be applied for enhancing data security in modern applications and communication networks.

Keywords: *Security, hybrid, Cryptography encryption, decryption, Information, Network.*

1. Introduction

In daily life activities, information plays an imperative function. The world at large has been reduced to a global village due to delivery and ease of access to information. According to [1], exchange of information is usually done by a traditional face to face culture. Topical advancement in information technologies, like the e-mail system and Internet has enabled the possibility for individuals to conveniently share insightful information across the world with powerful security measures in place. Internet being a global interconnectivity of computers and computer networks, over the years is increasingly becoming a ubiquitous means for exchange of information [2][3], providing reliable and effective platform for communication, including conducting business remotely [3][4]. For instance, information, in the form of text messages, computer files, to mention but two, can be exchanged via electronic mail, also known as email [3][5].

Despite the numerous advantages that the advances in Information Technology (IT) offer for information sharing, there are some challenges like the attendant issues. Messages on transit can be intercepted and accessed by an unauthorized agent. This phenomenon can be referred to as a failure of secrecy. When the information is altered without necessary authorization, we say there is a loss of integrity. Information can also be made inaccessible to authorized users. This habitually occurs when the media used for the processing, storage, retrieval, or/and transmission of the information is severely attacked.

The effect of disruption, loss, or damage to information and information systems are often invaluable to their proprietors. In many situations, the incessant survival of a business body depends to a very large degree on the security of its proprietary data or information. For example, in airline operations, a breach in the accuracy or safety measures of data could lead to serious loss of human lives. Data can be transferred from one point or host to another point / host or server. To ensure a secure data transfer is achieved, a few techniques of cryptographic measures can be enabled or deployed [6]. One of such approaches of cryptography is the mathematical transformation of data from readable text format to an unreadable format (encryption of data), which is normally prepared to be transmitted in that encrypted manner and also converted back to a readable format (decryption) whenever the data is needed for utilization.

The fundamental relevant structural design for a good number of IT systems, which includes the desktop computers and internet, does not warranty a total security measure. Malicious users with very devilish intentions always have a way or the other for exploiting one defenselessness or another. An attack that can compromise the secrecy of information over and over again opens the platform up to compromise the truthfulness of such information. It should be noted that if such information is intercepted on transit by an attacker, the information will be very meaningless since the attacker may not be able to make out sense from the content of the information. Hence, it is always advisable to guarantee that all relevant information is properly secured before transmission is done; so that the information will be useless or meaningless whenever an intruder or unauthorized user hijacks or intercept it thereby maintaining the confidentiality and integrity of the information. Therefore there is a need for hybrid encryption and decryption algorithms for safer data management. At present the RSA algorithm seems to be the most successfully in use technique for securing information and passwords. The key length of the RSA varies from 64 to 1024 bits.

A variety of studies and investigate has been conducted over the recent past to analyze and compare performance of different algorithms for cryptography.

In [7] authors analyze a range of symmetric encryption approaches by performing critical comparative evaluation based on certain criteria like execution time, avalanche effects by varying key, and so on. In [8] authors worked on enhancement of data security by using hybrid cryptography technique. In their work they made use of double symmetric cryptographic algorithms (DES-AES) to form a hybridized system. Their result shows that the developed hybrid model has higher encryption time than AES and DES counterparts; hence it will take a longer time to be broken by cryptanalyst than DES or AES alone. Their result was in conformity with the one obtained by [9] whose work is on secure data transmission using AES-DES hybrid algorithm. The major limitation of both research works is on the issue of key management because two symmetric techniques were used.

Based on the review of past research works on various data encryption techniques; it can be seen that DES has improved features in terms of execution time, throughput and power consumption while RSA algorithm on the other hand seems is to be the most thriving in use for keys ciphering and passwords. If both algorithms are combined to form a hybrid technique, this will boost data security in computer and other communication networks.

Designing encryption/ decryption systems, along with other methods will advance the security of data networks, as it requires an assessment on the purpose of the software, and the selection of cryptographic algorithm that could be adopted. This will both cater for the contextual and functional local software environments. The pleasant appearance of the system

is as a result of its functionality supports, while the type of cryptographic algorithm essentially determines the security class of the developed system.

Hence, this will form the main element of the system design. Presently, there are lots of accessible free to use and licensed encryption/decryption systems. This hybrid system when designed and implemented will make for faster encryption and decryption compared to asymmetric cryptography, such that it can be applied to applications that involves transport of huge data and instances where safety measures is of the most essence.

