Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:08:2021
DOI 10.17605/OSF.IO/43YD8

SECURED DATA TRANSMISSION USING DIFFERENT TECHNIQUES OF ENCRYPTION ON COMMUNICATION CHANNEL

Vijaya Pinjarkar
Department of Computer Science and Engineering, Sir Padampat Singhania University, Udaipur, Rajasthan, India

Amit Jain
Department of Computer Science and Engineering, Sir Padampat Singhania University, Udaipur, Rajasthan, India

Abstract In the fast evolution of digital data exchange information security plays an imperative role in the world of communication. The information transfer on network may face timidity. For elimination of insecurities over internet, many technological implementation and security policies have developed. Cryptography is one of the methods of protecting information and communication by using different mechanisms so that only intended person can read and process. The cryptography has the study of different algorithms. Both symmetric and asymmetric encryption techniques are best at their levels. This paper discusses about the comparison of different symmetric encryption algorithm. In addition, selecting the best algorithm according to requirements of application so that the confidentiality as well as integrity of the information, flowing on network is achieved.

Keywords— Cryptography; Confidentiality; Integrity; Information

1. INTRODUCTION

The whole world is now connected using internet. Almost every person is using mobile that is full of different applications installed on it, for example banking, supermarket, newspaper etc. When a mobile user draws on this application, there is an exchange of information between the users. When the data is transferred through network, there are chances that it may get altered, whether it is wired or wireless of type network. This takes place due to the insecurities in the network. Users cannot stop communicating because of insecurities. To overcome the issue of insecurities the information need to protect in such a way that alteration of information on the network is not possible.

Cryptography is the process which allows secure transition of information, by maintaining confidentiality and integrity of information [1] while confidentiality is defined as protecting information from being accessed by unauthorized user. In cryptography different algorithms like data encryption standard, advance encryption standard exist which immensely contribute for achieving confidentiality of information [2]. The algorithms in cryptography like message digest (MD), work to assure integrity of information [3]. In [4] authors said that the confidentiality and integrity is achieved by using stegonagraphy which include image file, document file. For stegonagraphic transmission the media files are ideal as their file size is large.

Security is ensuring the protection of data from unlawful access with the best line of defense. Encryption is one of the ways to shield information so that the data remains unchanged and protected during the transmission from the sender to intended recipient. Encryption, defined as the masking of data, so when data is being transfer from the network, unauthorized user is unable to access this data. Encryption categorized into two types, Symmetric encryption and Asymmetric encryption based on the number of keys used.

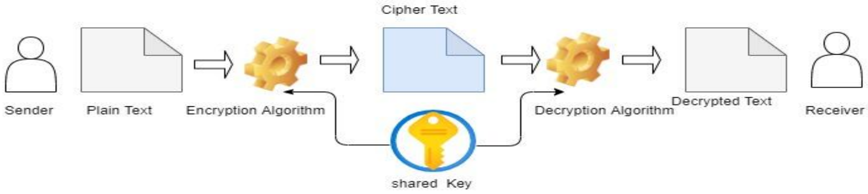

Fig.1: Symmetric Encryption Algorithm Process

Fig.1 shows the symmetric encryption process, which has five components including plain text, cipher text, encryption algorithm, decryption algorithm, and secrete key. Secrete key is required for encryption and decryption of plain text in algorithm.

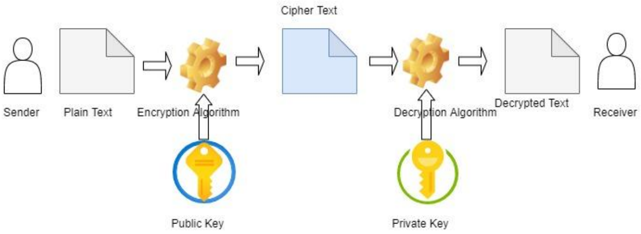

Fig.2: Asymmetric Encryption Algorithm Process

Fig.2 shows the asymmetric encryption algorithm process, which has six components that are plaint text, cipher text, encryption algorithm, decryption algorithm and public key and private key.

