IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

Comparative Analysis on Different parameters of Encryption Algorithms for Information Security

Md Asif Mushtaque[1]

[1]*School of Computer Science and Engineering, Galgotias University, India*

www.ijcseonline.org

Received: 2/03/2014 Revised: 17/03/2014 Accepted: 12/04/2014 Published: 30/04/2014

***Abstract*—** In this era information security is a very important issue in every field such as Government Agencies (CBI, FBI), Research Organization, E-commerce and etc. where internet is being used. We want to secure our data from unauthorized user. Cryptography is a technique to secure data on the network from unauthorized user. There are different types of a cryptography algorithm (a) symmetric and (b) asymmetric has been designed. To secure data it is necessary to know which algorithm provides better security, efficiency, accuracy and effectiveness. This paper presents the complete analysis of various symmetric key encryption algorithms (DES, 3DES, CAST-128, MARS, IDEA, Blowfish, AES, and RC6) based on different parameters such as: Architecture, Scalability, Security, Flexibility, and limitations.

Keywords- Symmetric Key, Information Security, Performance Matrices, Encryption, AES, DES, 3DES, CAST-128, MARS, IDEA, Blowfish, RC6

I. INTRODUCTION

Cryptography is a technique or method to protect data by changing its format to another format which is not easy to understand by unauthorized user. It includes techniques like microdots, combining words with image to protect data. Cryptography technique can be classified into two categories (a) Symmetric Key and (b) Asymmetric Key.

Symmetric key algorithm also known as private or secret key algorithm. In this algorithm a single key is used by the sender or receiver [15], it means same key is used to encrypt and decrypt data. Symmetric key is of two types (i) stream cipher encryption and (ii) block cipher encryption. DES, 3DES, IDEA, Blowfish, AES, TEA, MARS, RC6 and CAST-128 are the example of symmetric key encryption algorithm.

Asymmetric key algorithm is also known as public key algorithm. It uses two different keys to perform encryption and decryption process, means one key is used to encrypt the data is known as public key and another key which is used for decryption is known as a private key. Both public and private keys are mathematically interrelated [15]. Public key is known by everyone but private key is known by only the receiver of that message. RSA, SSH, DH and SSL are the example of an asymmetric key algorithm.

Some Basic Terms of Cryptography:-

- *Encryption*- It is a process in which original message is converted into another format using a secret key. In this process two things are required key and encryption algorithm.
- *Decryption*- Decryption is the reverse process of encryption; it is performed on the receiver side. It also requires two things a secret key and a decryption algorithm.
- *Key*- A key is a numeric or combination of character that is variable length which is used to change the format of the original message.
- *Plaintext*- this is the original message or readable message before encryption which is to be transferred.
- *Ciphertext*- Plaintext is a message before encryption and when we encrypt the plaintext it changes into ciphertext.

The objective of Cryptography: These are the objectives of cryptography.

- *Confidentiality* – It means the message cannot be understood by unauthorized people.
- *Integrity*- The message cannot be modified while transmitting (between sender and receiver).
- *Authentication*- It means confirming the identity of the receiver.
- *Non Repudiation*- It means that the transmission cannot.
- *Access Control*- It means only the authorized person can access the information.

Corresponding Author: *Md Asif Mushtaque*
School of Computer Science and Engineering, Galgotias University, India

