Performance Analysis on The Implementation of Data Encryption Algorithms Used In Network Security

Qurat Ashraf[1], Ambreena Muneer[2], Suhail Javid[3], Yasir Saleem Khan[4], Aasifa Arabi[5]
[1, 2, 3, 4, 5] Dept of Computer Science Engineering
[1, 2, 3, 4, 5] Iqbal Institute of Technology and Management

Abstract- *Over the last few years, e-commerce has become very popular; it is growing rapidly, improving business efficiency and reducing business process costs. Nowadays, e-commerce is a main channel for sales and services. Furthermore, various types of e-commerce services have been developed such as e-banking, e- shopping, e-bills and e-payments. E-commerce is not reliable without security. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. Cryptography plays a vital role in the field of network security. Currently many encryption algorithms are available to secure the data but these algorithms consume lot of computing resources such as memory and CPU time. This paper mainly focuses on comparative analysis of four symmetric encryption algorithms such as DES, TripleDES, AES and Blowfish. These algorithms are compared and performance is evaluated by means of encryption and decryption time, throughput, and memory usage. The implementations are carried out using the Java program on two computers with different operating system i.e. window 7 and window8.*

Keywords- Data Encryption, Performance Analysis, Implementation, Network Security, Cryptography.

I. INTRODUCTION

Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism. There is no single mechanism that will provide all the services specified. But we can identify a very important mechanism that a support all forms of information integrity is cryptographic technique. Encryption of information is the most common means of providing security.

Cryptography is one of the most important tools that enable e-commerce because cryptography makes it possible to protect electronic information. As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. 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. The key should be distributed before transmission between entities. E.g. RC2, DES, 3DES, RC6, Blowfish, and AES. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. 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 Digital Signatures).

Objective of the Study

Internet and networks applications are growing very fast, so the needs to protect such applications are increased. This paper provides evaluation of four of the most common encryption algorithms namely: AES, DES, 3DES, and Blowfish. The objective of this paper is to evaluate and compare the performance of data encryption algorithms by doing experimental analysis. Their functionality will be simulating by java programming language. The performance differential parameter will be analysed by means of throughput, CPU process time, memory utilization, and encryption and decryption time, different size of data block, and different key size. Based on the simulation result, we will recommend which encryption algorithm protocol efficient in resource usage.

Scope of the Study

There are three categories of encryption algorithms in cryptography. Symmetric key algorithms, asymmetric key algorithms and combination key algorithms. Encryption will make the data more secure on single system as well as on the cloud network. The algorithms will run on single system as well as on cloud network. In this project, four data encryption algorithms have been considered; these are AES, DES, 3DES, and Blowfish.

In this paper, the behavior of the above mentioned data encryption algorithms will be evaluated when implementing in a single system with a maximum file size of 2547kb. How these data encryption algorithms affect the system resources and how they behave in the system will thoroughly be looked. The algorithm implementation and analysis of these data encryption algorithm will be the main focus. In addition to this, detailed explanation of these data encryption algorithms and their difference on the system will be discussed.

II. LITERATURESURVEY

A study in [19] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [20].

In paper [14] provided a performance comparison between symmetric key cryptography algorithms: DES, AES and Blowfish. The comparison had been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's speed for encryption and decryption. The paper also shows the analysis on the basis of two block cipher modes: ECB and CBC. Each algorithm is designed and executed in these two modes. The simulation setup was in java programming language. The results of this paper shows that blowfish has a better performance than other common encryption algorithms used. AES showed poor performance results compared to other algorithms since it requires more processing power.

In paper [17] provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. The author have used Pentium IV of 2.4 GHz CPU speed with 4 GB RAM. In the experiment have used text files sizes range from 50 KB to 22300 KB. The performance metrics are analyzed by the following: Encryption/decryption time, CPU process time – in the form of throughput, and Power consumption. The author results show the superiority of Blowfish algorithm in terms of the throughput, processing time and power consumption. More the throughput, more the speed of the algorithm & less will be the power consumption. Again, AES has advantage over the 3DES and DES in terms of throughput and power consumption except Blowfish. 3DES has least performance because of its triple phase encryption characteristics. Finally the author concludes that Blowfish is the best of all.