The cryptographic algorithm classification based on number of keys used is as symmetric and asymmetric encryption. Figure 3 shows the classification of encryption algorithm with list of algorithms.

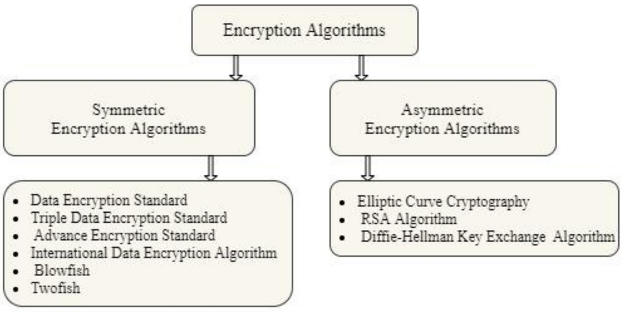
Encryption Algorithms
Symmetric Encryption Algorithms
Asymmetric Encryption Algorithms
Data Encryption Standard
Triple Data Encryption Standard
Advance Encryption Standard
International Data Encryption Algorithm
Blowfish
Twofish
Elliptic Curve Cryptography
RSA Algorithm
Diffie-Hellman Key Exchange Algorithm

Fig.3: Classification of Encryption Algorithms

II. RELATED WORK

The cryptography is an art of writing or converting normal text into unintelligible text. Cryptography is use in many applications for providing security. The author in [5] explained the homomorphic cryptography and pairing-based cryptography.

Homomorphic encryption is a form of encryption that allows computation on cipher messages, emerging in an encrypted result only which, when decrypted, matches the result of the operations, as if they had been performed on the plaintext [5]. [6] Show the comparison of various homomorphic encryption algorithms with analysis of those. Homomorphic Encryption algorithms are useful with GPS in Location Privacy[7] .

Pairing based cryptography is base on pairing function, which map pairs of points on an elliptic curve into a finite field. The properties of the pairing functions have facilitated many new cryptographic protocols that had not been previously feasible. [5] Monoaplabetic and Polyaphabetic encryption are also use widely for small applications.

In [8] a solution is proposed for creation of personal keys for cryptosystem using personal information as well as information encoding and secret sharing procedure. Cryptography is also helpful in wired and wireless network including mobile adhoc network [9].

In literature, the study of symmetric key encryption for different applications is available. For example, an adequate hierarchical key management scheme using symmetric encryption by [10] where the author implemented hierarchical access control, it is an access control where higher privileged user has a capacity to access the data from lower privileged user. The proposed cryptosystem reduced the time of generating and deriving keys in hierarchical key management.

Similarly in [11], authors proposed a protocol for generation as well as secured exchange of session keys between two users by means of symmetric key encryption .

Comparison of symmetric key encryption is given, in [12] where the authors inspect encryption and decryption time of symmetric encryption algorithm. Comparison of blowfish, two-fish and RSA algorithm is covered by [13]. [14] Present evaluation of symmetric and asymmetric encryption algorithm. The authors concluded that AES has better performance than other algorithms in term of through-put, encryption time and decryption time.

Day by day, there is an addition of new algorithm in cryptography. The key sizes, block size, number of rounds and type of operation are important parameters in any cryptographic algorithm. The current papers mainly compare and discuss about the symmetric encryption algorithms. Table I, shows the summary of different symmetric encryption algorithm with key size, block size and type of operation and the way of processing.