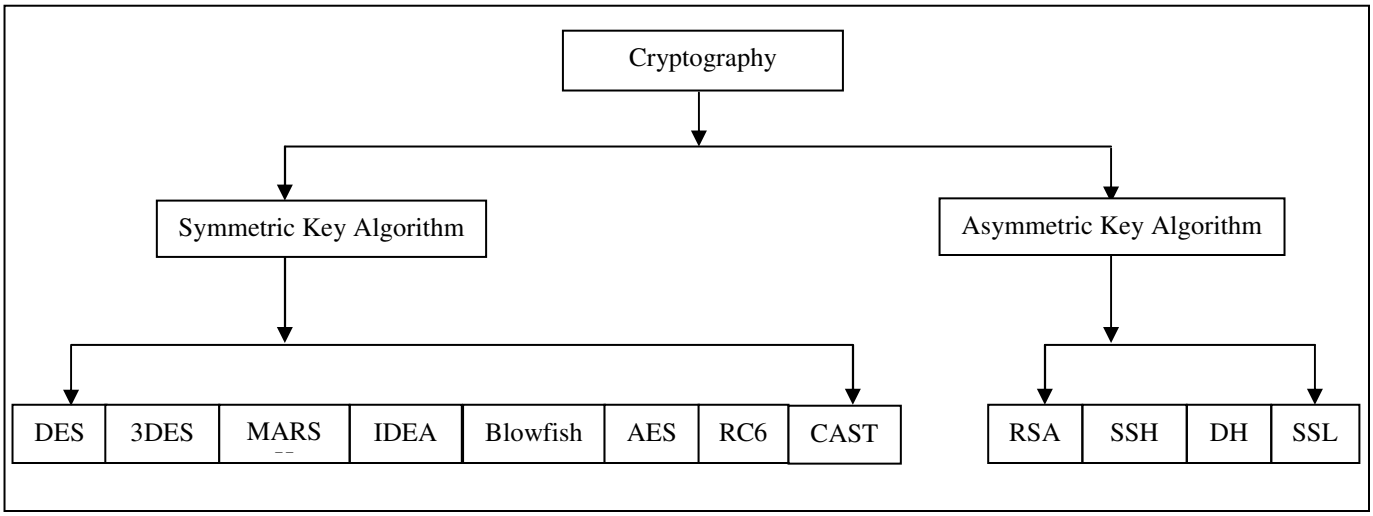

Figure1. Classification of Cryptography

II. RELATED WORKS

Many authors have compared these algorithms either on a single parameter or two parameters. But generally they have published their paper based on time complexity of these algorithms. In [1], the authors have compared AES and DES based on their performance, generally comparison has done for time complexity but they could not find which algorithm is better. In [2], the author compared some symmetric key algorithm on the basis of space complexity, in this paper, they discussed about how much space is required for the ciphertext.

Generally, in the review paper author compared two or three algorithms and focused on encryption and decryption time or their architecture [3-5]. On the base of encryption and decryption time we cannot say that the particular algorithm is efficient and effective. For this, we need to compare all the parameters of the algorithm and then we can easily decide which algorithm is efficient and secure.

An algorithm is said to be better on the basis of all these parameters. There are many more symmetric algorithms has been developed, so to apply any algorithm in application it is very necessary to know about strength and weakness.

So, in this paper, I compared various symmetric key encryption algorithms based on different features. Such as: Architecture, Scalability, Security, Flexibility and limitations.

III. DESCRIPTION

1. BASED ON ARCHITECTURE:

In this section, algorithms are discussed on their architecture (Basically structure, key size, block size and number of processing rounds).

1.1 DES (Data Encryption Standard):

DES designed by IBM in 1972 and it was adopted by the U.S. Government as standard encryption technique [1]. It is a symmetric key block cipher encryption algorithm based on Feistel Network. DES uses 64 bit block of text and 56 bit key length, it performs total 16 rounds of processing to encrypt data [15]. In DES, the key was 64 bits but due to some restrictions from NSA (National Security Agency) IBM decided to use 56 bit key length for encryption and the remaining 8 bits is used as a parity bit for error detection, it also uses 8 boxes. DES divides the 64 bit block into two equal parts and then applies F - function on each part. F-function performs four different tasks- Expansion, Key_Mixing, Substitution and Permutation. Decryption is the same process of encryption in DES.

1.2 3DES:

3DES was published in 1998 which is from DES. DES uses 56 bit key but 3DES uses 3 different keys total size of 168 bits [13]. All keys are identical or first key and third key may be same in 3DES. It also divides the text into 64 bit block and uses 8 S-boxes and performs 48 processing rounds [6]. 3DES is more complicated and designed to protect data again different attacks. 3DES encrypts data by applying DES encryption three times. 3DES is also approved by the U.S. Government to use because of its higher security.

1.3 CAST-128:

CAST-128 (CAST 5) designed by Carlisle Adams and Stafford Tavares in 1996. It is a block cipher algorithm used in various applications. It is based on Feistel structure and performs 12 or 16 processing rounds [7]. CAST uses 64 bit block, key length of 40-128 bit and contains the 4 S-boxes. CAST performs total 16 rounds if the key size is greater than 80 bits. To decrypt the encryption algorithm is used in reverse order [12].

