Indonesian Journal of Electrical Engineering and Computer Science
Vol. 20, No. 1, October 2020, pp. 521~527
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v20.i1.pp521-527

Improve the security of transfer data file on the cloud by executing hybrid encryption algorithms

Samar Zaineldeen[1], Abdelrahim Ate[2]
[1]School of Management, Jiangsu University, Xuefu Rd, JingKou, China
[2]Control department, Alneelain University, Sudan
[2]Department of Mechanical and Electrical Engineering, Dezhou University, China

Article Info

Article history:

Received Jan 17, 2020
Revised Mar 25, 2020
Accepted Apr 11, 2020

Keywords:

AES
Cloud computing
Cryptography
DES
Encryption
Security

ABSTRACT

Cloud computing is a model of sophisticated computing which has a strong effect on data innovation. Cloud computing offers remote access to shared computerized assets in the stored cloud. Operationally cloud servers utilize Web services that give enormus advantage to the user in a variety of applications such as banking and finance, storage, social networking and e-mail. Cloud computing accomplishes many of the features interrelated to elasticity, ease of utility, efficiency and performance with low cost. There are a number of potential concerns related to security and privacy since the requirement to protect cloud computing expanded, the encryption algorithms play the key part in data and information security systems, on side these algorithms consume a considerable quantity of computing resource. This paper,presenting a new hybrid encryption algorithm emphasising on AES and Enhanced Homomorphic Cryptosystem (EHC) as a hybrid encryption to guarantee the secure exchange of data between the user and the cloud server, and compression study for two proficient homomorphic encryption techniques for encoding Data Encryption Standard (DES), Advance Encryption Stander (AES). With The proposed techniques an evaluation has been conducted for those encryption algorithms at diverse file sizes of data, to evaluate time taking for encryption and decryption, throughput, memory consumption and power consumption. The major finding was thats the proposed method has the extremity throughput, memory consumption and our proposed work took advantage of the least time taken in sec for encryption and decryption.

Corresponding Author:

Abdelrahim Ate,
Department of Mechanical and Electrical Engineering,
Dezhou University, Dezhou, Shandog, China.
Email: wadalroob@gmail.com

1. INTRODUCTION

Cloud computing is described by NIST as a model for configurable computing assets (e.g., servers, storage, services, network, and applications)to empower and provide network access that is demand-driven. Computing assets could be speedily delivered with minor interaction and effort by administration [1]. The embracing of cloud computing services by clients is restricted due to considerations concerning the misfortune of secret information's value and it's privacy [2]. For storing data in cloud server, standard encryption methods are used to make sure there is security of transition of this dataprocess to the cloud. Security is the most vital issue of cloud computing, to attain security of data, a variety of cryptographic algorithms are used to encode and decode the data. However, the cryptography algorithms with higher security but low performance are insufficient and unacceptable.

Numerous coding algorithms are used and expatiated obtainable in data security. The algorithms can be classified into Asymmetric (public) and Symmetric (private) key encryption. One key is utilized to unscramble or scramble the information in secret or Symmetric key encryption. It should be spanned prior to broadcasting between entities. Keys has an essential part; a weak key may result in data compromised in the hands of unauthorized persons. Symmetric key encryption depends on the magnitude of the key. Using lengthy key encryption is trickier to decode than the one which uses a shorter key for the comparable algorithms [3].

Key distribution problem is resolved using asymmetric or public-key encryption. Private and public key is used for Asymmetric encryption. The private and public key function is to scramble and unscramble respectively because users make the use of 2 keys: private key, that only the user has knowledge about and public key which the public knows. It's not essential to span them before the transmission [3]. Mathematical functions and intensive computations are used to determine public key encryption which doesn't work well with phones [4].

1.1. Data encryption standard

DES is distinguished by its high decryption and encryption effectiveness with a shorter key length. It's a traditional symmetric encryption algorithm [5]. NIST suggested DES as the first encryption standard, it's a 64 bits block and key size. The round key size is 48 bits. In its entirety the plaintext is separated into blocks of 64bit size; the final block is padded if needed. Substitutions and many permutations are used throughout in order to raise the difficulty of performing cryptanalysis on the cipher. DES algorithmis comprised of 2 permutations (P-boxes) and 16 Feistel rounds. The whole operation can separate into three phases. The initial phase is preliminary permutation and final phase is the last permutations [6] Since the introduction of DES, there has been a number of attacks on systems utilizing it, exposing its vulnerabilities, making it an unconfident block cipher [7, 8]. To decipher this, a triple DES also written as 3DES encryption technique was suggested to overcome shortcoming of DES in [9], this technique stretched the length of key from 56 to 112 bits, but still, algorithm's software implementation is ineffective. With subsequent progress of encryption techniques, Data Encryption Standard has progressively been substituted by the AES, that is exceedingly safe, accomplished and trustworthy.