TABLE 1
COMPARISON OF SYMMETRIC ENCRYPTION ALGORITHMS

Algorithm Parameter	DES	3DES	AES	Blow fish	Two fish	IDEA
Key size	56 bit	Three 64-bit keys, with the overall key length of 192bits.	128-bit, 192-bit,256-bit	Variable length key up to 448bits.	Variable length key up to256bits.	28 bit
Block size	64 bit	64 bit	64 bit	64 bit	128 bit	64 bit
Number of rounds	16	48	10,12,14	16	16	8
Structure of algorithm	Fiestel Network	Fiestel Network	Substitution and Permutation Network	Fiestel Network	Fiestel network With objective F function	Numerous Mathematical activities.
Development Year	1974	1978	2001	1993	1972 and 1974,	1991
Developed by	IBM and US government in 1974	IBM in 1978	National Institute of Standards and Technology (NIST)	Bruce Schneier in 1993	Bruce Schneier the National Institute of Standards and Technology, or NIST	James Massey of ETH Zurich and Xuejia Lai .

III. PORPOSED MODEL

This section deals with the implementation of various symmetric encryption algorithms. Symmetric encryption algorithms like DES, 3DES AES, IDEA, and Blowfish are consider in execution. The parameters like key size, file size, encryption and decryption time along with memory required.

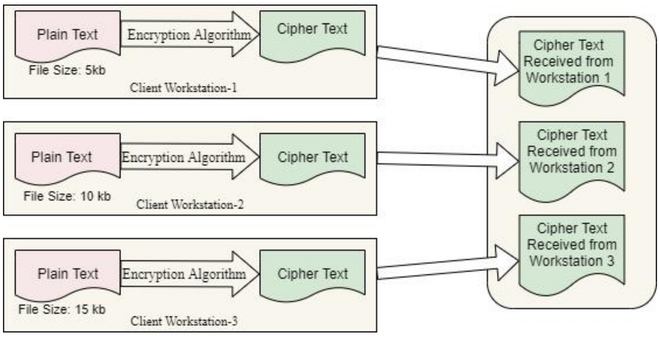

Fig.4: System Architecture

The Implementation scenario is like:

Sender is working on a workstation.
Sender has text file called “Plain Text”.
Sender wants to encrypt plain text using symmetric key encryption algorithms.
Sender encrypts plain text and sends encrypted file to receiver called “Cipher Text”.

In this scenario, the Sender who is working on a workstation sends files to the server.

As the file size is not fixed, consider different file sizes at sender site. Receiver site, server workstation receives encrypted files from sender, which decrypted with a shared key.

The aim is to find the outstanding symmetric key encryption algorithms based on performance in this scenario. Fig. 4 shows basic architecture.

IV. RESULTS AND DISCUSSIONS

As explained in the section III, symmetric encryption algorithms like DES, 3DES AES, IDEA, and Blowfish are consider for execution. For implementation, considered three file sizes viz. 25kb, 50kb, 75kb as input to different algorithms. The parameters like encryption time, decryption time, memory required, and files size changes (original file size, encrypted file size, decrypted file size) considered for comparison. Let us discuss the algorithm performance by considering all the parameters one by one. The very first parameter is Encryption time.

A. Parameter 1: Encryption time

Table II, shows the comparison of different algorithms based on encryption time. It shows that for encryptions 25kb file the AES-128 algorithm required less time i.e. 0.48 milliseconds and 3DES required the highest time i.e. 1.39 milliseconds. For encryption of 50kb and 75kb file, AES-128 algorithm required lowest time i.e. 0.56 and 0.79 where as blowfish noted with the highest time.

Fig. 5 shows the graphical representation of encryption time required for different symmetric algorithms. Y-axis represents the encryption time in milliseconds and X-axis shows the type of algorithm.

TABLE II

ENCRYPTION TIME (MS) FOR 25KB, 50KB, 75KB FILE SIZE

	DES	3DES	AES-128	AES-192	AES-256	IDEA	Blowfish
25kb	0.89	1.391	0.48	0.67	0.95	2.4	1.29
50kb	1.05	1.698	0.56	0.95	1.19	2.9	2.5
75kb	1.26	2.286	0.79	1.18	1.543	3.2	3.8