2. Related Works

In [10] authors proposed a secure technique by which the cloud service provider cannot openly get to partial data using an intelligent cryptography technique. The technique is meant to defragment a file and autonomously store the data in the dispersed cloud servers. The experimental results revealed that the proposed technique can efficiently guard key security threats from the clouds environment.

In [11] authors proposed a model based on the blind intermediaries principles. The model is characterized by a wide-ranging technique to e-voting. The developed algorithm was implemented using C#.Net Framework which communicated other a network. The efficiency and the areas for improvement of the developed system were well noted.

In [12] authors proposed a tough cryptographic based scheme that could solve the issues of data privacy disclosure. The system presented a fresh architecture for data consumer digital identity based on three most important components. The components are namely: ABE, PRE, and public key infrastructure (PKI). Results revealed that the proposed digital identity solves the scalability challenges faced by existing works and achieving data management for consumer and data owners in a simple way. It also removes the need for online existence of data owner and consumer in order to share any information. Finally, the system was able to guard against hive dropping attacks.

In a study by [13], a new cryptographic model that uses joined map lattice was projected for securing images. The proposed model integrated a mix based on sub-keys based substitution, randomly generated secret key, confusion algorithm and coupled map lattice based diffusion process to improve the security, understanding and toughness of the technique. The results revealed an average of 99.63% NPCR score and 33.46% UACI, which suggests the model as very promising candidate for encryption of images.

In [14] authors also suggested a hybrid cryptographic approach to sustain cyber security infrastructure. The hybrid model is a fusion of DES and RSA algorithm which uses asymmetric key process that is both the sender and receiver uses identical key pair for both processes of encryption and decryption.

In [15] authors developed a unique hybrid encryption model using Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) features for storing information in a database. The experimental outcome shows that the novel model has a level of overhead performance and also offers a secured approach for organizations

In [16] authors presented a novel method based on compound right translated AES Gray S-boxes (RTSs) and phase embedding technique for image encryption. The decryption procedure of the cryptosystem used a host image for generation of masks, which is indeed essential for securing the host image from unlawful persons. The potency of the security

model was calculated by executing it on different images. Results revealed that the novel cryptosystem developed is safe.

In [17] authors developed a cryptographic based algorithm for securing messaging in both android and the web platforms in order to prevent attackers from hijacking messages and its full contents. The proposed model was tested for video conferencing, chatting, messaging, and synchronized file sharing in both web and android platforms. Test results also revealed the application to be secure for messaging systems.

In [18] authors proposed a secure model for storage and retrieval of medical images stored in cloud using visual cryptographic technique such as AES technique that is based on the fact that attackers can easy retrieve patients medical data stored over cloud platform. Results revealed that the system proposed is able to securely store and retrieve medical images with high quality.

3. Methodology

The main method adopted in this research work is a fusion of the strength of DES and RSA algorithms, to form a hybrid method for securing data transfer over an information network.

3.1 The DES Algorithm

The basic process in encrypting a data of 64-bit with a 56-bit key using the DES algorithm as shown in Fig. 2, consist of three main stages according to [9].

(i) An initial Permutation
(ii) A multifaceted key dependent computations of 16 rounds
(iii) And finally, the reversal of the initial permutation was done

The DES algorithm takes an input of 64-bit long readable text (or a multiple of 64 bits) data block and 56-bit key (8 bits of parity) and generates an output of 64-bit block of unreadable text (ciphertext). If the input data was less than or greater than 64 bits, it pads the final block of such input data with some standard pattern of zeros, ones, or sometimes alternates between ones and zeros, to make it a full block (64-bit block). The readable text (plaintext) block will then be exposed to an Initial Permutation (IP) to shift the bits. The 8 parity bits were disconnected from the key by exposing the key to its Key Permutation thereby reducing the 64-bit key to 56-bits. After initial permutation has taken place, the readable text (plaintext) and key are processed together in an operation of 16 rounds as given below;

(i) The key was splitted into two halves consisting of 28-bit and each half of the key was shifted (rotated) by one or two bits, depending on the round.
(ii) The halves were fused together again and subjected to a density permutation to reduce the key from 56 bits to 48 bits. This condensed key was used to encrypt this round's readable text block
(iii) The rotated key halves from (ii) were used in next round. The data block was splitted into two halves; the left half (lh) and the right half (rh), with both halves having a 32-bit block of data. One half (rh) was subjected to an expansion permutation to increase its size to from 32-bits to 48-bits.
(iv) The output of step (vi) was XORed with the 48-bit compressed key from (iii)
(v) The output of step viii was now compressed to reduce the 48-bit block down to 32-bits.
(vi) The output of step (viii) was XORed with other half (lh) of the data block.

