ANALYSIS THE IMPACT OF SYMMETRIC CRYPTOGRAPHIC ALGORITHMS ON POWER CONSUMPTION FOR VARIOUS DATA TYPES

[1]Er. Rajender Singh, [2]Er.Rahul Misra, [3]Er.Vikas Kumar
[1, 2]*M.tech Scholar,* [3]*Asst. Professor*
[1]*rajendersinghk@gmail.com,* [2]*misra.rrahul@gmail.com*

Abstract: - **With the emergence of communication techniques as the human beings become advanced day by day these communication techniques also get some advancement or development day by day. After the emergence of internet the communication of data from one place to another is increasing day by day, because as we all know that internet is very fast mode of data transfer as compared to send your data through post with the help of post-office. As the data over the internet is increasing, it is very necessary that we must ensure to provide the best solution to offer the necessary protection against the data thefts & attacks. For that purpose we use many algorithms, and among these algorithms one of the best algorithms is Encryption algorithm, because it plays an important role in information security systems. But the main problems with such types of algorithms are that they consume a significant amount of computing resources such as CPU time, memory, and battery power. Power Consumption is not a big deal or big issue in case of wired environment but the computing resources in the wireless environment is limited and limited battery power available. As the technology advances it leads to a lot of changes in the processors and memory in the computers, by which they requires a lot of power, or in other words we can say that they needs power to boost up, but battery technology or battery backup technology is increasing at much slower rate, and this cause to forming a "battery gap". As it is like the heart of the electronic devices and as most of the equipment of electronics including computing devices and communication devices also requires a good battery backup. Today, as we all seen that Lap-tops, Palm-tops etc.are generally used instead of Desktop or PC and it is well known that all these are the wireless devices and for these devices the data communication also be wireless and on the contrary, the networking connection will also be wireless. From above as we seen, the increasing demand for services on wireless devices has pushed towards us into an important research which finding ways to overcome these limitation. The paper which I present of the behalf of thesis evaluate or analyze the six most common encryption algorithms namely AES (Rigndael), DES, 3DES, RC2, Blowfish and RC5. Now I'll try my best to find out the method to analyze the trade-offs between energy and security. There are different approaches used to reduce the energy consumption of security protocols. A comparative study also I planned to be conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed.**

Keywords: **- 3DES, AES, Blowfish, Computer Security, DES, Encryption Techniques, RC2, RC5**

*****

I. INTRODUCTION

Before move on further to discuss more about power consumption, let's first we take a review of encryption algorithms because encryption algorithms and encryption techniques plays an important role in information security. These encryption algorithms and the techniques of encryption which we used for the security purposes, uses symmetric and asymmetric encryption scheme.

Symmetric key encryption scheme or secret key encryption scheme has the following five ingredients:-

1) **Plain text:-**This is the original intelligible message or data is fed into the algorithm as input.
2) **Encryption algorithm:-**The encryption algorithm performs various substitutions and transformations on the plaintext.
3) **Secret key: -** The secret key is also input to the encryption algorithm .The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time .the exact substitutions and transformations performed by the algorithm depend on the key.
4) **Cipher text:-**This is the scrambled message produced as output .It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands is unintelligible.
5) **Decryption Algorithm: -** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

Asymmetric Mechanism: - In asymmetric mechanism 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 signature).But the main problem with public key encryption is that; that it is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices. Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques because they require more computational processing power.

A Public Key encryption scheme has:-**Plain text, Encryption Algorithm, Public and Private Key, Cipher text, Decryption Algorithm**.

This is clear from the following postulates that there are so many cryptography algorithms for conventional encryption scheme and asymmetric encryption scheme for e.g. such as RC2, DES, 3DES, RC5, Blowfish and AES. All these encryptions techniques with their brief description are discussed below:-

1) **DES**: - The most widely used encryption scheme is based on the data encryption standard (DES) adopted in 1977 by the National Bureau of Standards and Technology (NIST) as federal information processing standard 46(FIPS PUB 46)[15].The algorithm itself is referred to as the data encryption algorithm(DEA).For DES,data are encrypted in 64-bit blocks using a 56-bit key .The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used to reverse the encryption .Since at that time many of the authors said that due to severe attacks recorded the weaknesses of DES, which made it an insecure block cipher.

2) **3DES**:- The potential vulnerability of DES to a brute-force attack, there has been considerable interest in finding an alternative. One approach is to design a completely new algorithm and another alternative, which would preserve the existing investment in software and equipment, is to use multiple encryptions with DES and multiple keys. This multiple key approach is the 3DES or triple DES approach .This approach is an enhancement of simple DES; it is 64 bit block size with 192 bits key size. In this standard 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. It is a known fact that 3 DES is slower than other block cipher methods [15].

