OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Design of a Software Tool to Verify the Security Level of Cryptographic Algorithm

Roohi Zuwairiyah V A[1], S Megha[2], Sadiya Mehdees Ghori[3], Sahana H P[4]
[1, 2, 3, 4] *(Department of Computer Science and Engineering, GSSSIETW, India)*

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] which acts as a software tool using which we verify the strength of the cryptographic algorithm. 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 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 [1]. 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. 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.

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.

In RSA cryptography, **RSA** stands for Ron Rivest, AdiShamir and Leonard Adleman is an algorithm used by modern computers to encrypt and decrypt messages [2]. 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. REVIEW OF LITERATURE

Adaptive Distributed Systems (ADSs) are distributed systems that can evolve their behaviour's based on changes in their environments. A mainstay with adaptation of distributed systems is that in order to detect changes, information must be collected by monitoring the system and its environment. Contrariwise, the impact of implementation of security mechanism on the adaptation of distributed system is also determined. There should be security against the unauthorized access of the network and the information transmitted over the networks.

There are many researches done and are being done on the various security issues in distributed adaptive networks. The most of the literature works which are considered here discusses about the various security metrics involved in a secure distributed adaptive network.

Table.1 Overview of survey on Literature

SL.NO	TITLE	AUTHORS	TECHNIQUE
1.	"Evaluation of performance of Symmetric key algorithms: DES, 3DES, AES & Blowfish" Journal of Global Research in Computer Science, Volume 3, No 8, August 2012 **[3]**	Pratap Chandra Mandal	Internet and networks applications are growing very fast. So the importance and the value of the exchanged data over the internet are increasing. Information Security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security systems. This paper provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds, block size, key size, and encryption/decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES. Simulation program is implemented using Java programming.
2.	"Analysis of Different Security Issues and Attacks in Distributed System", International Journal of Advanced Research in Computer Science and Software Engineering, April 2013 **[4]**	Manoj Kumar, Nikhil Agrawal	This paper discusses the need of more secure distributed environment in which all transaction and operations can be complete successfully in a secure way. In distributed System environment it is very important to provide service at anytime, anywhere to the customers, this require proper time management of all computing and networking resources, resource allocation on time and their proper utilization. In distributed environment security is primary concern. In this paper an analysis of different security issues related to data, physical security, network security, possible distributed system attacks, has been made.
3.	"Implementation of Security in Distributed Systems – A Comparative Study", International Journal of Computer Information Systems, Vol. 2, No. 2, 2011 [1]	Mohamed Firdhous	This paper presents a comparative study of distributed systems and the security issues associated with those systems. Four commonly used distributed systems were considered for detailed analysis in terms of technologies involved, security issues faced by them and solution proposed to circumvent those issues. Finally the security issues and the solutions were summarized and compared with each other.
4.	"Network security with Cryptography", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, [5]	Mukund R.Joshi, Renuka Avinash Karkale	Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be Private, such as within a company, and others which might be open to public access.

5.	"Secure Communication using RSA Algorithm for Network Environment" International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 7, May 2015 [6]	Vivek Kapoor, Amrita Jain	Secure communication in network environment is primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and e-commerce transactions, digital signatures using public key cryptography is extensively employed. This research paper has proposed to develop a hybrid technique using Symmetric & Asymmetric key cryptography. It will also include Message authentication code to maintain integrity of message. Therefore, proposed model will not only help to maintain confidentiality and authentication of message and user but integrity of data too. Java technology has been proposed to validate the performance of proposed model in context of message length, key length, cipher text length and computational time for encryption and decryption.
6.	"A Review of RSA Cryptosystems and Cryptographic Protocols" West African Journal of Industrial & academic research Vol.10 No.1. April, 2014 [7]	Prince Oghenekaro Asagba, Enoch O. Nwachukwu	The use of cryptography in information security over insecure open network in both the convectional symmetric encryption and the public-key cryptography has witnessed tremendous developments over the years. The public-key cryptography is an established technology in terms of modern approach in information security despite the seemingly challenges it has. This paper, gives an overview of the public-key cryptography with emphasis on the RSA algorithm. A review of public-key cryptography i.e. RSA cryptosystems and cryptographic scheme, some security issues and challenges of RSA is performed. The objective of this paper is to present holistic appraisal of the RSA cryptosystems.
7.	"A Review and Comparative Analysis of Various Encryption Algorithm" International Journal of Security and Its Applications, Vol. 9, No. 4 (2015) [8]	Rajdeep Bhanot and Rahul Hans	Cyber-attacks broke all the security algorithms and affected the confidentiality, authentication, integrity, availability and identification of user data. Cryptography is one way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. In this paper, we have analyzed ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA etc. Among them DES, Triple DES, AES, RC5, BLOWFISH, TWOFISH, THREEFISH and IDEA are symmetric key cryptographic algorithms.