(vii) The two data halves were swapped to become the next round's input.
(viii) The entire process was repeated for sixteen times to get sixteen rounds of key dependent operations. The ith round of the computation is describe as by (equation 3.1) and (3.2)

This process was repeated for sixteen times to get sixteen rounds of key dependent operations. The ith round of the computation is describe as by (3.1) and (3.2)

$$L_i = R_i - 1 \qquad for\ 1 \le i \le 16 \tag{3.1}$$
$$R_i = L_i - 1 \ \blacksquare f(R_i - 1, k_{i)} for\ 1 \le i \le 16 \tag{3.2}$$

Where L is the left half, R, is the right half and, k is the key. , i is an integer showing the number of rounds; whose values ranges from 1 to 16. The result of the 16th round was reversed, obtaining the sequence R_{16} L16. After the 16th round, The 32 bits sequence of the right half and the left half were combined together and was subjected to a final permutation (inverse of the initial permutation) to produce the cipher text.

3.2 The RSA Algorithm

The process involved in RSA algorithm is about key generation. The RSA Key Generation Algorithm involves the steps listed below;

Algorithm
i) Random numbers were first generated by the program using a pseudo random number generator.
ii) The algorithm selects two different large prime numbers p and q.
iii) These chosen numbers were checked whether the numbers is a prime using primality test. A lot of primality testing algorithm was available in literature, but for this research the primality test command in C# was used. If p and q passes the primality test, then the algorithm proceed to stage (iii), otherwise, it returns to stage (ii) to select another p and q. For security, p and q must be of the same length in bits, they must not be equal and they should not be too close to each other for security, that is, p-q should not be a small number. After p and q have passed the primality test, the algorithm moved to the next step, that is, stage (iv)
iv) The multiplication of p and q were computed and attributed to n, that is,

$$n = p \times q$$

The Euler's quotient function
$z(n) = (p-1) \times (q-1)$ Was also computed
(vi) The algorithm then chooses an integer e (encryption key), such that

$$1 < e < z(n) \text{ and gcd (e,z(n))=1.}$$

This means that e and z(n) must share no common factors other than 1, that is, e is relatively prime to z(n).

The choices of e are 3,5,17,257 and 65537 which were derived from the Fermat theorem given by the following equation:

$$F(x) = 2^{2^x} + 1$$

Where x ranges from (0…….. 1 –N). The first five Fermat numbers F_1, F_2, F_3, F_4, are called Fermat primes and the corresponding values were given above. The number F_5 and above are not prime. In order to enhance the effectiveness of encryption, it is advisable to choose a small encryption exponent e; which when put into practice, it could be 3=e or 23567

is commonly used. The RSA encryption algorithms with small exponent *e*, are significantly faster [15].

(vii) After a value for e, have been successfully chosen the algorithm computes the private (decryption key) d , to satisfy the Extended Euclidean Algorithm is given as d*e = 1modz(n) From the expression,

$$d = e^{-1}1modz(n)$$

(viii) The pubic key is (n, e), and the private key is (n, d). Note the values of d, e, p, q and z(n) must be kept as secret.

4. Results and Discussion

4.1 The Hybrid Technique Implementation

Fig. 1 shows the hybrid technique. The Data Encryption Standard (DES) encryption algorithm was used to encrypt the data to be transmitted (plain text P) with the assistance of a randomly generated session key k in the transmitting side of the technique, turning it into a cipher text, C. The resulting cipher text is given by

$$C = E(k, p) \quad (4.1)$$

The pseudorandom number generator was used to generate the session key. Since DES technique or algorithm is a secret key system, the session key was encrypted using Rivest Shamir Adleman (RSA) algorithm with the help of the recipient public key, e in order to keep the key secret. This process will produce an encrypted session.

key u, given by (4.2)

$$u = k^e(mod(n)) \quad (4.2)$$

Where n is the multiplication of two randomly generated large prime numbers p and q used in the RSA algorithm. The cipher text C, and the encrypted session key u, were then sent to the receiver over a communication channel.

