International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 12, Issue 4, (April 2016), PP.61-68

Security in Distributed Adaptive Networks Using Rsa Cryptographic Algorithm

Roohi Zuwairiyah V A[1], S Megha[2], Sadiya Mehdees Ghori[3], Sahana H P[4]

Department of Computer Science and Engineering
GSSS Institute of Engineering & Technology for Women, Mysuru

Abstract:- Information security in distributed systems and the use of networks for carrying data between computers is a major factor that has affected security. In this paper, we discuss security and propose security metrics issues in the context of Adaptive Distributed Systems [ADS]. A key premise of ADS is to collect detailed information based on the changes in the environment and choose efficient mechanisms (algorithms and/or encryption techniques, and secured and cost effective communication channel) for exchanging the gathered information between the targets distributed systems and the central monitoring system. Security issues in distributed systems have been solved using techniques such as cryptographic algorithms i.e. using RSA algorithm

Keywords:- Adaptive distributed Systems, Encryption techniques, Cryptographic algorithms, Security metrics, and RSA algorithm

I. INTRODUCTION

A Distributed system consists of a collection of autonomous computers linked by a computer network and equipped with distributed system software. The security of data transmission is a vital problem in Distributed Systems [10]. Usually, users exchange personal sensitive information or important documents. In this case; security, integrity, authenticity and confidentiality of the exchanged data should be provided over the transmission medium. Nowadays, internet multimedia is very popular such as social networking, E-initiative (e-banking, e–commerce, e–shopping) etc. These phenomenal changes have brought about the need for tight security to data and information as a significant amount of data is exchanged every second over a non-secured channel, which may not be safe. Therefore, it is essential to protect the data from attackers [18]. Data in transit is data being accessed over the network, and therefore could be intercepted by someone else on the network or with access to the physical media the network uses. E-banking, e-commerce, e-shopping, etc., transactions over the un-trusted Communications channels are now possible because of the application of data encryption mechanisms.

Data encryption solution provides solid protection in the event of a security breach. There is an increasing use of end-to-end encryption of traffic to hide the content of transactions from the network. With encrypted traffic the users are no longer incidentally exposing their communications to the network and thereby risking exposure of their communications to unknown third parties [11].

To improve security and reliability of data being transmitted on information and communications systems; cryptography is used. Cryptography is especially useful in the cases of transmission of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over un-trusted medium like the Internet. Cryptography is the science of keeping the transmitted data secure. It provides data encryption for secure communication. The encryption process is applied before transmission, and the Decryption process is applied after receiving the encrypted data. The information hiding Process is applied before transmission and the extraction process is applied after receiving. Cryptography encrypts the message and transmits it; anyone can view the encrypted message, but is very difficult to be understood, especially if it has been encrypted with a strong cryptographic algorithm such as RSA cryptographic algorithm [17].

In RSA cryptography, **RSA** stands for Ron Rivest, Adi Shamir and Leonard Adleman is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

II. CRYPTOGRAPHIC ALGORITHMS

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA and ECC).

A. Symmetric Cryptography

Symmetric algorithms convert plain-text into cipher text which is unreadable, using a single key. They decrypt the cipher text using the same key. This key is kept secret among sender and receiver so that no intruder can access or steal the data being transferred by encrypting it. Symmetric key algorithms are primarily used for the bulk encryption of data streams. These algorithms are very fast and have a large number of possible keys. The best symmetric key algorithms offer excellent confidentiality; once data is encrypted with a given key, there is no fast way to decrypt the data without possessing the same key. These algorithms are relatively simple and quick, but if third parties intercept the key they can decrypt the messages.

Symmetric key algorithms can be divided into two categories: block and stream. Block algorithms encrypt data a block (many bytes) at a time, while stream algorithms encrypt byte by byte (or even bit by bit).

Some of the symmetric key algorithms are DES and Triple DES, RC2, Blowfish and Two fish, Serpent, etc.

Types of Symmetric Algorithms:

1) DES (Data Encryption Standard): DES is a block encryption algorithm. It was the first encryption standard published by NIST (National Institute of Standards and Technology [20]. It is an example for symmetric algorithm, this algorithm makes use of the same key for encryption as well as decryption. It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation, 8 bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part [22]. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text. There are many methods to prove the weakness of DES, which made it an insecure block cipher key.