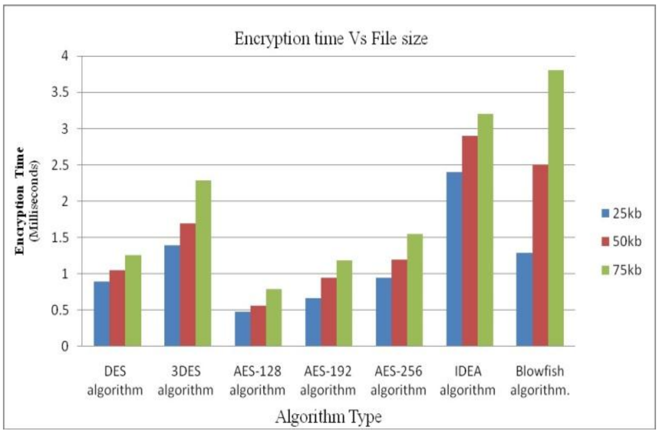

Fig.5: Encryption time Vs File size

B. Parameter2: Decryption time

Table III, shows the comparison of different algorithms based on decryption time. It shows that the AES-128 algorithm required less time for decryption i.e. 0.25, 0.46 and 0.65 milliseconds for decryption of 25, 50, and 75kb respectively whereas blowfish required highest time for encryption.

Fig. 6 shows the graphical representation of decryption time required for different symmetric algorithms. Y-axis represents the decryption time in milliseconds and x-axis shows the type of algorithm.

TABLE III

DECRYPTION TIME (MS) FOR 25KB, 50KB, 75KB FILE SIZE.

	DES	3DES	AES-128	AES-192	AES-256	IDEA	Blowfish
25kb	0.97	0.869	0.25	0.67	0.72	2.3	1.12
50kb	1.94	1.484	0.46	0.7	0.89	2.7	2.2
75kb	2.87	2.07	0.65	1.01	0.94	3.1	3.37

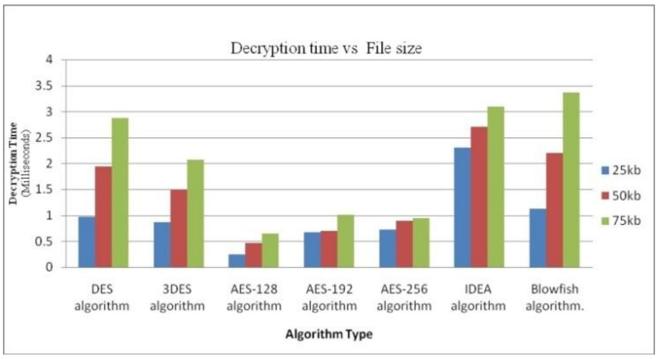

Fig.6: Decryption time Vs File size

C. Parameter 3: Memory required

Memory is the important factor for any application, so we have compared different algorithms based on memory required as shown in table IV and fig. 7.

Table IV, state that blowfish consumed highest memory i.e. 12.5, 24 and 33.7 respectively , while DES consumed the lowest memory.

TABLE IV

MEMORY REQUIRED (MB) FOR DIFFERENT ALGORITHM

	DES	3DES	AES-128	AES-192	AES-256	IDEA	Blowfish
25kb	6.4	6.7	7	7.2	7.2	12	12.2
50kb	6.4	6.9	7.2	7.2	7.4	23	24
75kb	6.4	7.3	7.2	7.3	7.8	33	33.7

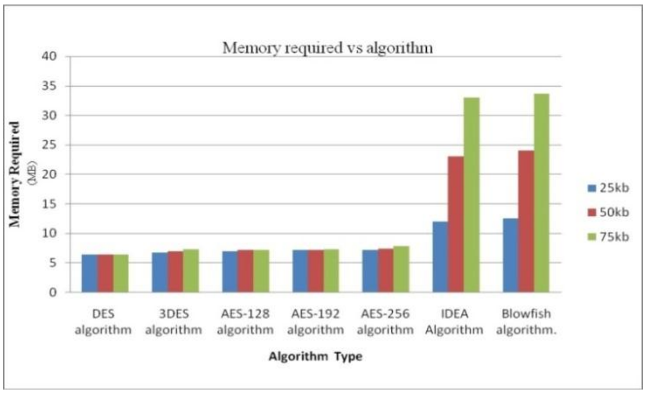

Fig. 7: Memory required vs. algorithm

In execution of complete scenario, three different file sizes are used. So it's good to check the effect of encryption algorithm on file sizes. In this section, we have compared the effect of encryption and decryption algorithm on file size.