3) **RC2:-** RC2 is a block cipher with 64 bits block cipher with a variable key size that bit block can be used as a replacement for the DES algorithm ranges from 8 to 128 bits; RC2 is vulnerable to a related key attack using 234 chosen plaintexts[15].

4) **Blowfish: -** Blowfish is a symmetric block cipher developed by Bruce Schneider [SCHN93, SCHN94]. Blowfish was designed to have the following characteristics: [15]

- Fast:-Blowfish encrypts data on 32-bit microprocessors at a rate of 18 clock cycles per byte.
- Compact: - Blowfish can run in less than 5K of memory.
- Simple:- Blowfish's simple structure is easy to implement and eases the task of determining the strength of algorithm.
- Variably Secure: - The key length is variable and can be as long as 448 bits. This allows a tradeoff between higher speed and higher security.

Blowfish encrypts 64-bit blocks of plaintexts into 64-bit blocks of cipher text. Blowfish is implemented in numerous products and has received a fair amount of scrutiny. So far, the security of Blowfish is unchallenged .Blowfish makes use of a key that ranges from 32 bits to 448 bits (one to fourteen 32- bit words).That key is used to generate 18 32-bit sub keys and four 8*32 S-boxes containing a total of 1024 32-bit entries .The total is 1042 32-bit values, or 4168 bytes.

5) **AES :-** The Advanced Encryption Standard(AES) was published by NIST (National Institute of Standards and Technology) in 2001.AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications .Besides this, its security mechanism and security strength is equal to better than 3DES and significantly improved efficiency .The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128,192 or 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits [15].

RC6:- RC6 was designed to meet the requirement of AES competition and it is advanced version of RC5 which is not a big issue to described over here .RC6 has data block size of 128 bits and key mechanism which is supported by RC6 are varying from 128-256 bytes .The most common three sizes which we take in RC6 are 128,192 and 256 bits[15].

The papers which we present our total emphasis on examine methods to evaluate or analyze the performance of various cryptographic algorithms on power consumption in which we not only concern on time but on other factor also such as CPU time, memory and battery power. We are examine some methods for analyzing trade-offs between energy and security .The goal is to aid the design of energy efficient secure communication schemes for the wireless environment in the future. For this purpose we are using three approaches:-

1) To reduce the high energy consumption of security protocols: for this first we replace high standard security protocol primitives that consume high energy while maintaining the same security level.
2) Secondly modification of standard security protocols appropriately.
3) Finally a totally new design of security protocol where energy efficiency is our main focus or main motto.

For this purpose we evaluate different encryption algorithms namely: - DES, 3DES, RC2, RC6,Blowfish,AES.The performance of these algorithms can be measured in terms of energy , changing of data types – such as text or document, Audio Data, Video Data and Pictures Data – Power Consumption changing packet size and changing key size for the selected cryptographic algorithms.

II. RELATED WORK

Studies shows that [5] the different popular secret algorithms such as DES, 3DES, AES, Blowfish etc. were implemented and their performance was compared by encrypting input files of varying contents and sizes. The results showed that blowfish had a very good performance compared to other algorithms. It was also concluded from [6] that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric schemes as well as study in [5] also concluded that AES had 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 more than DES to process the same amount of data.

Some postulates and theories are given on different popular secret key algorithms such as RC4, AES and XOR in [7] and on the basis of that they were implemented and their performance was compared by encrypting not text this time but encrypting a "Real Time Video Streaming "of varying contents. The results of encrypting "Real Time Video Streaming" proves that encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm.Therfore,AES is a feasible solution to secure real time Video transmission.

In order to measure the security level for a web programming language a study has been proposed in[10] to analyze or measuring the performances of encryption process at the programming language's script with the web browsers.

Studies conducted in[9] shows that the energy consumption or power consumption of different symmetric key encryptions on hand held devices and it proves that after only 600 encryptions of some MB file say 5 MB file using Triple DES the remaining battery power is 45% and rest of the encryptions or subsequent encryptions are not possible as the battery dies rapidly.

In [11] Crypto++library is a free c++ class library of cryptographic schemes .It evaluates the most the most commonly used cryptographic algorithms .It is also shown that Blowfish and AES have the best performance among others And both of them i.e. Blowfish and AES have better encryption (i.e. stronger against data attacks) than other two i.e. Triple DES and DES.

III. EXPERIMENTAL DESIGN

For our experiment we are collecting the following performance metrics that are given below:-
1. Power Consumption
2. Encryption Time
3. CPU Process Time
4. CPU Clock Cycles.