1.4 MARS:

MARS is a block cipher designed by IBM in 1998 and submitted to the AES and selected as one of the five finalists in AUGUST 1999. MARS is based on type-3 Feistel structure (heterogeneous structure), it uses 128 bits block, key size of 128, 192, 256 bits and a single S-box [8]. The same algorithm is used for decryption in reverse.

1.5 IDEA (International Data Encryption Algorithm):

IDEA designed by Xuejia Lai and James Massey in 1991. It is also known as Improved Proposed Encryption Standard (IPES) because it is derived from Proposed Encryption Algorithm. It is symmetric key block cipher algorithm; it is based on substitution-permutation structure. It uses 64 bit block, 128 bit key and performs 8.5 rounds. In each round it performs three main operation XOR, Addition and Multiplication. Decryption is same as encryption only the key is reversed [17].

1.6 Blowfish:

Blowfish is designed by Bruce Schneier in 1993. It is fast and simple block encryption algorithm used in the Secure Socket Layer and other program. Blowfish is based on Feistel Network supports 64 bit block and key size of 32-448 bit. It contains 4 s-boxes and performs 16 processing rounds [6, 11]. Two main functions are performed in this algorithm Key expansion and Data encryption. In blowfish the S-boxes are key dependent.

1.7 AES (Advanced Encryption Standard):

AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It is based on Feistel network and support 128 bit block size and key length 128, 192 and 256 bits [1]. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128 bit key length AES performs 10 rounds, for 192 bit key it performs 12 rounds and for 256 bit key it performs 14 rounds [14]. In AES each round performs some steps. Key-expansion, Initial-round, Rounds and Final-rounds. In Rounds step, Sub-byte generation, Shift-rows, Mix-columns and Add-round_key are performed whereas in Final-rounds step, same functions are performed except Mix-columns function.

1.8 RC6:

RC6 is designed by Ron Rivest in 1998, it derived from its predecessor RC5. It is also based on Feistel structure and takes block size of 128 bits, key size 128, 192 or 256 bits and total number of processing rounds are 20 [9]. RC6 differ from RC5 because it uses 4 registers while RC5 uses 2 registers and it performs an extra multiplication operation [10, 12].

Table1 shows the comparison of selected algorithm on the basis of architecture.

Algorithms	Key Size	Block Size	Rounds	Structure	No. of S-boxes
DES	56 bits	64 bits	16	Feistel Network	8
3DES	168 bits	64 bits	48	Feistel Network	8
CAST 128	40 – 128 bits	64 bits	12 or 16 (16-if key size greater than 80 bits)	Feistel Network	4
MARS	128, 192 or 256 bits	128 bits	32	Feistel (Heterogeneous Structure)	1
IDEA	128 bits	64 bits	8.5	Substitution-Permutation Structure	N/A
BLOWFISH	32 – 448 bits	64 bits	16	Feistel Network	4
AES	128, 192 or 256 bits	128 bits	10, 12 or 14 (depend on the size of key)	Feistel Network	1
RC6	128, 192 or 256 bits	128 bits	20	Feistel Network	N/A

Table1. Comparison of Algorithms base on Architecture

2. BASED ON SCALABILITY:

In this section, analyze the scalability of various encryption algorithms on the basis of performance (key scheduling and encryption) and space required by the encryption algorithm. The memory required by any algorithm depends on the number of variables and functions executed by the encryption algorithm. Due to lack of memory to execute program there is a need to require less memory to execute the algorithm. If any algorithm requires less memory space provide better efficiency.

Encryption rate is also very important to analyze performance of encryption algorithm. The processing time required by any encryption algorithm to encrypt data is encryption rate. Encryption rate depends on the complexity of algorithm, speed of processor, hardware used such as main memory and etc. to provide better performance of the algorithm both software and hardware should be according to that algorithm.