D. Parameter 3: Variation in file size

1) 25 kb file size**:** Table V, shows a comparison of Plaintext file size, Encrypted file size, and Decrypted file size. Here, the file size 25kb given as input to algorithms, so the result shows that DES, 3DES, and blowfish are producing a file size different from the plaintext file, whereas AES perform well by producing the same file size as the input file size.

TABLE V

COMPARISON OF PLAINTEXT FILE, ENCRYPTED AND DECRYPTED FILE SIZE. (FOR 25KB)

	DES	**3DES**	**AES-128**	**AES-192**	**AES-256**	**IDEA**	**Blowfish**
Original file size (kb)	25	25	25	25	25	25	25
Encrypted file size (kb)	25.29	25.3	25	25	25	25	25.2
Decrypted file size (kb)	25.29	25.2	25	25	25	25	25.2

Fig.8, shows the comparison of plaintext, encrypted and decrypted file size for 25kb, it is observed that the AES and IDEA algorithm performance is good than the DES, 3DES and blowfish.

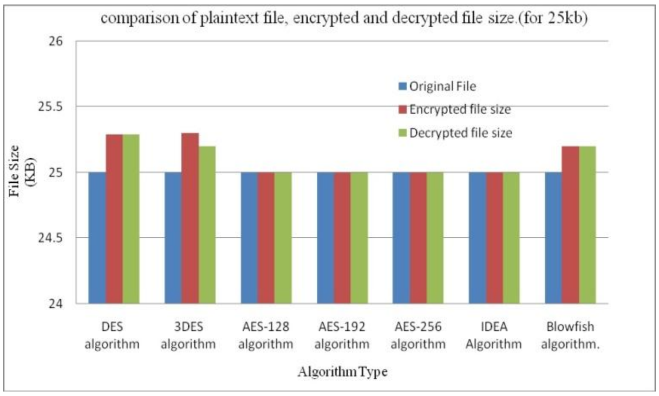

Fig. 8: comparison of plaintext, encrypted and decrypted file size.(for 25kb)

2) 50 kb file size: Fig. 9 and table VI show a comparison of Plaintext file size, Encrypted file size, and Decrypted file size. Here, the file size is given as 50kb, so the result shows that DES, 3DES, and blowfish are producing a file size different than the plaintext file, whereas AES performs well by producing the same file size as the input file size.

TABLE VI

COMPARISON OF PLAINTEXT FILE, ENCRYPTED AND DECRYPTED FILE SIZE.(FOR 50KB)

	DES	**3DES**	**AES-128**	**AES-192**	**AES-256**	**IDEA**	**Blow fish**
Original file size (kb)	50	50	50	50	50	50	50
Encrypted file size (kb)	50.89	25.9	50	50	50	50	50.4
Decrypted file size (kb)	50.89	50.8	50	50	50	50	50.8

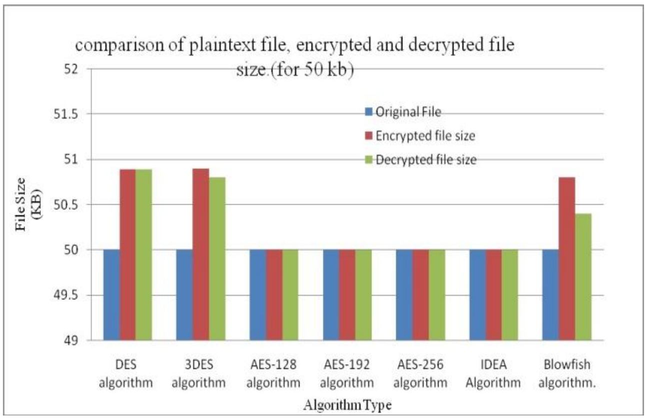

Fig. 9: comparison of plaintext, encrypted and decrypted file size.(for 50kb)