2) 3DES (Triple Data Encryption Standard): Triple Data Encryption Standard (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA). It is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block. Triple-DES is also proposed by IBM in 1978 as a substitute to DES. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text [19].

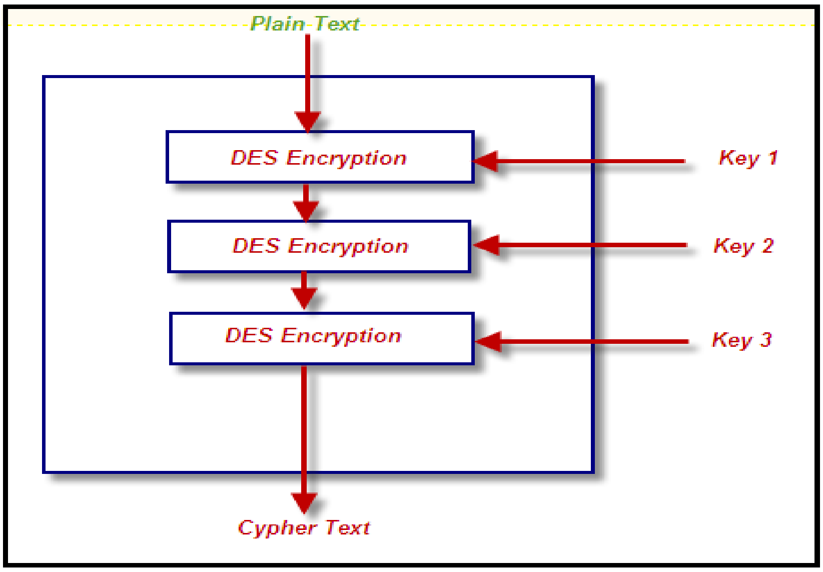

Fig.1: 3DES Structure

The encryption in this case is made more stronger by encrypting the same data two times more using DES, making the encryption more difficult to break and increasing the encryption level and the average safe time. It uses 64 bit block size with 192 bits of key size 3DES is slower than other block cipher methods [22].

3) AES (Advanced Encryption Standard): **In** 2001, the National Institute of Standards and Technology (NIST) choose the Advanced Encryption Standard as a replacement to DES and 3DES. It was recognized that DES was not secure because of advancement in computer processing power [22]. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [19].

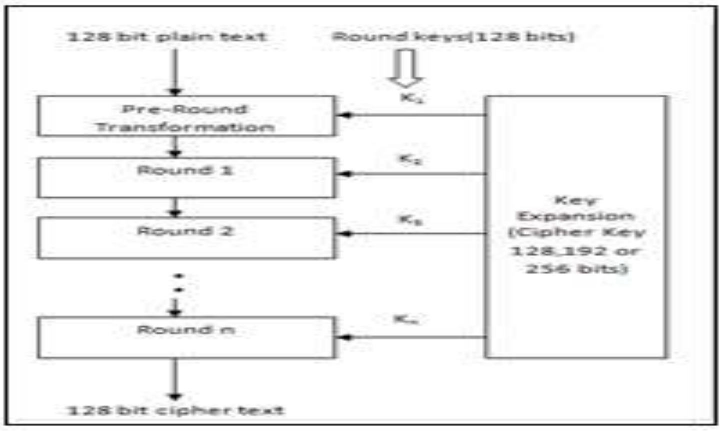

Fig.2: AES Algorithm

In each case, all other rounds are identical, except for the last round [19]. Each round in encryption process further follows some steps to complete each round till n. Each round further possess four rounds they are Substitute byte, Shift rows, Mix Column and Add round key.

4) Blowfish: Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round Feistel cipher and uses large key dependent S-Boxes. Each S-box contains 32 bits of data [19]. Schneier released Blowfish as a public-domain algorithm, freely available to anyone wanting to encrypt data.