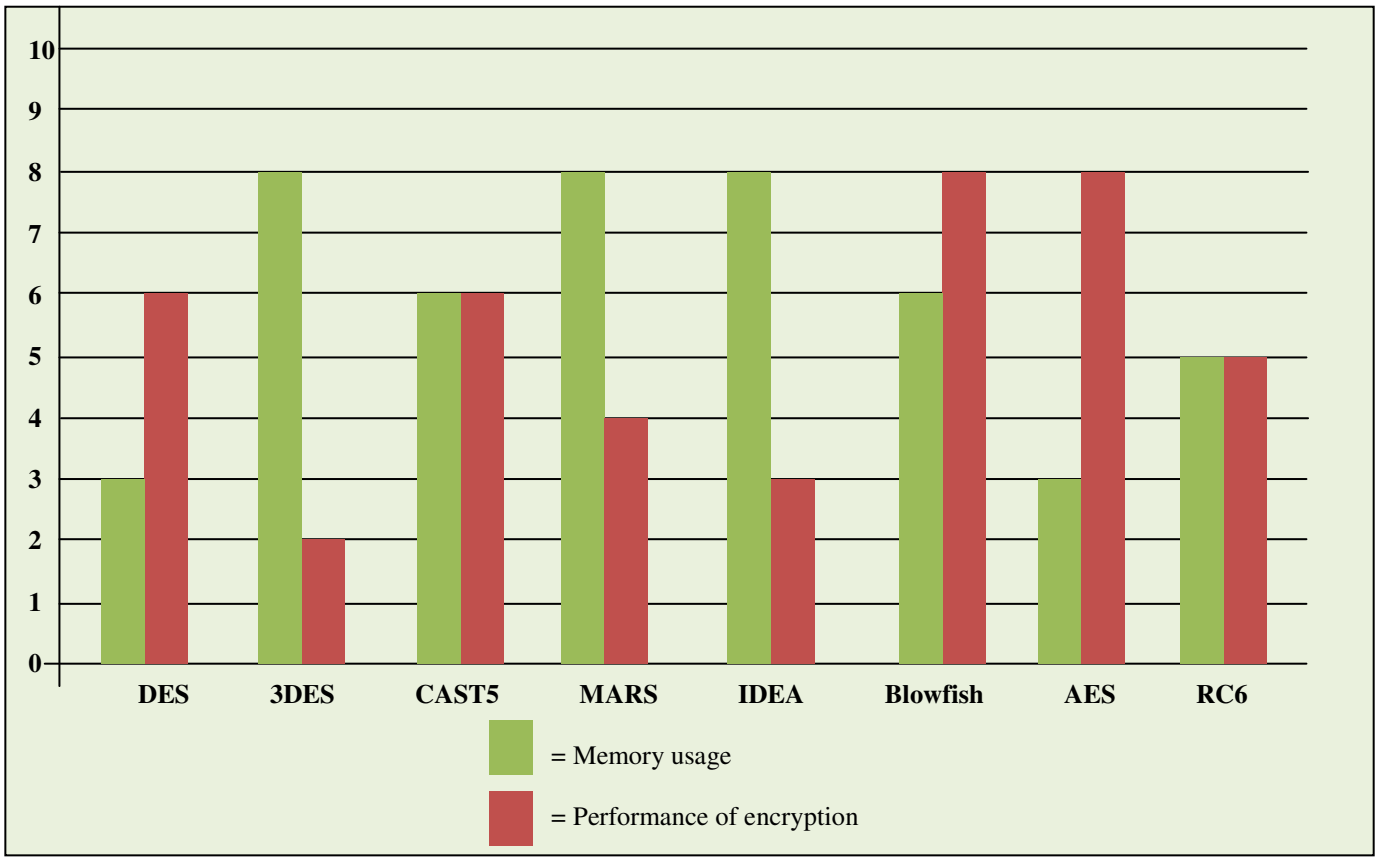

Figure2. Comparison of Algorithm based on scalability (Memory usage and Performance)

The figure2 shows a comparison between various encryption algorithms on the basis of memory usage and their encryption performance. From the figure2 we analyzed that AES is best among all these related algorithms. The encryption performance of the AES is equal to blowfish but the memory required by AES is less than blowfish. But on the basis of scalability we cannot say that AES is best among all these algorithms. To become a better algorithm different parameters (architecture, scalability, security and flexibility) should be effective.

3. SECURITY LEVEL:

In this section, I discussed about the security of these algorithms. It is the most important parameter of a cryptography algorithm because an algorithm is said to be better if they provide a strong security level.

