ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Survey on Different Data Security Cryptographic Algorithms

[1] S. SweetlinSusilabai, [2] Dr.D. S. Mahendran, [3] Dr. S. John Peter
[1] Research scholar, Manonmaniam Sundaranar University, Tirunelveli
[2] Associate Professor in computer science, Aditanar college of Arts & Science, Tiruchendur.
[3] Associate professor & Head, Department of Computer science, St.Xaviers College, Tirunelveli.

Abstract: **- In today's world cloud computing grows very fast and transferring a vast amount of data confidentially through clouds by using security algorithms. Clouds are the new platform in Information Technology (IT) and business world. Huge Number of users' stores their secured data on Cloud. We send more private data in the clouds. Data security is the most important role in transferring data through clouds. Cryptography is a technique that allows the user to send and receive the confidential data using security algorithms. So, data security is an important factor in cloud computing for ensuring clients data is placed in the secure mode in the cloud. In this paper, there are a number of existing cryptographic techniques used to implement security in cloud and we have to discuss the number of symmetric and asymmetric algorithms. We have focused on a comparative study of various cryptographic algorithms like DES, 3DES, AES, RC2, RC4, RC5, RC6, TWOFISH, THREEFISH, BLOWFISH, and RSA. We have to analyze their ability to secure data, key size, block size, features.**

Keywords: **Cryptography, Encryption, Symmetric Key Algorithm, Asymmetric key Algorithm, RSA and BLOWFISH.**

I. INTRODUCTION

The main important work of the Cryptography encryption algorithm is used to give security against unauthorized access. Cryptography is a fundamental building block for building information systems. Cryptography [1][2] is the science of secure data. It is a technique to transmit secure data between two parties. It uses two things i.e. plain text and cipher text. The sender can send plain text, it is an original data. The plain text can be converted into cipher text by using encryption algorithm and cipher text can be converted into plain text by using decryption algorithm. We can expect that the cryptography will become more and more important with time.

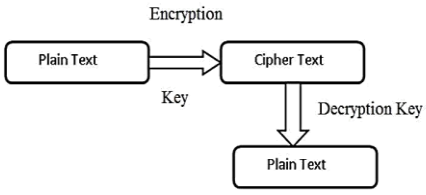


Fig 1. Cryptography

The main goal of cryptography is to effectively deal with the following areas:

1) Confidentiality:
It allows keeping the confidential information in computer and it is transmitted to be accessed only by the authorized party and not by someone else.

2) Secrecy:
It is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

3) Data integrity:
It is a service which secures the unauthorized modification of data. To ensure data integrity, one must have the capability to detect data manipulation by unauthorized parties. Only the authorized user is permitted to change the transmitted data. No one is allowed in between the sender and receiver to modify the given data.

4) Authentication
It is a service related to identification of two parties. The sender and receiver entering into a communication should identify each other. The information received by any computer has to check the identity of the sender that whether the information is arriving from a authorized user or a unauthorized identity.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

5) Non-repudiation:

It is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. Ensure that neither the sender, nor the receiver of message should be able to deny the transmission.

6) Access Control:

Access Control specifies and controls who can access what.

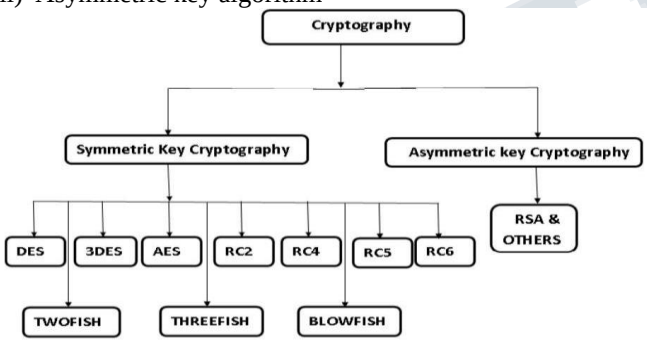
7) Availability:

The principle of availability states that resources should be available to authorized parties all the times.