III. METHODOLOGY

Many encryption algorithms are available and used in information security for communication over untrusted channels. This paper discusses the design of software system tool called as a distributive adaptive system which comprises of 2 or more clients and a server. The strength or the security level of the cryptographic algorithm is tested by introducing a third person or an intruder within the software tool while the communication process is happening. So, now the intruder receives an encrypted text while trying to access the data during transmission. In this paper, the software tool is developed in Windows C#, Socket Programming & ado.net.

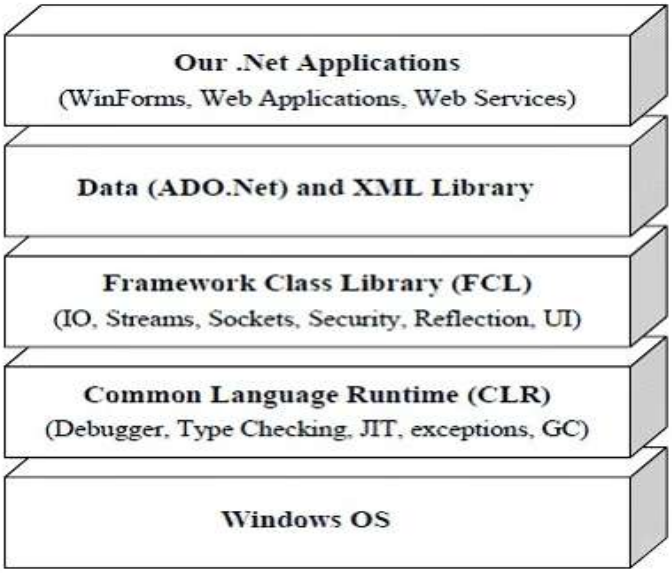

Figure 1: The .NET Framework.

In the above figure, it is seen that the .NET framework sits on top of the operating system. At the base of the .NET Framework is the Common Language Runtime (CLR). The CLR is the engine that manages the execution of the code. This layer contains classes, value types, exceptions and interfaces that one often uses in the development process. The next layer up is the .NET Framework Base Classes. The frame work class library is a standard library Microsoft .NET framework implementation of the standard libraries. The FCL is a collection of reusable classes, interfaces and value types. The next layer up is the ADO.NET which is a set of computer software components that programmers can use to access data and data services from the database. It is a part of the base class library that is included with the Microsoft .NET Framework. Most notably within the .NET Framework Base Classes is ADO.NET, which provides access and management of data.

The next layer of the framework is ASP.NET and Windows Forms. Using ASP.NET, it's possible to build robust Web applications that are even more functional than Win32 applications of the past. This was always quite difficult to do in the stateless nature of the Internet, but ASP.NET offers a number of different solutions to overcome the traditional limitations on the types of applications that were possible. The ASP.NET section of the .NET Framework is also where the XML Web services model resides. SOAP is a standard XML based protocol that communicated over HTTP.SOAP is a message format for sending messaged between applications using XML. It is independent of technology, platform and is extensible too.

A.**Implementation Of Distributed Adaptive System As A Tool**

In this module, we implement a software tool which runs as a Distributed Adaptive Network which includes Client & Server Application using C# socket programming.

C# simplifies the network programming through its namespaces like System.Net and System.Net.Sockets.A Socket is an End-Point off to and From (Bidirectional) communication link between two programs (Server Program and Client Program) running on the same network. Two programs are needed for communication of a socket application in C#. A Server Socket Program (Server) and a Client Socket Program (Client). The C# Server is multithreaded so connection can be made to more than one Client program to the Server.

C# Server Socket Program: A C# Server Socket Program running on a computer has a socket that is bound to a Port Number on the same computer and listens to the client's incoming requests.