At the receiving end, the private key of the recipient d, was used with the RSA decryption algorithm to decrypt u, thereby producing the session key as given by (4.3),

$$k = u^d(mod(n)) \quad (4.3)$$

Haven retrieved back the session key; the session key was then used alongside the DES decryption algorithm to get the original data (plain text P) according to

$$P = D(C, k) = D(E(P, k), k) \quad (4.4)$$

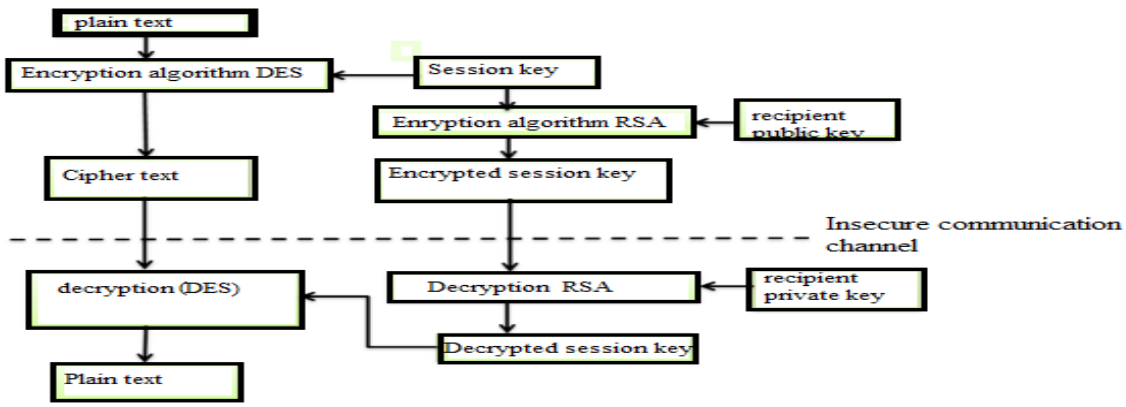

Fig. 1: The developed DES-RSA Hybrid Technique

The hybrid technique was then implemented using C# programming language on a computer system with the following system specification;

(a) Processor Speed: Intel (R) Atom CPU N270 @ 1.60GHz
(b) RAM: 1GB
(c) O. S.: Windows 7 Ultimate, 32-bit.

Ten (10) different data samples of text with (.txt) extension and images with (.jpg, jpeg and png) extension, of varying sizes were entered into the hybrid system. There are selection options for DES, RSA and the Hybrid technique, so that the algorithm type can be easily selected to encrypt and decrypt data. The encryption and decryption time for each data size were recorded for each technique accordingly. The different metrics that were used to evaluate the performance of the system includes; the encryption and decryption time (in millisecond), throughput (in MB/Sec), the average data rate (in KB/Sec), and central processing unit (CPU) power consumption [19].

The average data rate (ADR) was calculated using (4.5), given by

$$ADR = \frac{1}{N_b}\sum_{i=1}^{N_b}\frac{M_i}{t_i} \quad (4.5)$$

Where N_b is the number of message to be encrypted /decrypted, M_i is the size of the message in (kb) and t_i is the time taken to encrypt/decrypt a given message (in millisecond). The encryption ratio (ER) was computed using,

$$ER = \sum\frac{L_y}{L_x} \quad (4.6)$$

Where L_y, is the size of the encrypted data (the ciphertext) and L_x, is the size of the original plain text. The throughput T, of the system was then computed using

$$T = \frac{P_t}{E_t}、 \quad (4.7)$$

Where P_t, is the size of the total plaintext to be encrypted/decrypted (in MB) and E_t , is the total encryption/decryption time (in millisecond). The throughput of an algorithm is inversely proportional to the CPU power consumption; so the throughput was used to calculate the CPU power consumption of the developed technique.

Next, a hash function was now used as part of the evolving procedure of the hybridized encrypted data as adopted from [20]. This served as a check segment for integrity of the encrypted data. The cryptographic hash function is parameterized by a secret key. The exterior performance of a cryptographic hash function is defined as:

$$h = H(M) \quad (4.8)$$

and of a keyed cryptographic hash function is given by:

$$h = H[K](M) \quad (4.9)$$

The hash result h consists of a bit string of a particular length represented by nh. In the hashing of long mails or messages, it may not be inappropriate to keep the final message during the addition of the hash result. However, this is no problem for applied cryptographic hash function proposals because they all operate in a sequential manner, so that the messages can be hashed immediately without the need for any external storage.