II. CRYPTOGRAPHY ALGORITHMS

There are many cryptographic algorithms used for encryption data. Cryptographic algorithms mostly classified into two broad categories.

i) Symmetric key algorithm
ii) Asymmetric key algorithm



2.1. Types of Cryptography

i) Symmetric key algorithm

Symmetric key algorithm [2] uses same key for both encryption and decryption. Symmetric key algorithm is known as secret key or shared key algorithm or public key algorithm. It During data transmission the sender and receiver uses same secret key. Only one key is used for doing encryption and decryption. so this algorithm depends on two factors-secrecy of the key and its distribution for its success. Symmetric key algorithms are AES, DES, 3DES, RC2, RC4, RC5, RC6, TWOFISH, THREEFISH, BLOWFISH.

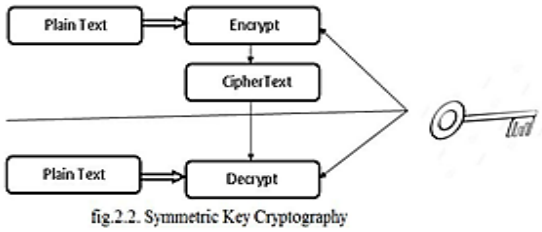


fig.2.2. Symmetric Key Cryptography

ii) Asymmetric key algorithm

Asymmetric key algorithm [9] uses two different keys for encryption and decryption. For encryption it uses public key and private key is used for decryption. Sender sends encrypted text with public key and receiver receive the decrypted text with private key. Asymmetric algorithms are Diffe-Hellman and RSA Public Key Encryption

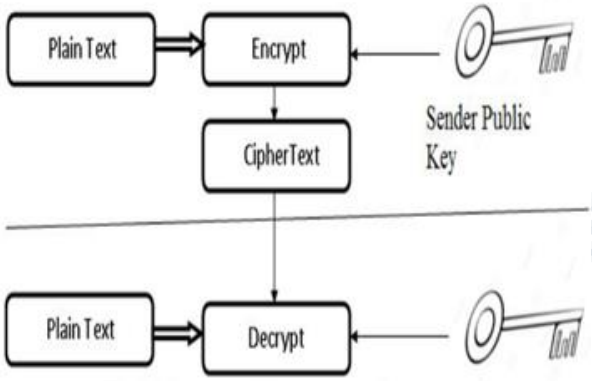


Fig.2.3. Asymmetric Key Cryptography

• AES (Advanced Encryption Standard)

AES [16] is also called Rijndael's algorithm. It is a symmetric cipher algorithm. It encrypts the data blocks of 128 bits using secret key. It has a variable key length of 128, 192 or 256 bits. It encrypts 128 bit data block into 10,12 and 14 rounds. Each round allows four rounds i.e Substitute byte, shift rows, Mix column, add round key. It uses different rounds of data.

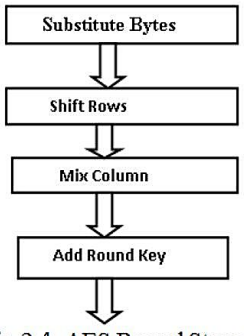


Fig.2.4. AES Round Steps

• **DES (Data Encryption Standard)**

DES [2] is a symmetric key algorithm. It uses a block size of 64 bits and key size of 56 bits. To encrypt the data which is 64 bits in size. It is a feistal structure which divides

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

a block into two equal size. It allows series of S-boxes and P-boxes. DES completes the 16 rounds of encryption.

- **3DES (Triple Data Encryption Standard)**

3DES [3] uses the Data Encryption Standard (DES) algorithm three times to each data block. It is also called T-DES. It has 64 bit block size and uses 56 bits of key length. It uses three 64 bit keys, so overall key length is 192 bits. The data can be encrypted first key the data can be decrypted again with the second key, and finally encrypted again with third key.