Besides these four our experiment we use wireless devices such as laptop with 1.5 GHZ CPU, in which performance data is collected .In our experiment we use laptop which is used for encryption which encrypts a file range from 321 KB to somewhat near around 7 or close to 8 MB .We take 139 megabytes for text data and data from 4006 KB to 5073 KB for video files

1) **Power consumption: -** As we all know that energy measured in joule and power in watts or may be power measured in joule/sec but here the question is not that, that in which unit energy or power is measured but here the question is how to calculate how much power or energy is consume during encryption. For this purpose we are using the techniques that are described in[12].We present a basic cost of encryption which is represented by the product of total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The encryption cost is calculated in the unit of ampere-cycle. To calculate how much energy is consumed during this whole process of encryption we divide the ampere-cycle by the clock frequency in cycles per second of a processor; we obtain the energy cost or energy consumption of encryption in ampere –seconds. Then we can easily calculate the energy cost or energy consumption or power consumption by simply multiply the ampere seconds with processor's operating voltage, and we obtain the energy consumption or cost in joule.

With the help of these cycles such as CPU clock cycle (the operating voltage count by the CPU) and the average current drawn for each cycle (ampere-cycle) we can easily calculate the energy consumption of cryptographic functions. For calculation of energy consumption by a any program (P) to achieve its goal of encryption or decryption is given by E=VccxIxT joules [12] and Vcc is fixed for every individual CPU and the hardware which is available to us.

2) **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 ciphertext from a plaintext .The throughput of the encryption scheme can be calculated as the total plaintext in bytes encrypted divided by the encryption time[14].

3**) CPU Process Time: -** This time reflects the load of the CPU and this load depends on the CPU time used in the encryption process, the more time the CPU will consume in the encryption process, the higher will be the load of the CPU and it is important to notice that; it is concern only in some particular process of calculations.

4) **CPU Clock Cycles:-** CPU clock cycles is one of the major concern of our paper because it reflects the energy consumption or power consumption of the CPU while operating an encryption standard and it is assumed that each CPU clock cycle will consume a small amount of energy or power.

The following major tasks or operations that we performed to analyze the power consumption and the security aspects are as follows:-

(**a**)A comparative study is conducted on the basis of results of the various kinds of encryption and decryption schemes in terms of the encryption time, battery power and throughput.

(**b**)A study is performed on the effect of changing packet size on power consumption, throughput and CPU work load for each cryptography algorithm.

(**c**)Another factor on which our power consumption is remarkable be effected is changing of data types such as text or document, Video Files for each cryptography selected algorithms.

IV. SIMULATION RESULTS

4.1) The Effect of changing packet size for Cryptographic algorithm on Power Consumption (doc or text files).

4.1.1) Packets Encryption with varying size:-

1) CPU Work Load:- The following figure illustrates or examines the performance of various cryptographic algorithms on the basis of CPU load sharing by various encryption processes having different data block size.

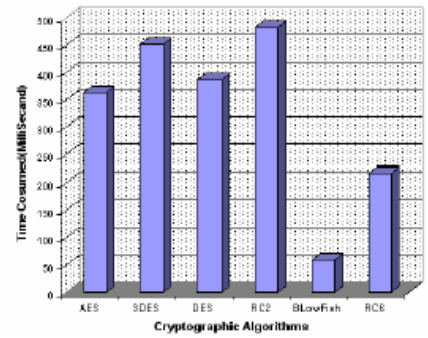

Fig-(A):- Time Consumption for encryption of different text and document data without data transmission (milliseconds)

2) Encryption Throughput:-Encryption throughput and power consumption are inversely proportional to each other. As the encryption throughput value is increased the power consumption of the following encryption is decreased and this "encryption throughput "can be evaluated by dividing the total plaintext in megabytes encrypted on the total encryption time for each algorithm which is ready for encryption or in the process of encryption or encrypted. This can be illustrated from the following fig (B):-

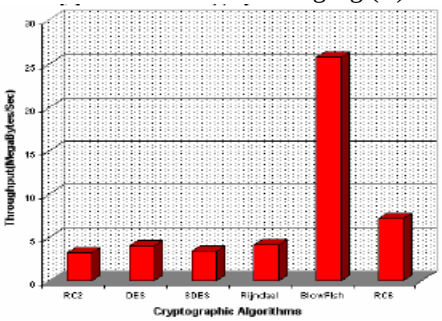

Fig-(B):- Throughput of each encryption algorithm to encrypt different text data or document data in (MB/sec)

3) Power Consumption:-From the given figure we can analyze the performance of different cryptographic algorithms in terms of power consumption for encryption for encryption process with varying data block size. The results from this figure proves that the best encryption algorithm is the **Blowfish** algorithm in terms of power consumption but not only in terms of power consumption; it proves to be the best when we consider the other factors also such as processing time and throughput this is clear from the given

Fig (A) and fig (B) as shown above. Now consider an example in which we encrypt a text or document by using Blowfish and AES we found that Blowfish consumes very less power near about 16% of the power which is consumed for AES.