Many existing cryptographic hash function applications can be described by the succession of the following operations [20]:

1. Dissection: where the input is divided into a number (denoted by s) of blocks mi of equal length and the last, generally incomplete, block ms is expanded in a unique and adjustable manner;
2. Initialization: the original chaining state d^0 is set equal to a value IV fixed by the requirement described;
3 Iteration: the chaining state is updated serially by a chaining change G for all message blocks, starting from m1 and ending with ms;
4. Outcome: the hash serial keyed cryptographic hash function is described by

$$(d^0,\kappa) = J(K) , \quad (4.10)$$
$$d^i = G[\kappa](d^{i-1},m^i) , \quad (4.11)$$
$$h = G_o[\kappa](d^s) . \quad (4.12)$$

For a serial non-keyed the result is calculated from the final chaining state by the output transformation G_o.

The hash function chaining is given by:

$$d^0 = IV, \quad (4.13)$$
$$di = G(di-1,mi), \quad (4.14)$$
$$h = G_o(d^s), \quad (4.15)$$

In some projects, the length of the input is attached in the padding process away from attacks created on lasting points. This was achieved by using a counter module in the change chain process. If it is spotted that the final (incomplete) block arrives, the change chaining process will complete the padding operation before the chaining state is updated.

4.2 The Hybrid RSA-DES Cryptosystem Graphical User Interface (GUI)T

The user interface is presented below, with the tabs where the cipher, VIN, candidate name and other features are entered. Fig 2 shows the input values of a test case scenario
s

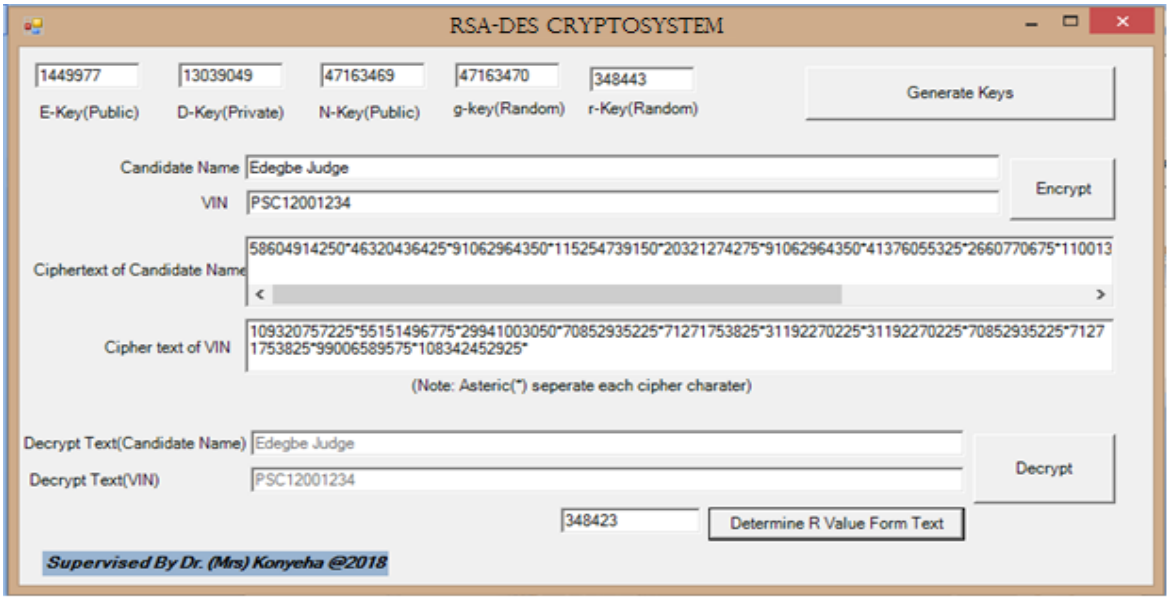

Fig. 2: The developed hybrid cryptosystem GUI

The Data Encryption Standard (DES) and the proposed Hybrid technique were developed and implemented in Microsoft Visual C# Environment. Figures 3 and 4 shows the plot for the encryption and decryption time for the various sizes of the input text data samples for both DES and the developed hybrid technique.