Basically, Blowfish encryption algorithm requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles. Blowfish contains 16 rounds. Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Key expansion generally used for generating initial contents of one array and data encryption uses a 16 round feistel network methods. Fig1 shows how blowfish algorithm works. plain text and key are the inputs of this algorithm.64 bit plain text taken is divided into two 32 bits data and at each round the given key is expanded and stored in 18 p-array and gives 32 bit key as input and XORed with previous round data. Then,

```
for i = 1 to 14:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P15 and xL = xL XOR P16.
Finally, recombine xL and xR to get the cipher text
```

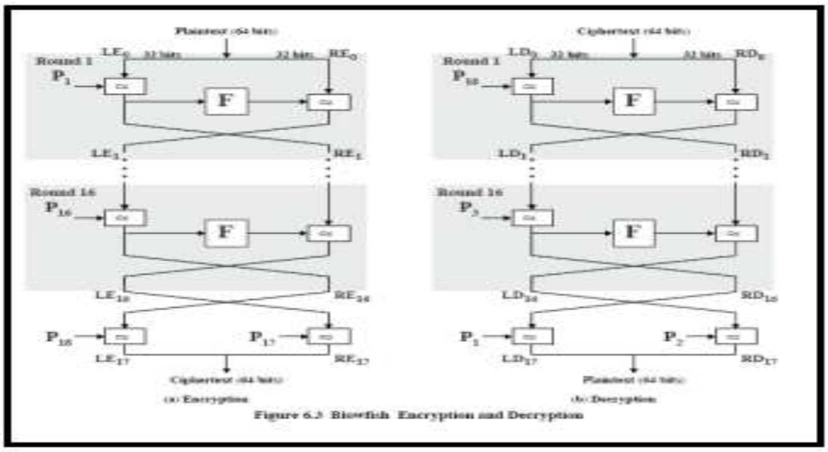

Fig.3: Blowfish encryption and decryption algorithm

Decryption is exactly the same as encryption, except that P1, P2... P18 are used in the reverse order [19]

5) Two fish: Twofish is also a symmetric block cipher having fiestel structure. It is developed and explained by Bruce schneier in 1998. This also uses Block cipher. It is efficient for software that runs in smaller processor. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Twofish is license-free, un-patented and freely available for use. In Twofish encryption it uses key sizes of 128, 192 and 256 bits. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm [19].

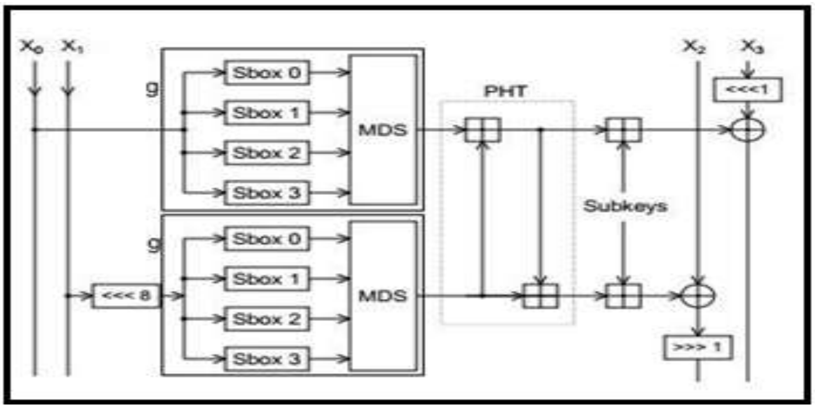

Fig.4: Round Function of Twofish

Above figure shows the Round function working of Twofish. This round function encrypts the data. This round function repeatedly encrypts the data 16 times and then gives final cipher text after the 16th round.
In above figure,

1. X0 and X1 on the left of the inputs to the g functions after the rotation by 8 bits of one of them.
2. The g function consists of 4 byte key-dependent S-boxes followed by a linear mixing step (MDS matrix).
3. The results of the two g functions are combined using a PHT (Pseudo-Hadamard Transform).
4. After that two keywords are added. One right among them is rotated by 1 bit and then both of these keywords are XORed into the result on the left.
5. For next round, right and left halves swapped.
6. After 16 rounds of encryption, the last swap is reversed and four keywords are XORed with another four keywords to produce the final encrypted text or cipher text.

Twofish encryption algorithm also provides good level of security but it lacks in encryption speed as compared to blowfish [19].