C# Client Socket Program: A C# Client Socket Program has to know the IP Address (Hostname) of the computer that the C# Server Socket Program resides on and the Port Number assigned for listening for the client's request.

Once the connection is established between Server and Client, they can communicate (read or write) through their own sockets.

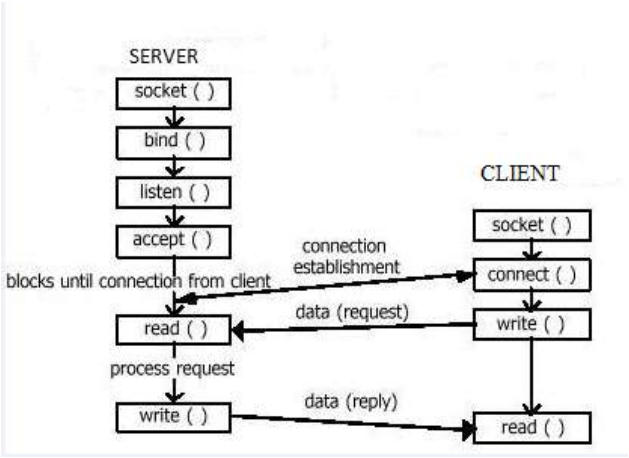

Figure 2. Communication between Client-Server Using C# Socket Programming

Here, the distributed system is created by having multiple instances of client applications and a server application. The client first has to register itself before sending and receiving data from the server. Once, he/she has successfully registered, a client application is started which contains a wall where he/she can post text & that text is received by server. The server application has a private key and it uses it to encrypt text & broadcasts the encrypted text to all users in the adaptive network.

B. **Creation Of An Intruder System**

An intruder is an unregistered client who tries to access data while it is in transit from the authorized clients to the server or vice versa. Inevitably, some information in the distributed system has to be downloaded or emailed, and this travel time is fraught with risk. When data is in transit, it can be subject to eavesdropping or tampering at various points in its journey. The consequences of not encrypting content – and subsequently losing or misplacing it – can be very damaging. The majority of data breaches stem from hack attacks, followed by data that's lost while physically in transit. So, an intruder system is intentionally introduced within the software tool so as to check its security level.

c.Encryption And Broadcasting Of Data Using Rsa Cryptographic Algorithm

Sensitive or confidential content must be encrypted both in transit, such as when sent via email; and at rest, such as when it is stored on flash drives, FTP servers, distributed systems or in cloud-based storage systems. Encryption can be not only a defence against inadvertent or malicious loss of data, but can actually generate a significant return-on-investment. It can also create new business opportunities, help businesses to retain or gain new customers, and provide competitive differentiation.

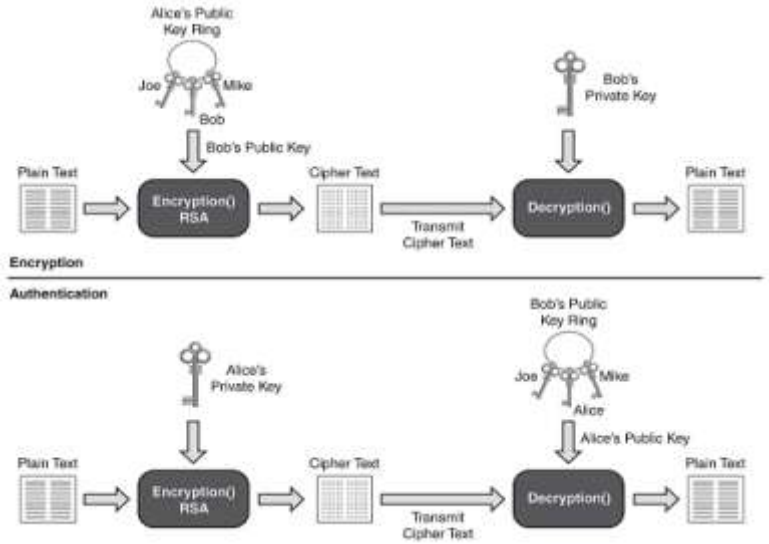

Figure 3. Encryption and authentication of the text using RSA algorithm

Cryptography was invented to protect communications: data in motion. A comparison of encryption algorithms is performed and RSA is found to be the best encryption algorithm amongst them for distributed systems.