In the paper [23] conducted a comparative analysis for the performance evaluation of symmetric and asymmetric encryption algorithms i.e. AES, DES and RSA in term of computation time, memory usage and output bytes on different file sizes. The result of their experiments showed that DES algorithm performed better among others in term of encryption time, AES has least memory usage and RSA algorithm generated least output file. In paper[15] compared the performance of RSA and NTRU asymmetric algorithms on variable text file sizes with the key size of 51 bits and 20 bits for encryption and decryption process respectively. They concluded that NTRU performed better in term of encryption, decryption and authentication than RSA. Vijayalakshmi et.al. compared the performance of RSA and Elliptic Curve. Cryptosystem (ECC) asymmetric algorithms over execution time and memory size for encryption and decryption process with variable word lengths and different key sizes. Their results showed the superiority of ECC over RSA in term of execution time and memory requirement [18].

It was identified from [21], [24] that AES operates faster and more efficient than other symmetric encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. The difference is not noticeable. Reducing the number of rounds leads to power savings but it makes the protocol in secure for AES and should be avoided. Seven or more round scan be considered fairly secure and could be used to save energy in some cases.

A study in [25] is conduct for performance comparison between four of the most common encryption algorithms: DES, 3DES, Blowfish and AES. The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. Simulation has been conducted using C# language.

A study in [22] provides a fair comparison between three most common symmetric key cryptography algorithms: AES, Two-fish, CAST-256 and Blowfish. The comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used; the author main concern here is to study the performance of algorithms under different settings. The comparison is made on the basis of these parameters: speed, block size, and key size.

III. PERFORMANCE METRIC AND SIMULATIONENVIRONMENT

Performance metric

The performance of any system needs to be evaluated on certain criteria, these criteria then decide on the basis of performance of any system. Such parameters are known as performance metrics. The four types of performance metrics used to evaluate the performance of encryption and decryption algorithm in this paper are described below:

Encryption Time

Encryption time is yet another an important issue because it is basically used to calculate the throughput of an encryption scheme as well as it indicates its speed. The encryption time can be define as the time that an encryption algorithm takes to produce a cipher text from a plaintext .The throughput of the encryption scheme can be calculated as the total plaintext in bytes encrypted divided by the encryption time.

Decryption time

The decryption time is the inverses of encryption time that can be define as the time that a decryption algorithm takes to produce a plaintext from a cipher text.

Throughput

The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in.

Memory usage

This is the amount of memory consumed when the encryption and decryption process.

Simulation Environment

The two computer that is used to support the simulation described in this paper are Laptops with Intel core i3 CPU @ 2.40GHZ, 4GB RAM Processor and Windows 7 ultimate (32- Bit) and Intel core i3 CPU @ 2.53GHZ, 2GB RAM Processor and Windows 8 ultimate (32-Bit) are used in which the performance data are collected. In this experiment the text file size that has been taking to encryption range290Kb to 2.54Mb. The performance analysis of encryption and decryption algorithm has been simulated with JDK jdk1.7.0_45 with NetBeans IDE 7.4. Several simulations with different text size were done to examine the performance of encryption algorithms.

The simulation uses the provided classes in java environment to simulate the performance of DES, AES Triple DES and Blowfish. The implementation uses managed wrappers for DES, AES and Blowfish available in java.cypto and java.security [CryptoSpec] that wraps unmanaged implementations available in JCE (Java Cryptography Extension) & JCA (Java Cryptography Architecture). The Cipher class provides the functionality of a cryptographic cipher used for encryption and decryption. It forms the core of the JCE framework.