Some of the other Symmetric Cryptographic algorithms are RC2, RC3, RC5, Serpent, etc.

Though these algorithms are considered as best in performance wise, these algorithms are relatively simple and quick, but if third parties intercept the key they can decrypt the messages. To overcome this drawback asymmetric encryption comes into picture.

B. Asymmetric Cryptography

Public-key cryptosystems help solve the key distribution problem by using separate keys for encryption and decryption, and making the encryption key public. Anyone can then encrypt a message, but only parties in possession of the private key can decrypt messages. Public key systems rely on one-way trap door functions, which are interesting mathematical functions that can be easily computed in one direction but are very difficult to reverse unless a secret key is known (the trap door). Since the encryption key is made public, finding the private encryption key from the public. Encryption key must be intractable.

Types of Asymmetric Algorithms:

1) *RSA (Rivest Shamir and Adleman) Algorithm:* RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [1]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key [2]. The prime factors must be kept secret. Anyone can use the public key to encrypt a message. The RSA algorithm involves three steps:

□ Key generation
□ Encryption and
□ Decryption

Key generation

RSA involves a **public key** and a **private key.** The public key can be known by everyone and is used for encrypting messages. The private key is used to decrypt the message which is encrypted with the public key. The keys for the RSA algorithm are generated the following way:

- Choose two distinct prime numbers p and q, the integers p and q should be chosen at random.
- Compute $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are co-prime. e is released as the public key exponent. Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$). This is more clearly stated as solve for d given $d{\cdot}e \equiv 1 \pmod{\varphi(n)}$ d is kept as the private key exponent. By construction, $d{\cdot}e \equiv 1 \pmod{\varphi(n)}$.
- The public key consists of the modulus n and the public (or encryption) exponent e.
- The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He then computes the cipher text c corresponding to

c=m^e(mod m)

Bob then transmits c to Alice.

Decryption

Alice can recover m from c by using her private key exponent d via computing

m=c^d (mod n)

Given m, she can recover the original message M by reversing the padding scheme

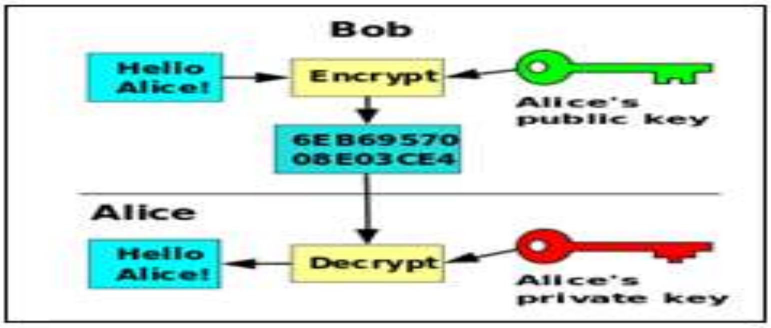

Fig.5: RSA Encryption and Decryption

2) Diffie-Hellman Algorithm: This algorithm is used for exchanging cryptography keys between two users. Here user doesn't know about the keys used by each other and they use a shared secret key for communication, then this key is used to encrypt subsequent communications using a symmetric key cipher. New protocol proposed for two goals:

1. Authenticated key agreement and
2. Authenticated key agreement with key confirmation

These protocols in the asymmetric (public-key) setting is given by Simon Blake-Wilson et al. [4].The oracle model provides formal definitions of AK and AKC and is proposed with several variants which is demonstrated to provide security. Here AK and AKC are made secure by providing clear, formal definitions of the goals of AK and AKC protocols, and secondly by furnishing practical, provably secure solutions in the random oracle model [4]. Briefly speaking; the process of providing security can be explained in five steps [4]:

a. Specification of model
b. Definition of goals within this model
c. Statement of assumptions
d. Description of protocol
e. Proof that the protocol meets its goals

3) Digital Signature Algorithm (DSA): DSA is used to verify the sender's identity and to check that the message has not been altered during transmission .A digital signature is an electronic version of a written signature in that the digital signature can be used by recipient to check that the message was signed by the sender. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time [6]. One method for sending low size and capacity data by using DSA is proposed by Erfaneh Noorouzil et al. "Hash function" is used in this method and it generates dynamic and smaller size of bits which depends on each byte of data. The main function which is used for hashing is bitwise or and multiply functions. If hashed file sized is 4% of the original file in the messages with size lower than 1600 bytes. This algorithm can be used in several applications which have low file size for sending and want simple and fast algorithms for generating digital signature [7].