1.2. Advance encryption stander (AES)

Is a block cipher. Its key length varies between 256, 192, or 128 bits. It encodes 128 bits data blocks in 10, 12 and 14 rounds according to the key length. Advanced Encryption Standard is the most certified symmetric encoding algorithm. It operates computation on bytes instead of bits and runs plaintext blocks of 128 bits as 16 bytes. Matrix of 4 rows and columns are prepared for these 16 bytes. It operates on whole data blocks by using substitutions and permutations. The size of key AES cipher use designates the transformation rounds quantity used in the encryption process [10] American Encryption Standard encryption is immediate along with being expandable; we can implement it on diverse platforms such as tiny devices [11]. Its also used in many of defense applications [7, 12].

1.3. Enhanced homomorphic cryptosystem (EHC)

Homomorphic encryption permits the use of mathematical operations on encrypted data so that the decryption result would be in line unencrypted data, when similar operations are applied [13] low effectiveness of calculation and lengthy key sizes are disadvantages of EHC [14], There are some EHC encryption schemes illustrated in [15]. EHC, Homomorphic encryption, proposed by Gorti et al. [16] in 2013 empowers a secured environment where operations are conducted on earlier encrypted data and the identical result is acquired as original data [17].

In recent times, homographic cryptosystems have been commonly used in many applications. Private keys r,q, and p are used by the algorithm at EHC encryption. These keys are lengthy which is why they need extensive time and effort to breach them. For each encryption procedure, the private key is arbitrarily created, ensuring that in reality similar plaintext doesn't result in similar ciphertext, this phenomenon prohibits any unintended person from cracking ciphertext [16].

Enhanced Homomorphic Cryptosystem is a fully homomorphic cryptosystem which provides equal multiplication and addition. It consumes less power and memory plus the decryption takes less time. This paper focuses on enhancing the security of the data transferred to the cloud by implementing hybrid coding algorithms using EHC and AES128 to conserve the confidentiality of data and information, taking into consideration the time taken of coding and decoding, throughput, and power memory consumption.

2. THE PROPOSED WORK

2.1. AES encryption algorithm

2.1.1. Encryption profile/used

DES algorithm is gradually superseded by AES and has emerged as a modern generation data encoding standard [18]. It's an iterative block cipher algorithm, in which key and packet length are the variables.256 192 and 128 bits are the optional key length which is equivalent to 14, 12 and 10 rounds respectively. (DES) has been the standard for the long-time substitute by AES since (NIST) selected the Rijndael algorithm to be approved as Advanced Encryption Standard (AES). [19] investigate the construction and design of new AES, subsequent three criteria, resistance against every identified attack, code compactness ranging platforms, rate and design effortlessness; as well as its congruity and incongruity with other symmetric ciphers. Compared with the DES, AES has an edge as it has high performance, robust and string security, competence, and elasticity.

2.1.2. Encryption and decryption process of advance encryption standard algorithm

Substitution and Replacement are the roots of The Advance Encryption Standard algorithm. Exchange of data unit with another is the Substitution, while rearranging of the data is the Replacement. ShiftRows, AddRoundKeys SubBytes, and MixColumns operations are the round functions, the basic elements of advance encryption system encryption algorithm. In Encryption every round is comprised of 4 steps [20].

a) Sub Bytes: The encoding site is where it's initially used. The byte is created as 2 hexadecimal digits to replace the byte
b) Shift Rows: The alteration is termed as Shift rows in encoding
c) Mix Columns: Its alteration runs at column level; every column of the positions transformed to the renewed column.
d) Add Round Key: The procedure in this is matrix addition, only one column runs at one time. With every case, column matrix word is added from the round key. The final step comprised of XO Ring production of prior 3 steps along with 4 key schedule words, as well as"MixColumns" step does not include in final round for encoding [21].