Today the opinion that Java is not the language to be used for cryptographic applications still seems to be popular. Obviously we do not agree. While Java is of course slower than C the difference is typically less than a factor of two, heavily optimized C code excluded, as demonstrated by the results presented in this paper. Although this difference is of course significant Java on today's hardware is faster than C on two year old hardware. The point being that while Java will hardly be the language of choice for high load servers it may well is the choice for medium load servers and especially clients. Add to that handheld and other small devices and performance in Java becomes an issue. One particular advantage of Java is that there is a well-established standard cryptographic API, the JCA and JCE architecture from Javasoft. The success of cryptography libraries in Java including the libraries from the IAIK confirms this position [32].

Measure CPU Time and Memory

NetBeans IDE includes a powerful profiling tool that can provide important information about the runtime behavior of your application. The NetBeans profiling tool easily enables you to monitor thread states, CPU performance, and memory usage of your application from within the IDE, and imposes relatively low overhead. Netbeans ide profile obtains the following profiling results: Runtime behavior of an application, CPU time used by an application's methods, Objectcreation[33].

Analyzing CPU Performance

When you choose the CPU task, the IDE profiles the method-level CPU performance (execution time) of your application and processes the results in real-time. You can choose to analyze the performance by periodically taking a stack trace or by instrumenting the methods in the application. You can choose to instrument all the methods or limit the instrumentation to a part of the application code, even down to a specific code fragment.

Analyzing Memory Usage

The Analyze Memory Usage task gives you data on objects that have been allocated in the target application such as the number, type and location of the allocated objects.
Java packages those are necessary for cryptography

Procedure for Simulation

Study the Algorithm

Before starting the simulation it very crucial to study the encryption algorithms how they work. As stated on the above the author trying to understand how they work from different book and research papers.

Write java program for encryption and decryption algorithm

In comparing the encryption algorithm it necessary to implement the algorithm by using java program. For this paper the author write a java program to encryption algorithms (DES, AES, Triple DES, and Blowfish).The program has three parts: key generation, encryption and decryption.

Measure the Performance Metrics

Measure the encryption time, decryption time and memory usage by using Netbean profile and java methods for all text sizes (range from290Kb-2.487Mb).

Calculate the throughput

The throughput is calculated from the file size and the time it takes to processing encryption or decryption. This is repeated for all file sizes.

Throughput = file size/encryption time

Gather Results

We collected all the results, stores in excel table, and lastly draw the graph.

IV. RESULTS ANDDISCUSSIONS

A. Encryption Time

Encryption time in pc1 and pc2 are based on the encryption time of the algorithms with different file sizes which both show the same trend. From figure 1, it can be observed that the encryption time is high for Triple DES when compared to others, especially when the file size is increased the change is rapid. As the file size increases the encryption time also increases. In both figures it shows that the Blowfish and AES have similar trends, in addition to that they take less time to encrypt the plain text.

B. Decryption time

A decryption time result of pc1 is shown on figure 2. The output on pc2 shows a similar trend. These results are based on the decryption time of the algorithms with different file sizes. The results are comparable to the encryption time result. So it can be observed that the decryption time is high for Triple DES as compared to others, especially when the file size is increased the change is rapid. As the file size increases the decryption time also increases. In both figures it shows that the Blowfish and AES have similar trends, in addition to that they take less time to decrypt the plain text.

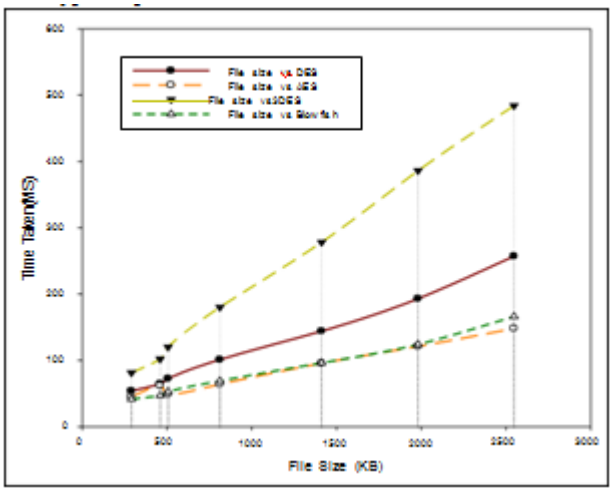

Fig. 1 PC1 Encryption Time

C. Encryption Throughput

The throughput of the encryption scheme is calculated using the following formula:

$$\text{Throughput} = \frac{\text{plain text size}}{\text{encryption time}}$$

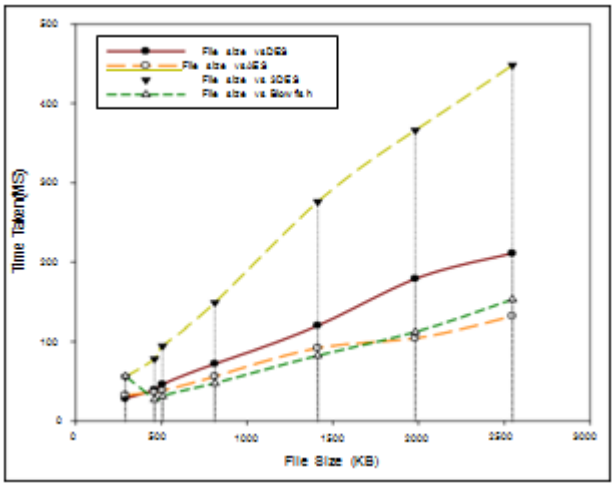

Fig. 2 PC1 Decryption Time

Calculating the throughput time for the encryption algorithm is required to determine the performance of the algorithm. Figure 3 shows the Encryption throughput in pc2, it can be observed that the Triple DES has the lowest throughput which pc1 also revealed the same trend; while the Blowfish and AES have similar result in addition to that they have the highest throughput.

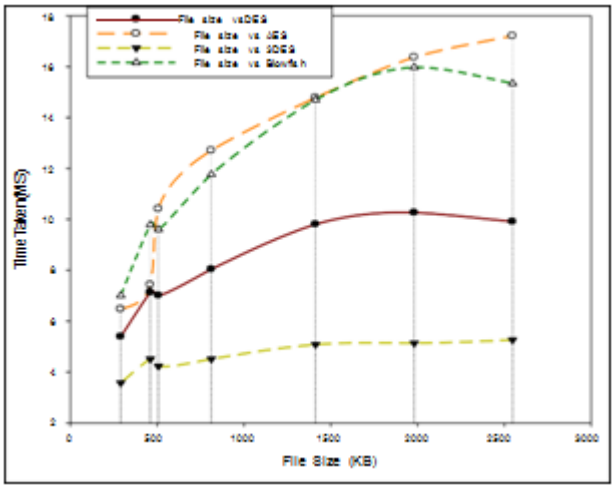

Fig. 3 Encryption Throughput in PC2

D. Decryption Throughput

The throughput of the decryption scheme is calculated by dividing the total cipher text in Megabytes decrypted on the total decryption time in each algorithm. These results as shown in figure 4 are similar to the result of encryption throughput. The results show that Triple DES has the lowest throughput; while the Blowfish and AES have similar result in addition to that they have the highest throughput.

E. Encryption Memory Usage

Encryption memory usage in pc1 and pc2 results is based on the memory usage of the algorithms with different file sizes which shows the same trends. From figure 5, it can be observed that DES and Triple DES have used similar memory size, while Blowfish is used smaller memory than DES and Triple DES till it the file size of 1421, in this situation AES has used smallest memory compared to other algorithm. After file size of 1421 onwards the three algorthims i.e. Blowfish, DES and Triple DES have used similar memory, which is smaller compared to AES's.