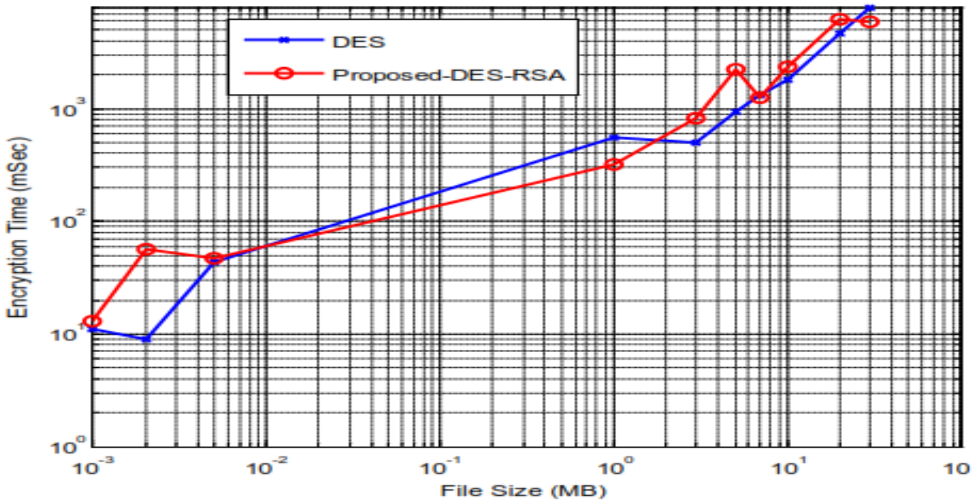

Fig 3: Encryption time for both DES and the Hybrid method for text data samples (Both axes are logarithmic).

From Fig. 3, it can be observed that, the developed hybrid method has a little bit higher encryption time than DES especially for file size above 1MB. This means that it takes a little more time to encrypt data with the developed hybrid technique than encrypting with DES only. This is as a result of computational complexity of the hybrid technique since it combines two algorithms together. The decryption times for the two methods are almost the same.

Fig. 4 and Fig. 5 respectively show the encryption and decryption time for a variety of sizes of image data samples for both DES and the developed hybrid model. From the figures, it is noted that for image data samples, the hybrid method has higher encryption and decryption times than the DES, which is also significant.

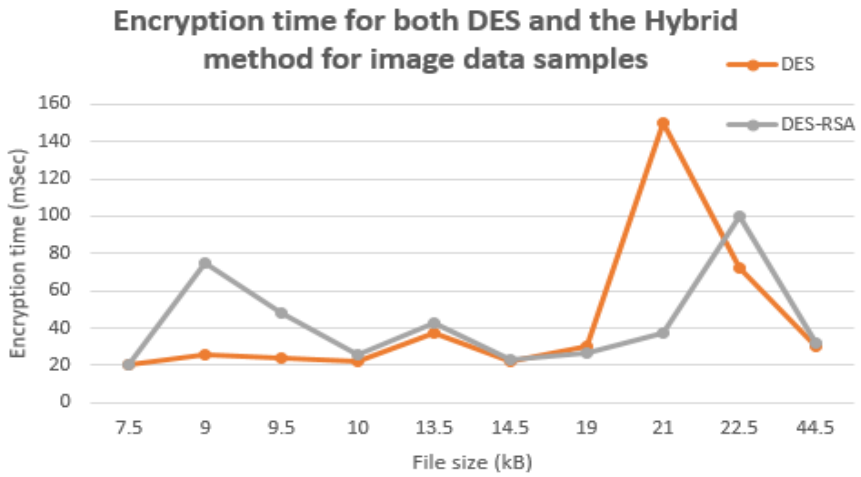

Fig 4: Encryption time for both DES and the Hybrid technique for image data samples