This algorithm works on ".doc, .pdf, .txt" and other types of files, and hash function can be used for dynamic size of data. The term dynamic means, results of hash function depends on size of the data [8].

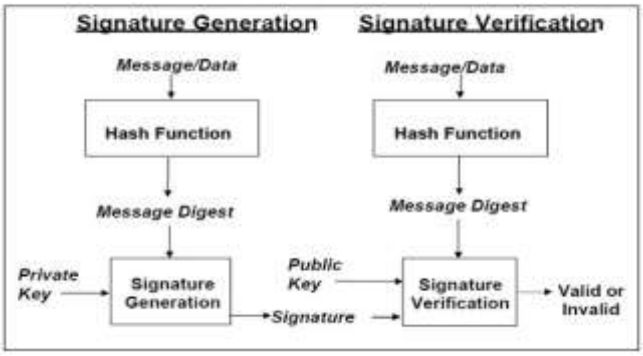

Fig.5: Digital Signature Process

III. DISCUSSION

This paper also gives a comparison of all the above algorithms described. The systems that have been studied have certain common features [15]. Though symmetric algorithms are considered as best in performance wise, these algorithms are relatively simple and quick, but if third parties intercept the key they can decrypt the messages. To overcome this drawback asymmetric encryption comes into picture. Public-key cryptosystems help solve the key distribution problem by using separate keys for encryption and decryption, and making the encryption key public [16]. Either key may be used for encryption or for decryption, but the most important point is that the private key never be revealed. Anyone can then encrypt a message, but only parties in possession of the private key can decrypt messages.

In asymmetric cryptosystems, we can achieve the following basic form of security: authentication, integrity, and nonrepudiation by using what is called as digital signature.

The advantages of distributed systems is

Reliability**:** If one machine crashes, the system as a whole can still survive.

Speed**:** A distributed system may have more total computing power than a mainframe.
Open system: Since it is an open system it is always ready to communicate with other systems and allows scalability.

Table I: Consolidated Report of Cryptographic Algorithms

PARAMETER	SYMMETRIC ENCRYPTION				ASYMMETRIC ENCRYPTION	
	DES	3DES	AES	BLOWFISH	DIFFIEHELL MAN	RSA
KEY USED	Same key used for encryption & decryption	Same key used for encryption & decryption	Same key used for encryption & decryption	Same key used for encryption & decryption	Key exchange	Different key used for encryption & decryption
KEY LENGTH	56 bits	112 to 168 bits	128,192,or 256 bits	32 bits to 448 bits	Key exchange management	>1024 bits
TUNABILITY	No	No	No	Yes	Yes	Yes
SPEED	Fast	Fast	Fast	Fast	Slow	Fast
SECURITY	Very Low	A little higher than DES	High	Medium	Larger the key size, the more it is secure	Larger the key size, the more it is secure
SECURITY AGAINST ATTACKS	Brute force attack	Brute force, chosen plain text, known plaintext	Chosen plain, known plain text	Dictionary attacks	Eavesdropping	Timing attacks
DIGITAL SIGNATURE AND VERIFICATION	Inconvenient	Inconvenient	Inconvenient	Inconvenient	Convenient	Convenient
USAGE	for encryption & decryption (confidentiality),can't be used for integrity & non repudiation checks	for encryption & decryption (confidentiality),can't be used for integrity & non repudiation checks	for encryption & decryption (confidentiality),can't be used for integrity & non repudiation checks	for encryption & decryption (confidentiality),can't be used for integrity & non-repudiation checks	for encryption & decryption (confidentiality),as well as for integrity & non repudiation checks	for encryption & decryption (confidentiality),as well as for integrity & non repudiation checks
KEY EXCHANGE	Exchanging of key is a big problem	Exchanging of key is a big problem	Exchanging of key is a big problem	Exchanging of key is a big problem	Not a problem	Not a problem

IV. CONCLUSIONS

In this study, we did a comprehensive review of public and private key cryptosystems in general and RSA algorithm in particular. This paper provides evaluation of encryption algorithms like AES, DES, 3DES, Blowfish [14], and RSA, Diffie Hellman. The paper presents various schemes which are used in cryptography for Network security purpose. A comparison has been conducted for those encryption algorithms and RSA is found to be the best encryption algorithm for distributed systems. Several points can be concluded from the simulation results. RSA encrypts message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security [13]. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity.