In Decryption: encoding using converse functions like a) converse Substitute Byte, b) converse Shift Rows, c) converse Mix Columns, and d) Add Round Key and decoding includes reversal of every step taken in. The 3rd step is composed of XO Ring production of the prior 2 steps along with 4 key schedule words. The "Converse Mix columns" step is not included in the final round of decoding. Figure 1 shows the decoding and encoding process of the Advanced Encryption Standard.

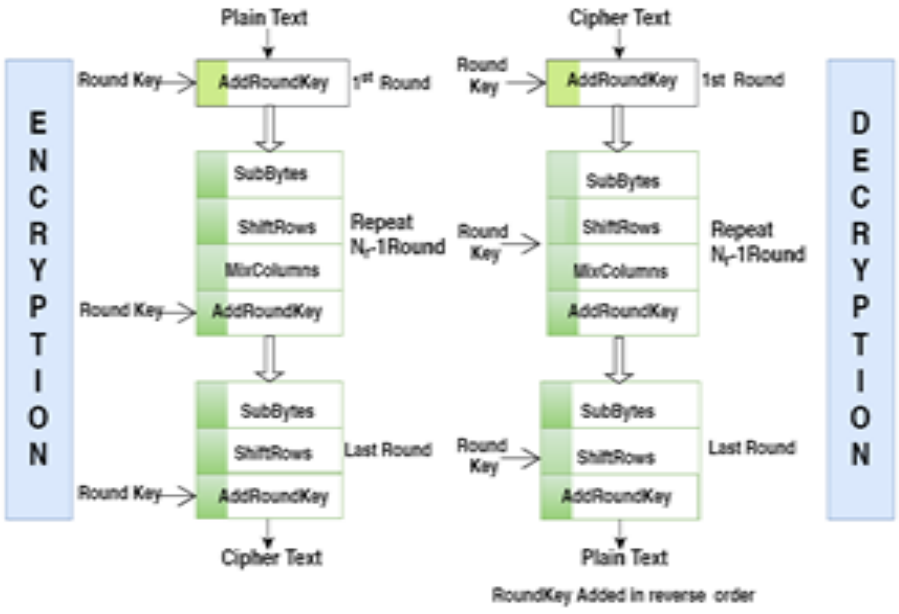

Figure 1. Decryption and encryption process of the advanced encryption standard

2.2. EHC encryption algorithm

2.2.1. Encryption profile/used

EHES method was proposed by Gorti VNKV Subba Rao for homomorphic decryption and encryption with the security system of IND-CCA. Homomorphic encryption permits us to execute multiplication, mixed and addition operations [16]. In real-time, these sorts of homomorphic coding have varied uses and applications. It is the essential thought that computations can be performed of the already encrypted data by the computer while not possessing information concerning data's true value. Eventually, this computed encoded data will be returned as a result and decoded [22]. This scheme demonstrates higher performance in memory, power consumption and processing speed than existing schemes. EHC is a non-detestable scheme and it includes multiplication, addition, mixed multiplication and addition operations.

2.2.2. Encryption and decryption process of EHC algorithm

Their Construction [23]. For nondeterministic, scheme a random number 'r' 'p', and a huge prime number 'q' such that q < p are taken. Take a set of cleartext data Zp and cleartext set operations consisting of the subtraction, mixed multiplication, addition, and multiplication, with m= pq modulo m. Let the ciphertext data set be Zc, Encryption key definition

k = (q, r p,m) and

ENCRYPTION

$E(X)=(x + r*pq) \pmod m = Y$

DECRYPTION

$D(Y) =y \bmod p = X.$

If p discovered it can be broken but it is is very hard to solve. That number can be factored by a computer quite quickly, excluding it, in essence, does it by trying the majority of the probable combinations. Two huge prime numbers can be found q and p that have maybe 400 or 200 digits each. Q is secret key, and we can make a number m=pq by multiplying them together. The number m is used to encrypt the data and as it's a secret key. By multiplying p and q, its relatively easy to get m. but it is impossible to get q and p if anyone knows m.M needs to be factored to get p and q, which is a really tough, finding ' r ' also complex it further as this concerned variable value will be created randomly. M is usually supposed to be if not 2048 at least 1024.

2.2.3. Hybrid encryption algorithm

For cloud computing security is important, especially the security-sensitive applications. we suggest propose hybrid method to provide security for cloud computing, considering the performance metrics (encryption time, throughput, average time, memory consumption and power consumption), taking the advantage of AES and EHC.