- **RC2**

RC2 is a symmetric block cipher security algorithm. It operates on block size of 64 bit and make use of variable size keys ranging from 8 to 128 bits. RC2 is susceptible to differential attacks

- **RC4**

RC4 is the stream cipher cryptography. It uses both encryption and decryption XOR together with a collection of generated keys. It uses keys of random length and this is commonly known as producer of pseudo arbitrary numbers.

- **RC5**

RC5 is the symmetric key cipher algorithm. It stands for "Rivest Cipher" .It is also called "Ron's code". It uses key sizes of 32,64 or 128 bits. But normally 64 bits are suggested. It uses 1 to 256 rounds. But normally 12 rounds are to be suggested. It is well suited for software and hardware implementations.

- **RC6**

RC6 is more accurately specified as RC6. RC6 uses a block size of 128 bits and uses key sizes of 128, 192 and 256 bits. RC6 structure is similar to RC5 in structure. It is symmetric cipher algorithm.RC6 is susceptible to brute force attacks

- **TWOFISH**

Two fish algorithm [7] is a symmetric block cipher cryptography. It is efficient for software. It uses key sizes of 128, 192 and 256 bits. It allows 16 rounds of encryption algorithm. It allows good level of security.

- **THREEFISH**

Three fish algorithm [13] is a symmetric block cipher. It is tweakable block cipher. It takes three inputs, a key, a tweak and block of message. It uses three types of keys 256 bits, 512 bits or 1024 bits.

- BLOWFISH Algorithm

Blowfish algorithm [15] is a symmetric key algorithm it has 64 bit block size and variable key length from 32 bits to 448 bits. It has larger key size so it is very difficult to break the code. It is strong encryption algorithm [13]. It has 16 rounds.

- **RSA algorithm.**

Rivest, Shamir and Adlemen developed RSA algorithm. RSA algorithm [14] is a asymmetric cryptography. RSA is a public key algorithm. It uses two keys. Public and Private Key is used for encryption and decryption. It is a highly secured public key encryption algorithm. By using this cryptography, it is very difficult to find what private key is used for public key.

- **Diffie Helman**

In this each party generates a key pair and distributes the public key. After obtaining an authentic copy of public keys, then shared secret can be used as the key for a symmetric cipher .The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure communication channel.

III. LITERATURE SURVEY

Many cryptographic algorithms have already been discussed.

Aamer Nadeem and Dr M. Younus Javed [1] describes the four of the popular secret key encryption algorithms, i.e., DES, 3DES, AES(Rijndael), and Blowfish. Their performance is compared by encrypting input files of varying contents and sizes, on different Hardware platforms. In this paper, authors compared the performance of the algorithms. Blowfish is fastest one. Blowfish uses larger block of size with single execution time cycle.

Ankita verma, Paramita guha, Sunitha Misra[2] compares various key algorithms i.e AES, DES, 3DES, Blowfish and RSA. They compared on different set of parameters. This study also states that AES and blowfish are the most secure algorithms. These algorithms provide better speed and power consumption when compared to other algorithms.

Brijesh Kumar Patel, Mukti Pathak [3] presents detailed analysis of symmetric and asymmetric algorithm is compared on the basis of different parameters. This paper analyzed the terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security. They presents blowfish has yet no attack.

Chaitali Haldankar, Sonia Kuwelkar[4] discussed AES and blowfish algorithms.They compared t the superiority of Blowfish algorithm with AES depending on throughput, processing time. Finally conclude that Blowfish is the best when compared to AES throughput and speed.

Deepika Rani Bansal and Preeti Thakur [5] reviewed different existing symmetric key and asymmetric key algorithms .They found that symmetric key algorithms are faster than Asymmetric key algorithms . In this survey, They suggest that blowfish performed best among other

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

symmetric key algorithms .They surveyed Performance of blowfish on various types of file like image file , text file , video file etc. with different loads under different operating system and various web browsers .

Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha[6] presents the performance evaluation of symmetric algorithms of AES,3DES, blowfish and DES. They concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES has least efficient of all the studied symmetric algorithms.

K.Lakshmi Narayanan [7] analyze encryption security depending on encryption speed and power consumption for both the algorithms. The author proved that the Blowfish encryption algorithm may be well suitable for wireless network application security. This paper discussed AES and BLOWFISH algorithms. These results showed that Blowfish has superior performance than AES since Blowfish has not any known security weak points. The blowfish considered as an excellent standard encryption algorithm. Blowfish algorithm is faster than AES. Thus Blowfish algorithm may be more appropriate for wireless.

Maulik P. Chaudhari , anjay R. Patel [8] describes that the Blowfish algorithm is faster than other encryption algorithm. It reduces the execution time and provides a better security and it reduces less memory usage when compared to any other algorithm. To improve the performance of blowfish to prevent from brust force attack, change the size of plain text and try o minimize the key size of blowfish and making round.

Mitali, Vijay Kumar and Arvind Sharma [9] discussed AES, DES, 3DES, and Blowfish algorithms. They have survived all strength and weakness of all algorithms. This focuses performance of these encryption algorithms. They surveyed that Blowfish has better performance than other algorithms followed by AES.

Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz [10] discussed AES, BLOWFISH, DES, RC4, RSA encryption algorithms. In this performance have been compared depends on key sizes and file sizes with all symmetric and asymmetric algorithms. They conclude that the symmetric encryption/decryption techniques are faster than the asymmetric encryption/decryption techniques

Pramod Gorakh Patil, Vijay Kumar Verma [11] discussed encryption techniques. They compared different parameters like key size, security level, modification and flexibility. The study of this paper blowfish and 3 DES give flexibility. And also allows high level of security.

Priyadarshini Patil,, Prashant Narayankar,Narayan D G, Meena S M [12] compares encryption techniques has its own strong and weak points. The comparison was made depends on performance, strength and weakness of the algorithms. Finally suggests that the memory required for implementation is smallest in blowfish whereas it is largest in RSA. DES and AES encryption algorithms require medium size of memory. So blowfish is best choice. Results shows that RSA consumes more time for encryption and decryption compared to others encryption algorithms. Blowfish consumes the least time amongst all. Blowfish is efficient in software. The concluded that AES can be used in applications where confidentiality and integrity is of highest priority. When evaluating DES, 3DES, AES, Blowfish and RSA algorithms based on parameters entropy, Blowfish secures highest priority; Blowfish is strongest against guessing attacks. When compared to time and memory in the application, Blowfish is the best suited algorithm. When compared to cryptographic strength is a major factor in the application, AES is the best suited algorithm. When compared to network bandwidth in the application; DES is the best suited algorithm.

Rajdeep Bhanot and Rahul Hans [13] analyzed a study on the encryption algorithms. They found that each algorithm has its own strengths depending in their different parameters. This study observed Strength of each algorithm depends on key agreement, types of encryption used, number of keys and key length. A comparison was made on basis of these parameters. It was concluded that blowfish is the more secure and fastest algorithm.

Rakhi Emeleya, Dr. Sanjay Agarwal [14] presents cloud security algorithms. They survey the study of RSA,RC4,KP –ABE ,AES and blowfish algorithms. A comparison was made with key length and computation time of different encryption algorithms. Finally suggests that blowfish algorithm give better performance and more security and strongest against intruders. It allows longer key size do it is more secure. But the encryption time is slow. The authors suggest that blowfish algorithm reducing of two S-boxes will increase the speed. Veena Parihar, Mr. Aishwary Kulshrestha [15] describes the study of blowfish algorithm. In this paper suggests blowfish does not have any week points. Blowfish is the standard encryption algorithm. This paper analyzed all types of image sizes and also the format that can be encrypted.