Here, the client sends a message to the server. Server receives textual information sent by each client and encrypts the received text using RSA algorithm. This cipher text is broadcasted to all the registered clients in the network along with the public key using which the respective clients will be able to de-cipher the message. Every client who receives encrypted information with public key sent by server will be able to decrypt in their respective places making use of the private key. Thus, authorized users will hold a private key to decrypt the data sent by the server.

RSA ALGORITHM

Step 1: Start
Step 2: Assign two large prime numbers to p and q respectively.
Step 3: Compute n=p*q and also compute z= (p-1) *(q-1).
Step 4: Choose a number relatively prime to z and call it D
Step 5: Find e such that e*d =1(mod z) [e->Used for Encryption technique]
Step 6: Let us assume a character s->19 [whose value is 19]
Step 7: Encrypt S using the value of e
Step 8: To obtain the cipher text we mod the encrypted value with value of n.
Step 9: In this step we generate a secret key using a technique [power (cipher text, d)]
Step 10: This encrypted text is sent to the server/peers.
Step 11: The value of key is mod with the value of n to obtain decryption.
Step 12: Stop.

Explanation:

Assume that the values of p and q are 3 and 11.
Now get the values of n and z where n=p*q [i.e. 3*11=33] and z= (p-1)*(q-1), [i.e. 2*10=20].
Choose a number relatively prime to z. So assume d=7.
Find e such that e*d=1(mod z) [i.e. 7e=1 mod 20] thus, e=3. Encrypt a character 'S' using above technique. Let the value of 'S' be 19.
To obtain the encryption, [Power (19, e) ----> power (19, 3) =6859].
To obtain the cipher text, mod the encrypted value of s with value of n [6859 mod 33 =28].
To Obtain the secret key, power (cipher text, d) [i.e. power (28, 7) =134929……etc.]
This secret key is always sent to peers or servers.

C. **Verify The Strength Of The Algorithm**

The strength of the algorithm is found by introducing an intruder within the software tool. This tests the security level of the software tool i.e. distributed adaptive networks and the strength of the cryptographic algorithm. Also, it provides highly secure & reliable communication within the system avoiding anonymous users in the system to trace the conversations.

Security is implemented for anonymous access in the system using RSA implementation holding private & public keys. If anonymous user in the network don't have a public key, he/she is unable to decrypt text. Hence the conversation is displayed as encrypted text.

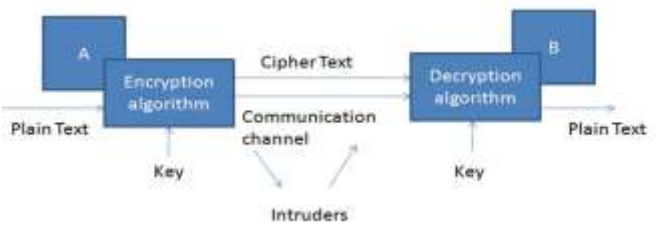

Figure 3: Intruder receives cipher text when he tries to access data in transit

IV. RESULTS AND DISCUSSIONS

The aim of this paper is to develop and implement a software tool i.e. distributed adaptive network in social community applications and to monitor their conversations within the system by checking the strength of security within the system.The purpose of this paper is to report the results of the practicality of developing metrics for use in specifying the strength of cryptographic algorithms. Also it provides highly secure & reliable communication within the system by avoiding anonymous users in the system to trace the conversation between the clients of the distributed systems. This paper only deals with a selected asymmetric key algorithm and RSA in particular. Other algorithms and cryptographic techniques for message integrity, authentication, and digital signatures were not investigated. Only information available in the public domain was used during this investigation.

The paper presents the Encryption and Decryption of text using RSA cryptographic algorithm.