Advanced Encryption Standard encryption is the most widely used technique that is both flexible and scalable and is comfortably implemented. Moreover, the needed memory for the Advanced Encryption Standard algorithm is fewer, it displays signs of resistance against a diversity of attacks like recovery and differential attack. We can also protect data against the likes of smash attacks. Advanced Encryption Standard encryption algorithm has high performance and minimal storage space without any deficiency and limitations compared to other symmetric algorithms which have some instability in performance and storage space. Enhanced Homomorphic Cryptosystem uses the sharing key p and EHC makes use secret keys q, r and m for encryption so it's very strong. So it's really tough to get hold of secret keys. P is only known to receiver and sender so it gets really tough to find r and q. A random number that is 'r' will randomly generate so that each and every time the similar plaintext is mapped to another cipher text leading us to the fact that even with strong observation of the opposition it gets really difficult to track. Opponent fails to get a random number and secret value. EHC scheme has Multiplication, Addition, mixed multiplication, and Mixed addition. EHC consumes less memory and is faster than existing schemes. In addition EHC security is enhanced by non-deterministic feature.

3. METHOD

In this paper we particularly examined techniques for assessing the performance of DES, AES-128, and AES-128 with EHC at hexadecimal based cryptography in term of coding and decoding time taken, a studys carried out on the impact of adjusting the size of key of AES on Encryption and Decryption time consuming with fix file size, a study performed on average time and throughput for dissimilar file size, as well memory consumption and power consumption for all algorithm, for experimentation, we had a laptop with 2.70 GHz CPU, which performed data file ranging from 1MB byte to 20MB in size.

4. RESULTS AND DISCUSSION

As for the case of Advance Encryption Standard, in this paper it can be seen that higher size of key lead to a clear time consumption change. Conjointly higher key size means that higher security according to numbers of rounds, in our experiment we tend to use AES with 128 key sizes to not increasing the time consumption. Table 1 shows different AES key length, number of rounds and their effect on computational time at the fix file size. Figure 2 shows Time consuming in second for different key length in AES.
Table 2 shows the comparative study of throughput, average time and time consuming in encryption and decreption for the different algorithms in different file size

Table 1. The effect of the computational time at the fix file size

AES KEY LENGTH	ROUND	COMPUTATIONAL TIME	
		ENC	DEC
AES - 128	10	0.17 sec	0.16 sec
AES - 192	12	0.22sec	0.20 sec
AES - 256	14	0.26 sec	0.25 sec

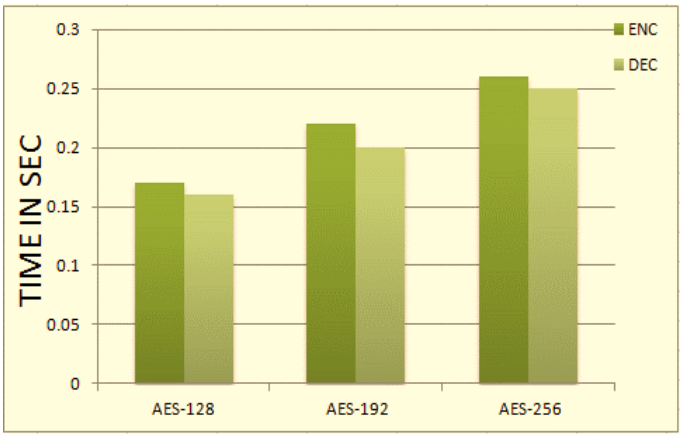

Figure 2. Time consuming in sec for different key length in AES

Table 2. The throughput, average time and time consuming

FILE SIZE	DES		AES-128		PROPOSED METHOD	
	ENC	DEC	ENC	DEC	ENC	DEC
1 MB	2.886	2.901	2.936	3.07	2.982	2.98
5MB	14.352	14.321	14.887	14.813	14.89	14.744
10MB	28.579	28.22	29.667	29.217	30.073	29.23
15MB	43.056	46.44	45.963	45.006	45.212	44.481
20MB	62.675	62.702	61.019	60.711	59.826	58.996
AVR	30.3096		30.8944		30.5966	
TROUGHPUT	1.642		1.668		1.695	

The generation of ciphertext from plaintext is the encryption time. We utilized the encryption time of an encryption algorithm to estimate the throughput. Throughput refers to the rate of encoding, computed as entirety plaintext is divided by the encryption time [24, 25]. Figure 3 shows that the outcome of the proposed method has the extremity throughput.

$$\text{Throughput of encryption} = \frac{\text{Total Plaintext (byte)}}{\text{Total Encryption Time (sec)}} \quad (1)$$

The performance evaluation conducted for the different algorithms according to memory consumption, encryption and decryption time took and power consumption. Table 3 shows memory or space storage in bytes for coding and decoding for fix file size is same for each algorithm, and our proposed algorithm need less space storage than DES and AES-128. Also the result shows in Figure 4 that our proposed work takes advantage of the least time taken in sec for encryption and decryption.