IV. COMPARISON BETWEEN SYMMETRIC AND ASYMMETRIC ALGORITHMS

Algorithm	Advantages	Disadvantages
Symmetric Key Algorithm	1)In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the	1)Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

	data, the chances of data being decrypted are null. 2)A symmetric cryptosystem uses password authentication to prove the receiver's identity. A system only which possesses the secret key can decrypt a message.	to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.
Asymmetric Key Algorithm	1) In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem 2) The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone. 3) Can provide digital signatures that can be repudiated	1)A disadvantage of using public-key cryptography for encryption is speed: there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

V. COMPARISON OF VARIOUS CRYPTOGRAPHY TECHNIQUES

Algorithms	**Algorithm type**	**Key size**	**Block size**	**Encryption & Decryption Key**	**Structure**	**Round**	**features**
AES [Advanced Encryption standard Algorithm]	Symmetric Key algorithm	128, 192, 256 bits	64 bits	Same	Substitution permutation	10, 12, 14	Excellent Security, Fast and Flexible
DES[Data Encryption standard Algorithm]	Symmetric Key algorithm	56 bits	64 bits	Same	Feistel	16	Not Strong Enough
3DES[Triple Data Encryption standard Algorithm]	Symmetric Key algorithm	112, 192, 256 bits	128 bits	Same	Feistel	48	Fast
RC2	Symmetric Key algorithm	8, 128, 64 by default	64 bits	Same	Feistel	16	Stream cipher
RC4	Symmetric Key algorithm	Variable	40-2048	Same	Feistel stream	256	Moderate security
RC5	Symmetric Key algorithm	0 to 2040 bits	32, 64 or 128 bits	same	-	12	--
RC6	Symmetric Key algorithm	128 to 256 bits	128 bits	Same	Feistel	20	Good Security
TWO FISH	Symmetric Key algorithm	128, 192, 256 bits	256, 512, 1024 bits	same	Feistel	16	Good security lacks in speed
THREEFISH	Symmetric Key algorithm	128 bits	256, 512, 1024 bits	same	Feistal	72	-
BLOWFISH	Symmetric Key algorithm	32-448 bits	64 bits	Same	Feistel	16	Good security, fast
RSA	Asymmetric Key algorithm	1024 to 4096 bits	128 bits	Different	Public key Algorithm	1	Excellent Security Low speed

VI. COMPARISION TABLE FOR STRENGH AND WEAKNESS OF VARIOUS CRYPTOGRAPHY

Algorithm	**Merits**	**Demerits**
AES	1) AES encryption is fast and flexible.	1) The size of key length is too long that makes it complex

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

	2) The AES has also been employed in other areas such as to secure information in smart cards and online transactions. 6) The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths.	sometimes.
DES	1) It has been a popular secret key encryption algorithm.	1)) Its key size is too small
3DES	1) It uses 64 bit block size with 192 bits of key size. It is simple like DES because the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. 2) 3DES is easy to implement in both hardware and software.	1) 3DES is slower than other block cipher methods. 2) It has poor performance.
RC2	1) RC2 is three times faster than DES in software implementations	1) The algorithm encryption speed is independent of key size
RC6	1) RC6 uses an extra multiplication operation that is not present in RC5. This helps to produce the dependency of the rotation on every bit of the word. .	1)The main performance limitation of RC6 is its Reliance on specialised hardware support for multiplication and rotation that is not available on many CPUs, in particular, on RISC and low end processors. Thus, there is a considerable variety in the cipher's performance results across different hardware platforms. 2) RC6 has favourable memory requirements that make the cipher suitable for implementation on limited resource devices such as smartcards.
BLOWFISH	1) Blowfish is fast as its encryption rate on 32-bit microprocessor is 26 clock cycles per byte. 2) It is compact as it can execute in less than 5 kb memory. 3) It is simple because it uses only primitive operations like addition, XOR and table lookup, making its design and implementation simple. 4) It has a	-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