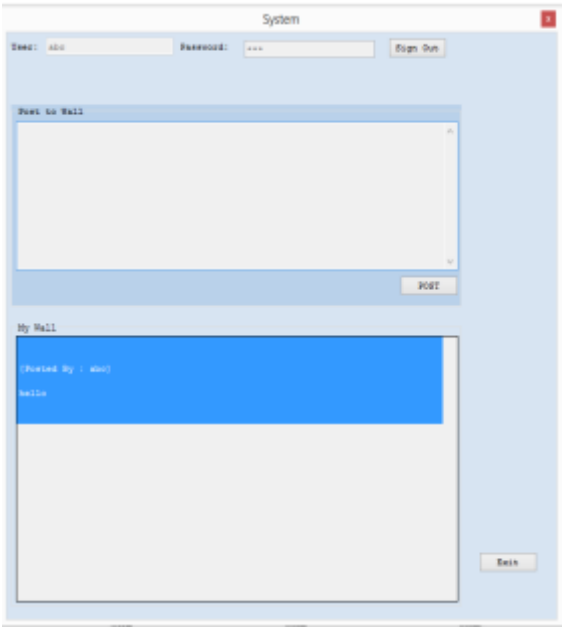

Figure 4

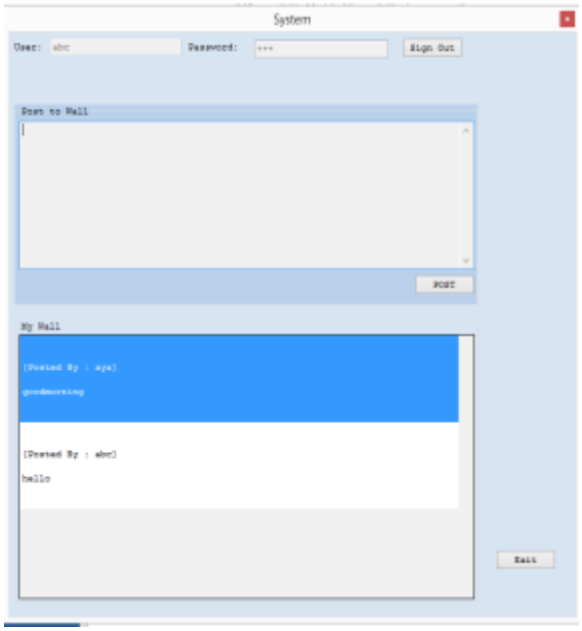

Figure 5

Fig.4-5: shows the interaction of clients with each other. When a client posts a message on his wall, it can be seen on other client's wall who have been registered.

Figure 6

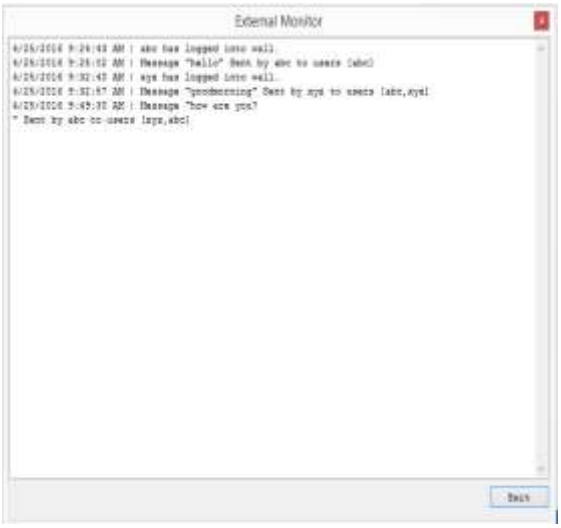

Figure 7

Fig.6 shows the Hacker who is receiving the messages in encrypted form. Hacker is a client who is not registered.
Fig.7 shows the Server receiving the updates of interaction of two or more clients. Server gets the update when a client logs in, posts the message and logs out.

V. CONCLUSION

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, and RSA, Diffie Hellman [9]. 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 [10]. 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. 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 [11].

REFERENCES

Journal Papers:

[1]. Prince Oghenekaro Asagba, Enoch O. Nwachukwu, A Review of RSA Cryptosystems and Cryptographic Protocols. West African Journal of Industrial & academic researchVol.10 No.1. April, 2014

[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]. 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

[4]. 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.

[5]. Mukund R.Joshi, Renuka Avinash Karkale, Network Security with Cryptography, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015.

[6]. Vivek Kapoor, Amrita Jain, Secure Communication using RSA Algorithm for Network Environment. International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 7, May 2015

[7]. Mohamed Firdhous, Implementation of Security in Distributed Systems – A Comparative Study, International Journal of Computer Information Systems, Vol. 2, No. 2, 2011

[8]. 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)

[9]. Saleh Saraireh, A Secure Data Communication System using Cryptography and Steganography, International Journal of Computer Network & Communications, Vol. 5, May 2013.

[10]. 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.

[11]. 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.