The results show that our proposed work consumed less time in coding and decoding. In case of power consumption, power consumption is a percentage usage of CPU by the current application our proposed work takes the peak power consumption because it is hybrid encryption algorithm. It consumes more recourses compare to DES and AES-128. Figure 5 shows the effect of DES, AES-128 and our proposed method on CPU usage.

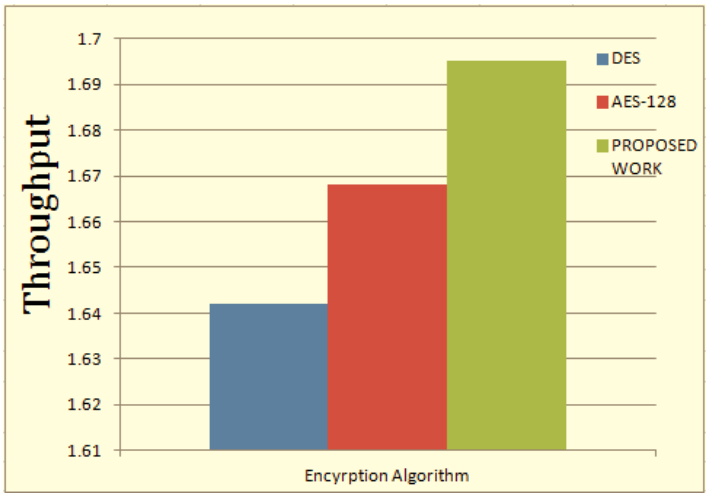

Figure 3. Shows the throughput of various algorithms with fix file size 20MB

Table 3. The Performance evaluations for encryption and decreption data with the fix file size 20MB

Performance evaluation	DES		AES-128		PRPOPOSED WORK	
	ENC	DEC	ENC	DEC	ENC	DEC
Memory	815104 byte	815104 byte	811008 byte	811008 byte	806912 byte	806912 byte
Power	24.0413%	23.927%	24.13%	24.2365	24.5228%	24.4522%
Time Taken	62.675 sec	62.702 sec	61.019 sec	60.711 sec	59.826 sec	58.996 sec

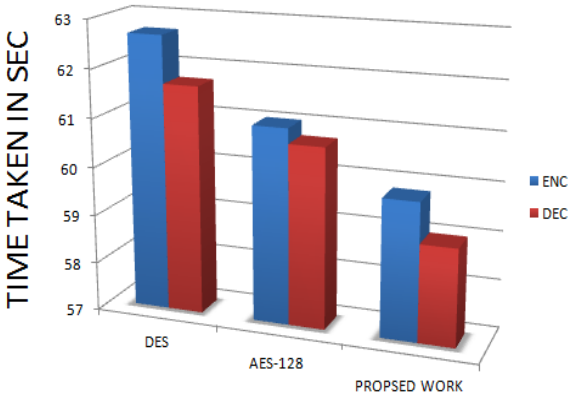

Figure 4. The time taken in a sec for encryption and decryption for the different algorithm with fix file size

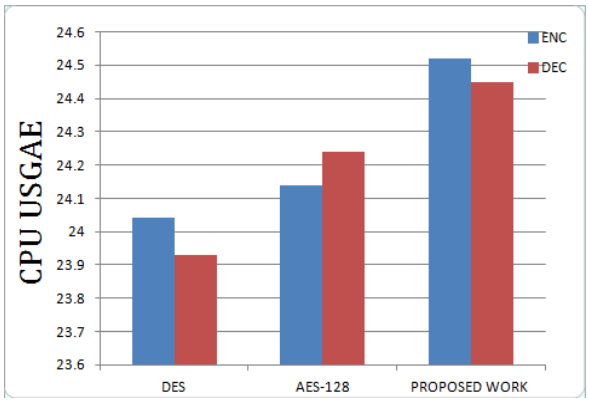

Figure 5. The effect of algorithms on CPU usage

5. CONCLUSION

With the service offered by the cloud provider, companies can increase their productivity in the shortest potential time though the adoption of such service can only be done if protection is ensure with high performance. Our proposed technique achieved a high performance and high security because it takes the good characteristic of AES and EHC. In this work the proposed technique can offer enhanced results in terms of security, throughput, memory consumption and time taking for encryption and decryption compare to AES-128 and DES.