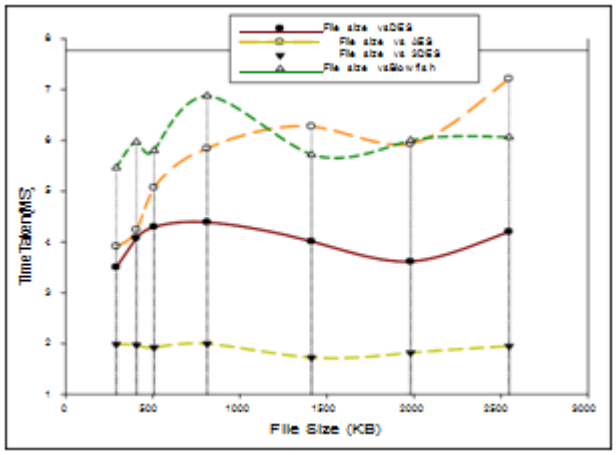

Fig. 4 Decryption Throughput in PC1

F. Decryption Memory Usage

Decryption memory usage in pc1 and pc2 results is based on the memory usage of the algorithms with different file sizes which both shows similar trend. From figures 6, it can be observed that DES and Triple DES have used similar memory size in addition to this they used the smallest memory, while in both figures the AES has used larger memory as compared to others.

V. CONCLUSION

This paper compares four cryptographic algorithms those are DES, AES, Triple DES, and Blowfish, implemented in the powerful portable programming language Java and JCA (Java Cryptography Architecture) which are used in implementing the encryption algorithms, under different scenario- with different file sizes. To measure the performance of four cryptographic algorithms, the results are compared and necessary conclusion sare made. The paper has concluded on the basis of the performance offered by cryptographic algorithms performances metric considered.

From the result on this paper it can be concluded that Triple DES needed more time to encrypt/decrypt, used less memory, and has low throughput. AES and Blowfish has similar time to encrypt/decrypt and better throughput, but AES need more memory than blowfish, in addition DES needs similar memory to Triple DES, but it took minimum time to encrypt/decrypt and higher throughput than Triple DES.

As obtained from the results, Blowfish encryption/decryption algorithm has better performance relative to the rest algorithms. The result may be altered for file size greater than 2547kb.

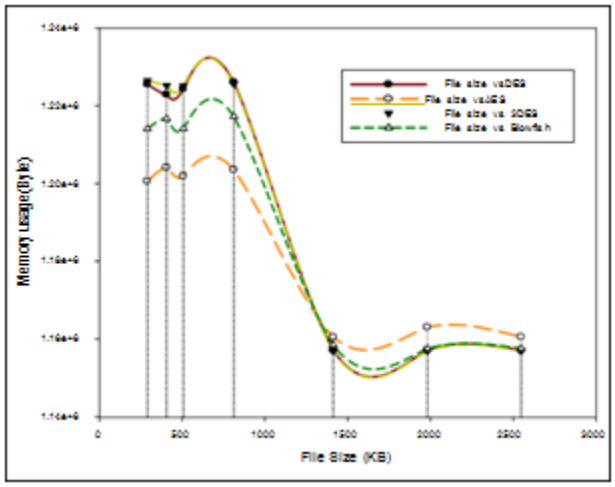

Fig. 5 Encryption Memory Usage in PC1

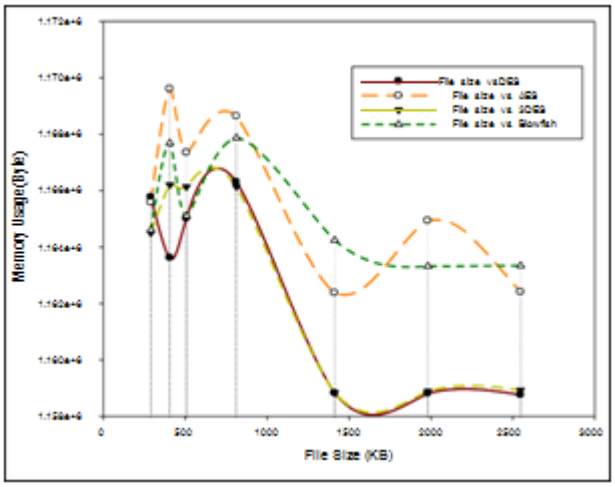

Fig. 6 Decryption Memory Usage in PC1

REFERENCES

[1] Ali Makhmali, Hajar Mat Jani "Comparative Study On Encryption Algorithms And Proposing A Data Management Structure" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2,2012