3) 75 kb file size*:* Fig.10 and table VII, shows a comparison of Plaintext file size, Encrypted file size, and Decrypted file size. Here, the file size is given as 75kb, so the result shows that DES, 3DES, and blowfish are producing a file size different than the plaintext file, whereas AES performs well by producing the same file size as the input file size.

TABLE VII

COMPARISON OF PLAINTEXT FILE, ENCRYPTED AND DECRYPTED FILE SIZE. (FOR 75KB)

	DES	3DES	AES-128	AES-192	AES-256	IDEA	Blow fish
Original file size (kb)	75	75	75	75	75	75	75
Encrypted file size (kb)	76.4	76.4	75	75	75	75	76.2
Decrypted file size (kb)	76.4	76.3	75	75	75	75	75.5

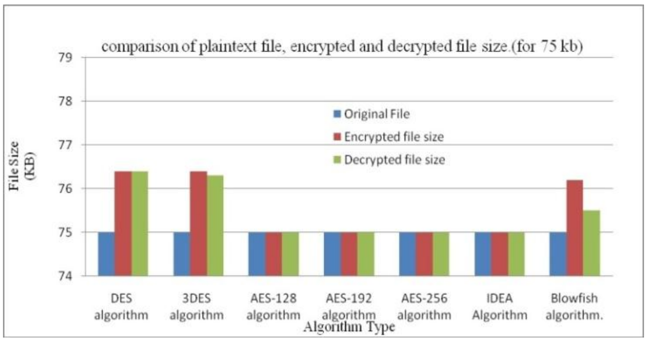

Fig.10: comparison of plaintext, encrypted and decrypted file size.(for 75kb)

E. Parameter 3: Average execution time

Fig. 11 and table VIII, show the comparison of different algorithm based on average execution time. It shows that the AES-128 algorithm requires less time i.e. 0.36, 0.51, 0.72 for encryption and decryption of file as compared to DES, 3DES, AES-192, AES-256, IDEA and Blowfish algorithm.

TABLE VIII

AVERAGE EXECUTION TIME (MS) FOR 25KB, 50KB ,75KB FILE SIZE.

	DES	3DES	AES-128	AES-192	AES-256	IDEA	Blowfish
25kb	0.93	1.13	0.36	0.67	0.835	2.35	1.205
50kb	1.49	1.59	0.51	0.825	1.04	2.8	2.35
75kb	2.06	2.17	0.72	1.09	1.24	3.15	3.58

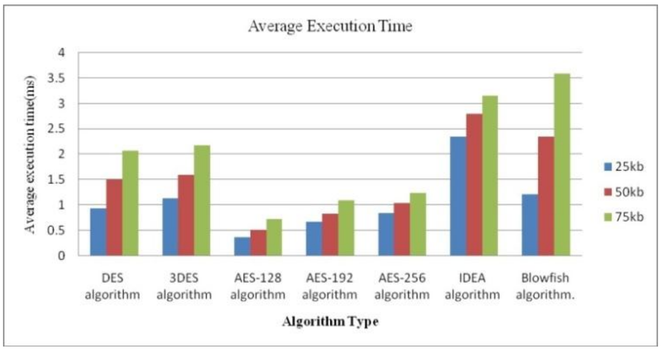

Fig.11: Average execution time Vs File size

After comparing all symmetric encryption algorithms with different parameters, it found that for the mentioned file sizes AES algorithm works excellent. AES-128 is excellent in working amongst three types of AES.