	variable key length up to a maximum of 448 bits long making it both flexible and secure. 5) No attack is known to be successful against this. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. 6) Blowfish is considered to be the best out of all encryption algorithms.	
RSA	1) RSA is increased security: as the private keys do not ever need to be transmitted or revealed to anyone. Whereas in a secret-key system, there is always a chance that an enemy could discover the secret key while it is being transmitted. 2) Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. 3) Digitally signed messages can be proved authentic to a third party, such as a judge, thus allowing such messages to be legally binding.	1) A disadvantage of using public-key cryptography for encryption is speed: they are very slow in processing.
DIFFIE HELLMAN	1) One way authentication is free with this type of algorithm	1) The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack

VII. CONCLUSION

Data security is the most aspects of communication. Security of data is archived using encryption algorithms. In this paper we have analyzed various encryption algorithms. We compare DES, 3DES, AES, RC2, RC4, RC5, RC6, TWOFISH, THREEFISH, BLOWFISH and RSA algorithms. We observed that the strength of each encryption depends on key size, type of algorithm used, number of keys and number of bits in the key. We found that blowfish algorithm is best when compared to all symmetric key algorithms. Blowfish provides better performance because of its larger block size. This algorithm is more secure, work fast and also in future. And there is broad scope of implement in blowfish algorithm.

REFERENCES

[1] Aamer Nadeem, Dr M. Younus Javed "A Performance Comparison of Data Encryption Algorithms",IEEE-2005.

[2] Ankita verma, Paramita guha, Sunitha Misra,"Comparative Study of Different Cryptographic Algorithms" International journal of emerging

&Technology in computer science(IJETTCS),volume 5, Issue 2,March –April 2016

[3] Brijesh Kumar Patel, Mukti Pathak "Survey on Cryptography Algorithms" International Journal of Innovative Technology and Exploring Engineering (IJITEE),ISSN: 2278-3075, Volume-4 Issue-7, December 2014

[4]Chaitali Haldankar, Sonia Kuwelkar "Implementation of AES and blowfish Algorithm " IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN:2321-7308, Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014

[5] Deepika Rani Bansal and Preeti Thakur,"A review of symmetric key and asymmetric key encryption algorithms ", International Journal of Computer Science Engineering (IJCSE), Vol. 5 ,Mar 2016

[6] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Through Put Analysis of Various Encryption Algorithms", IJCST, Vol 2, September 2011

[7] K.Lakshmi Narayanan, "Performance Evaluation of Cryptographic Algorithms: AES and Blowfish", International Journal Of Technology And Engineering Science [IJTES]TM Vol 1(7), pp1064-1069, October 2013

[8] Maulik P. Chaudhari , anjay R. Patel "A Survey on Cryptography Algorithms" International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 3, March 2014

[9] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014

[10] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6,March 2016 .

[11] Pramod Gorakh Patil, Vijay Kumar Verma "A Recent Survey on Different ymmetric Key Based Cryptographic Algorithms" IJCAT - International Journal of Computing and Technology, Volume 3, Issue 2, February 2016 ISSN : 2348 – 6090.

[12] Priyadarshini Patil,, Prashant Narayankar,Narayan D G,, Meena S M "A comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Elsevier.

[13] Rajdeep Bhanot and Rahul Hans, "A review and comparative analysis of various encryption algorithms" , International Journal of Security and its application", vol.9, 2015.

[14] Rakhi Emeleya, Dr. Sanjay Agarwal , "A survey : Secure Data Storage Techniques in cloud computing", International journ.al on recent and innovation trends in computing and communication",volume 3, September 2015.

[15] Veena Parihar, Mr. Aishwary Kulshrestha, "Blowfish Algorithm : A detailed study", International Journal For Technological Research In Engineering,Volume 3,May-2016.