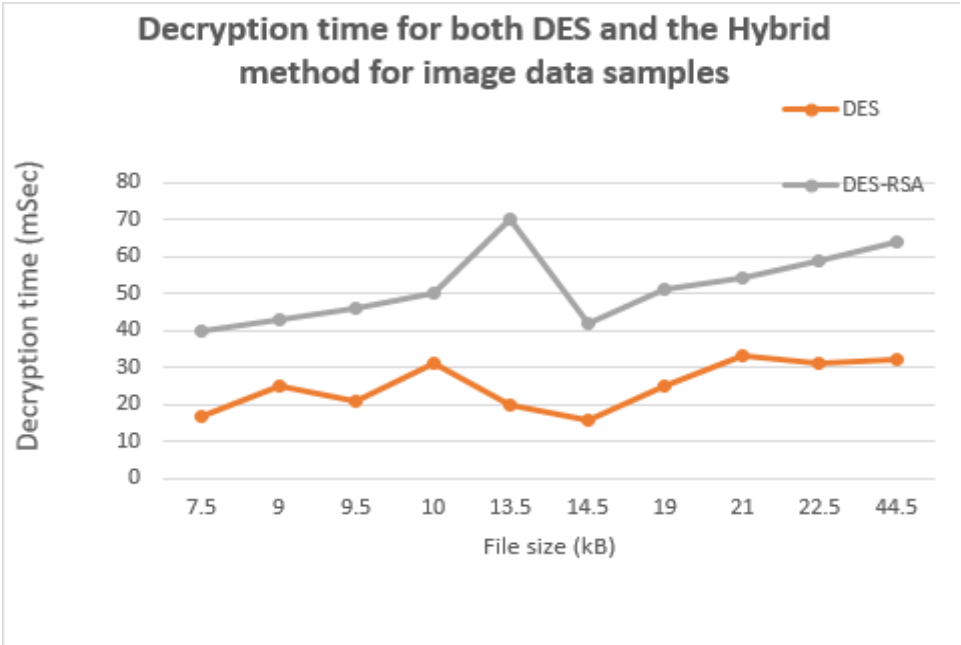

Fig 5: Decryption time for both DES and the Hybrid technique for image data samples

Table 1 show the results for the throughput of encryption and decryption, average data rate of encryption and decryption for the different data packet size of plaintext (txt) and images (jpg, jpeg, and png) respectively, for both DES and the developed hybrid technique.

From Table 1, it can be observed that the throughput of the hybrid technique for encryption of data is lower than that of DES alone, but for decryption, its throughput is higher than that of DES. The implication of this is that, the hybrid technique will consume or draw more power from the central processing unit (CPU) during encryption, but lesser power during decryption.

This is because the throughput of an algorithm is inversely proportional to the CPU power consumption. It can also be seen from the table that both techniques have the same encryption ratio, which indicate a little increase in the size of the ciphertext with respect to the size of the input data. Both techniques produce the same size of ciphertext after file encryption.

Table 1: Other performance criteria used for encryption and decryption for image file input

Performance criteria	DES	DES-RSA (hybrid system)
Encryption throughput (MB/sec)	0.399	0.391
Decryption throughput (MB/sec)	0.674	0.330
Average data rate of encryption (KB/sec)	533.82	474.43
Average data rate of decryption (KB/sec)	659.20	318.27
Encryption ratio	1.918	1.918

From Table 1, it can be observed that the throughput of the hybrid method for encryption of data (0.391MB/sec) is lower than that of DES alone (0.399 MB/sec), this means that, less memory will be consumed for the image data samples. However, the throughput of the hybrid technique for decryption of data (0.330 MB/sec) is remarkably lower than that of DES alone (0.674 MB/sec), this means that the hybrid technique for decryption, is much more secure than that of DES. This can easily be realized if a time out mechanism is combined with the hybrid method.

The hybrid method average data rate value, for image and text file data, was low when compared to that of DES for both encryption and decryption. This means that, for the image data samples, the hybrid technique developed will consume less memory and CPU resources for encryption operation (533.82 KB/sec, 474.43 KB/sec). and decryption operation (659.20 KB/sec, 318.27 KB/sec).

The value of Encryption ratio for both the DES and hybrid method was found to be the same (1.918), indicating that the key lengths and the key management method for both DES and hybrid method are the same.

5. Conclusions and Future Work

From this study, the combined concepts of DES and RSA to form a hybrid technique have been achieved and presented. The performance of the developed hybrid (DES-RSA) have been evaluated and compared to the DES and RSA algorithms. The results show that the hybrid technique developed is better in terms of speed of encryption, throughput and CPU power consumption usage.

Therefore, it can be concluded that the hybrid technique developed will be a suitable choice for encrypting data in modern applications and for information systems.