V. CONCLUSION AND FUTURE SCOPE

In nutshell, cryptography is a technique of shielding information and communications via the use of codes, so that only a legitimate person can read and process information. Cryptography allows secure transmission of data without dropping confidentiality and integrity of data. Symmetric encryption and asymmetric encryption are its prominent types. This paper has discussed the performance evaluation of the symmetric encryption algorithm by considering the different parameters like input plain text size, encryption time, decryption time, and memory. After comparing different symmetric encryption algorithm for the text file, it found that AES imparts excellent results. AES-128 is excellent in working amongst three types of AES.

So sender will select AES-128 symmetric encryption algorithm for encrypting files and send this encrypted files to server. Server will decrypt received files and combine them. Therefore, without compromising integrity, comfidentilaity and by using less memory, with less encryption and decryption time sender sends files to server. In future, the implementation can be done on image files.

REFERENCES

[1] R. Sanchez-Reillo, C. Lopez-Ongil, L. Entrena-Arrontes, and C. Sanchez-Avila, “Information technology security using cryptography,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 18, no. 6, pp. 21–24, 2003, doi: 10.1109/MAES.2003.1209586.

[2] A. V. Mota, S. Azam, B. Shanmugam, K. C. Yeo, and K. Kannoorpatti, “Comparative analysis of different techniques of encryption for secured data transmission,” *IEEE Int. Conf. Power, Control. Signals Instrum. Eng. ICPCSI 2017*, pp. 231–237, 2018, doi: 10.1109/ICPCSI.2017.8392158.

[3] Ronald L. Rivest, “RFC 1321 - The MD5 Message-Digest Algorithm,” Cambridge, 1992. [Online]. Available: https://tools.ietf.org/pdf/rfc1321.pdf.

[4] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, “Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques,” *2019 2nd Int. Conf. New Trends Comput. Sci. ICTCS 2019 - Proc.*, 2019, doi: 10.1109/ICTCS.2019.8923060.

[5] Y. Nogami, “Pairing – based cryptography for homomorphic cryptography,” in *2014 International Symposium on Information Theory and its Applications, Victoria, BC, Canada*, 2014, pp. 318–321, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6979856&isnumber=6979787.

[6] P. Chaudhary, R. Gupta, A. Singh, and P. Majumder, "Analysis and Comparison of Various Fully Homomorphic Encryption Techniques," *2019 Int. Conf. Comput. Power Commun. Technol. GUCON 2019*, pp. 58–62, 2019.

[7] S. Gupta and G. Arora, "Use of Homomorphic Encryption with GPS in Location Privacy," *2019 4th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2019*, pp. 42–45, 2019, doi: 10.1109/ISCON47742.2019.9036149.

[8] M. R. Ogiela and L. Ogiela, "Cognitive keys in personalized cryptography," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 1050–1054, 2017, doi: 10.1109/AINA.2017.164.

[9] H. Mu and Z. Changlun, "Security evaluation model for threshold cryptography applications in MANET," *ICCET 2010 - 2010 Int. Conf. Comput. Eng. Technol. Proc.*, vol. 4, pp. 209–213, 2010, doi: 10.1109/ICCET.2010.5485630.

[10] C. Lin, W. Lee, and Y. Ho, "Encryptions," in *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), Taipei, Taiwan*, 2005, pp. 399-402 ,vol.2, doi: 10.1109/AINA.2005.99.

[11] S. Arora and M. Hussain, "Secure Session Key Sharing Using Symmetric Key Cryptography," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 850–855, 2018, doi: 10.1109/ICACCI.2018.8554553.

[12] N. A. Advani and A. M. Gonsai, "Performance analysis of symmetric encryption algorithms for their encryption and decryption time," *Proc. 2019 6th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2019*, pp. 359–362, 2019.

[13] R. S. A. Cryptosystems and M. Iavich, "Comparison and Hybrid Implementation of," *2019 IEEE 2nd Ukr. Conf. Electr. Comput. Eng.*, pp. 970–974, 2019.

[14] M. Panda, "Performance analysis of encryption algorithms for security," *Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016 - Proc.*, pp. 278–284, 2017, doi: 10.1109/SCOPES.2016.7955835.