3.1. DES:

Security is the main drawback of DES. DES does not provide strong security because of its key length 0f 56 bits. DES can easily crack by 2^56 imagination [6]. Initially DES was accepted as the standard algorithm with strong security but after sometimes Brute force attack cracked DES. So, DES is not a secure encryption algorithm.

3.2. 3DES (TDES):
3DES removes the security problem of DES, it uses 3 different keys of larger size (3x56=168 bits). In 3DES, DES process is performed three times with three different keys to provide better security. It provides high level security in comparison to DES that's why 3DES is used by the U.S. Government [16].

3.3. CAST 125
To increase security level CAST uses variable key length operation, its security level is great and CAST 125 protects information from linear and differential attacks [12].

3.4. MARS:
Security level of MARS is very stronger than DES and 3DES because of its 32 different round and data rotation with Boolean complexity, middle round considered as a strong part of MARS. MARS encryption algorithm provides better security against timing attacks, relative key attacks and differential attacks [8].

3.5. IDEA:
It provides a strong security level again differential attacks; IDEA performs multiple operations to increase its security level. Uses of 128 bits key size make it strong encryption algorithm. There is no any weakness related to differential and linear attacks in IDEA [8, 9].

3.6. Blowfish:
Blowfish has a high security level because it uses variable length key of 32-448 bits [6]. Blowfish is a secure algorithm against differential key attacks, because each bit of the master key involves multiple round key which is independent.

3.7. AES:
AES is also provides a very high security level because of using variable length key i.e. 128, 192 or 256 bits. Different types of attack tried to crack AES like Square attack, Key attack, Differential attack and improved square attack but none of them is possible to crack this algorithm. So, AES is a highly secured encryption technique [1, 8]. AES can also protect data against future attack (collision attack).

3.8. RC6:
RC6 also provides better security level against differential attacks, the main parameter of RC6 that protect this algorithm from such attacks is that following random series of output. Linear attack can apply for 16 rounds RC6 but needs 2^119 imagination of plaintext which is impossible.

4. ON THE BASIS OF FLEXIBILITY:

In this section, compared these algorithms base on their flexibility i.e. in the future according to the need the algorithm is able to modify or not.

Algorithms	Flexibility	Modification	Remarks
DES	No	No	DES does not support any modification.
3DES	Yes	168	The structure is same as its predecessor DES; 3DES performs DES operation three times so the key size in 3DES is extended from 56 to 168 bits.
CAST 125	Yes	64, 128 or 256	CAST5 has a flexible structure so it modified to 128 and 256 bits to increase its security level.
MARS	Yes	128 - 448	MARS supports variable length key, but the length of the key should be multiples of 32.
IDEA	No	No	Its structure does not support modification.
BLOWFISH	Yes	64 - 448	Key length in blowfish should be multiples of 32.
AES	Yes	128, 192 or 256	Its structure was flexible to the multiples of 64.
RC6	Yes	128 - 2048	It can be extended to 2048 bits key length but the key length should be multiples of 32.

Table2. Comparison of Algorithms based on Flexibility

5. LIMITATION:

5.1. DES:

Due to short key length brute force attack crack easily by performing 2^56 imaginations. Weak key is the major problem of DES. It doesn't protect data against linear and differential attacks. DES didn't design for software so it runs slowly.

5.2. 3DES:

3des overcomes the problem of DES, but 3DES has also some disadvantages. 3DES performs DES operation three times to encrypt data so it requires almost 3 times more space than DES [6].

5.3. CAST 128:

Using a known plain text attack Key of CAST 128 can be known by linear cryptanalysis. It can be broken by 2^17 chosen plaintexts along with one related-key query in offline work of 2^48 [8].

5.4. MARS:

In MARS, no any significant limitation has been observed. Hardware implementation of MARS is some difficult and complex. Due to performing the function with Boolean complexity MARS is very complex to observe.

5.5. IDEA:

Some possibilities of being attack were found in IDEA regarding minimum round version and different classes of weak keys [8]. First three rounds of IDEA algorithm is observed for related-key differential timing attacks and key-schedule attacks.

5.6. Blowfish:

Blowfish is a very secure algorithm but Initial 4 rounds of blowfish are observed unprotected from 2^{nd}-order differential attack.