At this juncture, the researchers will like to say that data/ information security over communication networks or standalone systems is still an ongoing research work as so many security threats comes out on a daily basis. The researchers will like to recommend that further research work should be done using other cryptographic algorithms and artificial intelligence concepts to meet with the changing nature of the security threats.

References

[1]. Meyer, H. W. J. (2000). *The transfer of agricultural information to rural communities.* Unpublished doctoral dissertation, University of Pretoria, Pretoria, S. Africa.

[2]. Adesanya, O. (2004). The impact of information technology on information dissemination. In Madu, E.C. and Dirisu, M.B. (Eds.), *Information science and technology for library schools in Africa* (pp.10-24). Ibadan, Nigeria: Evi-Coleman.

[3]. Ogbomo, M. O. and Ogbomo, E. F. (2008). Importance of Information and Communication Technologies (ICTs) in Making aHealthy Information Society: A Case Study of Ethiope East Local Government Area of Delta State, Nigeria. *Library Philosophy and Practice 2008,* ISSN 1522-0222, pp 1 – 8.

[4]. Woherem, E.R. (2000). Information Technology in the Nigerian Banking Industry,Ibadan, Nigeria: Spectrum Books.

[5]. Nwosu, I. (2004). Digital public relations: concept and practice, In Nwokocha, J. (Ed.). *Digital public relations: New techniques in reputation management* (pp. 33-34). Lagos, Nigeria: Zoom Lens Publishers.

[6]. Lama, S.,and Ishank,S. (2013). Data Security Using RSA Algorithm in Matlab, International Journal of Innovative Research and Development, 2: 479 – 481.
[7]. Himani A and Marisha, S (2012). "Implementation and Analy-sis of Various Symmetric Cryptosystems", *Indian Journal of Science and Technology,* vol. 13, pp.1173-1176, 2012. Available online at http://www.indjst.org
[8]. Jigar, D, Neekhil C and K. Bhagyashri,(2013) "Enhancing Data Security by Using Hybrid Cryptography Algorithm", *International Journal of Engineering science and Innovative Technology,* vol. 2, issue 3, pp. 221-228, 2013.
[9]. Jignesh,S., Rajesh, B., and Vikas, K. (2012). Hybrid Security Algorithm for Data Transmission using AES-DES, International Journal of Applied Information Systems, 2: 15 – 21.
[10]. Li, Y., Keke, G., Longfei, Q., Meikang, Q., and Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing, Information Sciences, 387: 103 – 115.
[11]. Liudmila B., Ilya, P., and Oleg, M. (2017). A model of a secure electronic voting system based on blind intermediaries using russian cryptographic algorithms, In Proceedings of the 10th International Conference on Security of Information and Networks, October 2017 Pages 45–50, https://doi.org/10.1145/3136825.3136876
[12]. Ibrahim, M. M., Sherif, H. N., Rania, E., Hossam, F. and Mostafa, G. M. (2017). A robust cryptographic-based system for secure data sharing in cloud environments, Security and Communication Networks, 9:6248 – 6265, DOI: 10.1002/sec.1770
[13]. Sunil, K., Manish, K., Rajat, B., Das, M. K., and Sanjeev, S. (2018). A cryptographic model for better information security, Journal of Information Security and Applications, 43: 123 – 138.
[14]. Vivek, K., and Rahul, Y. (2015). A Hybrid Cryptography Technique to Support Cyber Security Infrastructure, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 4(11): 2278 – 1323.
[15]. Onyesolu, M. and Ogwara, N. (2017), 'On Information Security using a Hybrid Cryptographic Model', IRJCS: International Research Journal of Computer Science, 4(11): 15-22.
[16]. Naveed, A. A. (2017). A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding, Security and Communication Networks, 1 – 9.
[17]. Rahman, M. M, Akter, T., and Rahman, A. (2016). Development of Cryptography-Based Secure Messaging System. Journal of Telecommunication Systems and Management 5: 142. doi:10.4172/2167-0919.1000142
[18]. Bincy, J., and Senthilnathan, T. (2019). An Efficient E2C2 Visual Cryptographic Technique to Secure Medical Images in Cloud Environment, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(2): 2278 – 3075, DOI: 10.35940/IJITEE, B6491.129219
[19]. Adedeji K. B. and Ponnle A. A. (2014). A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development, International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 5, Issue 10, pp 804-816.
[20]. Daemen, J. (1995). Cipher and Hash Function Design Strategies based on linear and differential Cyptanalysis.