[2] Amandeep Singh, Manu Bansal "FPGA Implementation of Optimized DES Encryption Algorithm" I. J. Computer Network and Information Security, 2012

[3] Apoorva, Yogesh ,Kumar "Comparative Study of Different Symmetric Key Cryptography Algorithms" International Journal of Network Security &Its Applications (IJNSA), Vol.1, No 1,2013

[4] Arjen K. Lenstra Citibank, and Eric R. Verheul "Selecting Cryptographic Key Sizes" jornal of cryptology Research volume 10.1007=s00145-001- 0009-4,2006.

[5] Ayushisonipat, Haryana "A Symmetric Key Cryptographic Algorithm" International Journal of Electronics and Computer Science Engineering, 2010

[6] BRUCE SCHNEIER applied cryptography, secondedition,
[7] Dhawan “Choices - Building Distributed Applications with.NET,"Microsoft Developer Network, 2002.(http://msdn.microsoft.com/library/default.asp).
[8] Fundamentals of Computer Security, Springer publications “Basic Cryptographic Algorithms”, an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms
[9] Ghesmati, S., M. Sate, and A. Asosheh. A 2-level model for e-commerce Security in Internet Security (WorldCIS), 2011 World Congresson.
[10] G. RAMESH1 Dr. R. UMARANI2 “Performance Analysis of Most Common Symmetrical Encryption Algorithms” International Journal ofPower Control Signal and Computation(IJPCSC) ISSN: 0976-268X Vol3. No1. 2012
[11] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani “New Comparative Study Between DES, 3DES and AESwithin NineFactors”
[12] International Journal of Scientific & Technology Research Volume 2, Issue 6,2013
[13] He, Y. and J. Jiang. E-commerce security payment system research and implementation.inComputer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conferenceon.
[14] K. McKay, "Trade-offs Between Energy and Security in Wireless Networks; Thesis, Worcester Polytechnic Institute,2005.
[15] Nagesh Kumar, Jawahar Thakur, ArvindKalia “Performance Analysis Of Symmetric Key Cryptography Algorithms: DES, AES and BLOWFISH” International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 1, Issue 2,2011
[16] NarasimhamChalla and JayaramPradhan, “Performance Analysis of Public key Cryptographic Systems RSA and NTRU”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.8,2007
[17] Maqableh, Mahmoud,Mohammad “Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce”, Durham theses, Durham University. Available at DurhamE-Theses Online:http://etheses.dur.ac.uk/738/
[18] Pratap Chandra Mandal “Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish” International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 5, 2012, pp.914-917
[19] P.R.Vijayalakshmi, K. Bommanna Raja, Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol, International Conference on Computing, Communication and Applications (ICCCA),2012,
[20] "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, ICICT 2005 First International Conference proceedings report, 2006. PP. 84-89..
[21] Results of comparing tens of encryption algorithms using different settings- Crypto++
[22] Benchmark-Retrieved,2013. (http://www.eskimo.com/~weidai/ benchmarks. html)
[23] R. Chandramouli, "Battery power-aware encryption - ACM Transactionson Information and System Security (TISSEC)," Volume 9 , Issue2 ,May.2006.
[24] Rohtak, Harayana, Yogesh Kumar “Comparative Study of Different Symmetric Key Cryptography Algorithms” International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 7,2013
[25] ShashiMehrotra Seth, Rajan Mishra, Comparative Analysis Of Encryption Algorithms For Data Communication, IJCST Vol. 2, Issue 2,2011
[26] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," universityof Pittsburgh, April 9, 2003. Retrieved,2008,
[27] SimarPreet Singh, and Raman Maini “Comparison of data encryption algorithms” International Journal of Computer Science and Communication, 2011.Vol. 2, No. 1, pp.125-127,
[28] Sombir Singh* Sunil K. MaakarDr.SudeshKumar “Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques” JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, 2010, ISSN 2151-9617
[29] William stalling “cryptography and network security: principles and practice, fifth edition, 2006.