In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds [12].

REFERENCES

[1]. Perrig, J. Stankovic, and D. Wagner, *"Security In Wireless Sensor Networks,"* ACM, Vol. 47, No.653.2004.

[2]. Chandra M. Kota et al., *"Implementation of the RSA algorithm and its cryptanalysis,"* In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002.

[3]. Wikipedia, *"http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange,"* Dated: 13-dec-2012 at10:33.

[4]. Simon Blake Wilson, *"Key agreement protocols and their security analysis,"* 9-sep-1997.

[5]. David A. Carts, *"A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols,"* SANS institute, 5-nov-2001.

[6]. Vocal, *"http://www.vocal.com/cryptography/dsa-digital-signature-algorithm/,"* 13-dec-2012 at 13:18.

[7]. Erfaneh Noorouzil, *"A New Digital Signature Algorithm",* International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.

[8]. WilliamStallings,*"http://williamstallings.com/Extras/SecurityNotes/lectures/authent.html",*13-dec-2012at 14:05.

[9]. *"File Encryption and Decryption Using Secure RSA",* Rajan.S.Jamgekar, Geeta Shantanu Joshi, International Journal of Emerging Science and Engineering (IJESE)ISSN: 2319–6378, Volume-1, Issue-4, February 2013

[10]. Vijay Prakash, Manuj Darbari, *"A Review on Security Issues in Distributed Systems"*, Intenational Journal of Scientific and Engineering Research,Vol. 3,Sept. 2012.

[11]. Oleksandr Bodriagov, Sonja Buchegger,*"Encryption for Peer-to-Peer Social Networks"* , IEEE Third International Conference on Social Computing,2011.

[12]. Sen-Ching Samson Cheung,Yan Lindsay Sun, *"Guest Editional Special Issue on Privacy and Trust Management in Cloud and Distributed Systems"*, IEEE Transactions on Information Forensics andSecurity,Vol. 8,June 2013.

[13]. Meenakshi Shankar Akshaya.P, *"Hybrid Cryptographic Technique using RSA algorithm and Scheduling concepts"*, International Journal of Network Security and its Application,Vol. 6, Nov 2014.

[14]. Gurpreet Singh, Supriya, *"A study of Encryption Algorithms (RSA, DES, 3DES AND AES) FOR Information Security"*, International Journal of Computer Applications,Vol. 67,April 2013.

[15]. Rajdeep Bhanot, Rahul Hans, *"A Review and Comparative Analysis of Various Encryption Algorithms",* International Journal of Security and its Applications, Vol. 9, 2015.

[16]. Thomas Beth, Dieter Gollmann, *"Algorithm Engineering for Public Key Algorithms"*, IEEE Journal on selected areas in communications, Vol. 7, May 1989.

[17]. Mukund R.Joshi, Renuka Avinash Karkale *"Network security with Cryptography",* Vol. 4, January 2015.

[18]. Manoj Kumar, Nikhil Agrawal, "*Analysis of Different Security Issues and Attacks in Distributed System",* International Journal of Advanced Research in Computer Science and Software Engineering, April 2013.

[19]. Rajdeep Bhanot and Rahul Hans, "*A Review and Comparative Analysis of Various Encryption Algorithm*", International Journal of Security and Its Applications, Vol. 9, No. 4 (2015)

[20]. Jawahar Thakur, Nagesh Kumar, "*DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Anaysis*", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011

[21]. Saikumar Manku and K. Vasanth, "*Blowfish Encryption Algorithm for Information Security*", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 10, JUNE 2015

[22]. Pratap Chandra Mandal, *" Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish",* Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012