5.7. AES:

No any such kind of weakness has been observed in AES. Some initial rounds of AES are observed unprotected i.e. initial round can break by square method.

5.8. RC6:

For a class of weak keys, RC6 is analyzed that randomness is not achieved for up to 17 rounds. Otherwise it is observed that RC6 is a very secure algorithm [8].

IV. CONCLUSION

In this paper, a complete analysis of symmetric key encryption algorithm has been presented based on different parameters. Performance of DES and CAST 5 are same, memory required by the AES and DES are equal but the performance of the AES is very high than DES. DES encryption has very disadvantages and doesn't support future modification while AES has no serious disadvantages. IDEA, 3DES and MARS require the same amount of memory for the same size of data but there is the minimum difference between their performances. 3DES is also observed as a secure algorithm but it takes 3 times more space than DES. After the comparison, it is analyzed that AES is secure, fast, better and effective encryption algorithm among all these encryption algorithms with less storage space, high encryption performance without any weakness and limitations while other algorithm has some weakness and differences in performance, storage space.

V. ACKNOWLEDGMENT

I would like to thank the proof readers, honorable teachers, fellow students, supportive friends and specially my family. I would also like to say thank to that person who guides me through the way, he continually and persuasively conveys a spirit of adventure in regard to my thesis/project work Md. Tauqir Azam Kausar.

REFERENCES

[1] A. K. Mandal, C. Parakash and M. A. Tiwari, "Performance Evaluation of Cryptographic Algorithms:
DES and AES", 2012 IEEE Student's Conference on Electrical, Electronics and Computer Science.

[2] V. Singh and S. K. Dubey, "Analyzing Space Complexity Of Various Encryption Algorithms", International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, January- February (2013).

[3] Tingyuan Nie, Yansheng Li and Chuanwang Song, "Performance Evaluation for CAST and RC5 Encryption Algorithms", International Conference on Computing, Control and Industrial Engineering, IEEE, 2010.

[4] E. Thambiraja, G. Ramesh and Dr. R. Umarani " A Survey on Various Most Common Encryption Techniques", IJARCSSE, Volume 2, Issue 7, July 2012.

[5] A.Ramesh and Dr.A.Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], IEEE, 2013.

[6] Md Asif Mushtaque, H. Dhiman, S. Hussain and Shivangi Maheshwari,"Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[7] Tingyuan Nie, Yansheng Li and Chuanwang Song, "International Conference on Computing, Control and Industrial Engineering", IEEE, 2010.

[8] Harmanpreet Singh, Amritpal Singh Danewalia, Deepak Chopra and Naveen Kumar N, "Randomly Generated Algorithms and Dynamic Connections", ISROSET-International Journal of Scientific Research in Network Security and Communication, Volume-02, Issue-01, Page No (1-4), Jan -Feb 2014.

[9] Kirti Aggarwal, Jaspal Kaur Saini, Harsh K. Verma, "Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers", International Journal of Computer Applications (0975 – 8887), April 2013, Volume 68– No.25, pp. 10-16.

[10] E. Thambiraja, G. Ramesh and Dr. R. Umarani" A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, July 2012.

[11] Z. Zahang and Shiliang sun, "Image encryption algorithm based on logistic chaotic system and s-boxes scrambling", Image and Signal Processing (CISP), 4th International Congress on (Volume: 1),2011 .

[12] "Practical-Cryptology-and-Web-Security", http://www.scribd.com/doc/126378371/Practical-Cryptology-and-Web-Security, accessed on 5th april 2014.

[13] Michal Halas, Ivan Bestak, Milos Orgon, and Adrian Kovac, "Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks", IEEE, 2012.

[14] Fei Shao, Zinan Chang and Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Second International Conference on Communication Software and Networks DOI 10.1109/ICCSN.2010.124, IEEE, 2010.

[15] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST , Vol. 2, Iss ue 2, June 2011.

[16] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "NewComparative Study between DES, 3DES and AES", journal of computing, volume 2, issue 3, march 2010.

[17] Md Imran Alam and Mohammad Rafeek Khan," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.

AUTHOR'S PROFILE

Student of M.Tech in Computer Science and Engineering of Galgotias University, Greater Noida, U.P., India. My research interest include Network Security, Failure Handling and cloud computing.