REFERENCES

[1] P. M. Mell and T. Grance, *SP 800-145. The NIST Definition of Cloud Computing*: National Institute of Standards & Technology. 2011.

[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?," in *ACM Cloud Computing Security Workshop, Ccsw 2011, Chicago, Il, Usa, October*, pp. 113-124, 2011

[3] H. M. A. K. a. M. M. H. Diaa Salama Abdul. Elminaam1 "Performance Evaluation of Symmetric Encryption Algorithms," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 12, 2008.

[4] P. K. Ruangchaijatupon, "Encryption and Power Consumption in Wireless LANs-N," *The Third IEEE Workshop on Wireless LANs*, September, pp. 27-28, 2001.

[5] X. K. Qiu Weixing, Li Fang, etc, "A kind of method of extension of the DES key," *Computer Engineering*, vol. 37, no. 5, pp. 167-168, 2011.

[6] M. R. K. V. Nasarul Islam.K.V, "Analysis of Various Encryption Algorithms in Cloud Computing," *International Journal of Computer Science and Mobile Computing*, vol. 6, pp. 90-97, 2017.

[7] W. Stallings, "Cryptography and Network Security: International Edition 4th edition - paper."

[8] D. Coppersmith and T. J. W. R. C. IBM Research Division, P. O. Box 218, Yorktown Heights, New York 10598, USA, "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development* vol. 38, pp. 243 - 250, 1994.

[9] J. Bo, "DES integrated with RSA encryption methods," *Microcomputer Information*, pp. 52-54, 2007.

[10] Rijndael, "Advanced Encryption Standard (AES). FIPS.," 2001.

[11] K. Naik and D. S. L. Wei, "Software Implementation Strategies for Power-Conscious Systems," *Mobile Networks & Applications*, vol. 6, pp. 291-305, 2001.

[12] M. A. Wright, "The Advanced Encryption Standard," *Network Security*, vol. 2001, pp. 11-13, 2001.

[13] [O. Mazonka, Nektarios Georgios Tsoutsos, and Michail Maniatakos, "Cryptoleq: A heterogeneous abstract machine for encrypted and unencrypted computation.," *IEEE Transactions on Information Forensics and Security* vol. 11, no. 9, pp. 2123-2138, 2016.

[14] [Y. W. Xidan Song, "Homomorphic Cloud Computing Scheme Based on Hybrid Homomorphic Encryption," *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, 2018.

[15] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of Various Homomorphic Encryption algorithms and Schemes," *International Journal of Computer Applications*, vol. 91, pp. 26-32, 2014

[16] M. S. K. Gorti VNKV Subba Rao, Mr.A.Yashwanth Reddy, Mr.K.Narayana "Data Security in Bioinformatics," *International Journal of Advanced Research in Computer Science and Software Engineering*, 2013.

[17] Z. B. V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE," *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pp. 97-106, 2011.

[18] F. Dengguo, "Domestic and abroad research status and development trend of cryptography," *Journal of communications*, pp. 18-26, 2002.

[19] C. Sanchez-Avila and R. Sanchez-Reillol, "The Rijndael block cipher (AES proposal) : a comparison with DES," in *IEEE International Carnahan Conference on Security Technology*, pp. 229-234, 2002.

[20] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Global Journal of Computer Science & Technology*, vol. 13, 2013.

[21] D. Das and R. Misra, "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm," *International Journal of Network Security & Its Applications*, vol. 3, 2011.

[22] L. Ertaul and W. Lu, "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)," in *Ifip-Tc6 International Conference on NETWORKING Technologies, Services, and Protocols; PERFORMANCE of Computer and Communication Networks; Mobile and Wireless Communication Systems*, pp. 102-113, 2005.

[23] G. V. S. Rao and G. Uma, "An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme," *Global Journal of Computer Science & Technology*, 2013.

[24] O. P. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Peformance analysis of data encryption algorithms," in *International Conference on Electronics Computer Technology*, 2011.

[25] Rihan, S. D., Khalid, A., & Osman, S. E. F. "A performance comparison of encryption algorithms AES and DES," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 12, pp. 151-154, 2015.