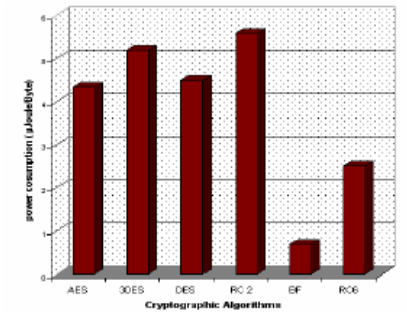

Fig (C):- Power consumption during encryption of different text data or documents measured in micro joule/byte.

4.1.1) Packets Decryption with varying size:-

1) CPU Work Load:-This doesn't require much explanation; decrypted text with CPU work load will analyze with the help of following fig:-

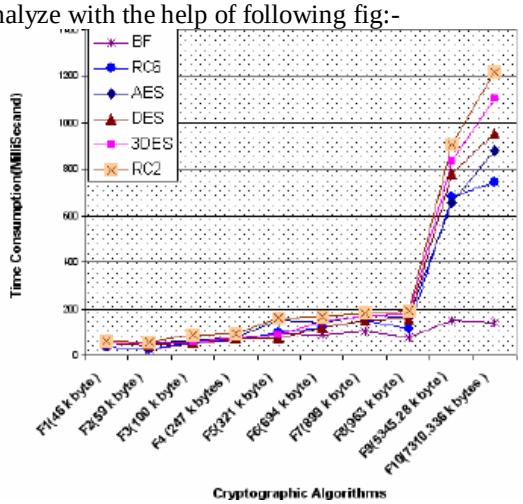

Fig-(D) - Time Consumption for decryption of different text and document data without data transmission (milliseconds)

2) Decryption Throughput:-This is clear from the encryption process that throughput is calculated in terms of megabytes /second and as we know that every encrypted text should be decrypted and during decryption three major points we concern i.e. CPU work load, throughput and power consumption in which throughput plays a important role because it deals with the performance of following algorithms which is used for decryption.

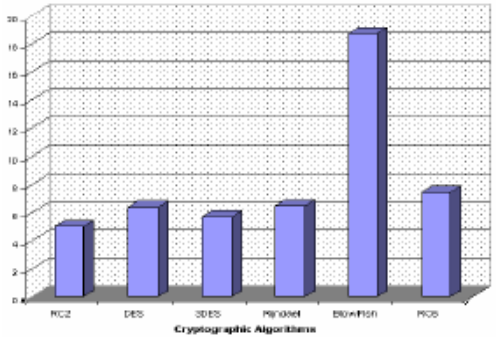

Fig-(E) - Throughput of each decryption algorithm to encrypt different text data or document data in (MB/sec)

3) Power Consumption:- Power consumption for decrypted text or decrypted documents in micro-joule/byte and to determine which algorithm consume how much power is shown below

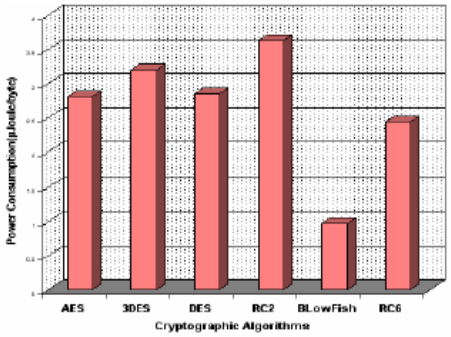

Fig (F):- Power consumption during decryption of different text data or documents measured in micro joule/byte.

4.2) The Effect of changing File type (Video files) for Cryptographic algorithm on Power Consumption.

4.2.1) Encryption of Different Video files

1) **CPU Work Load:-**It is measured in terms of milliseconds and the following figure analyze the performance of cryptographic algorithms in terms of sharing the CPU load with varying video block size.

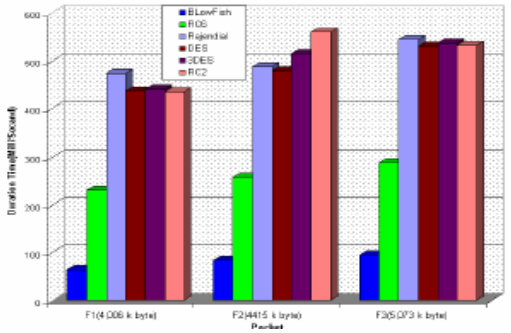

Fig-(F):-Time Consumption for encrypting different video files

2) Encryption Throughput:- In order to measure the performance of different algorithms for various video files can be identified with the help of following figure as shown below:-

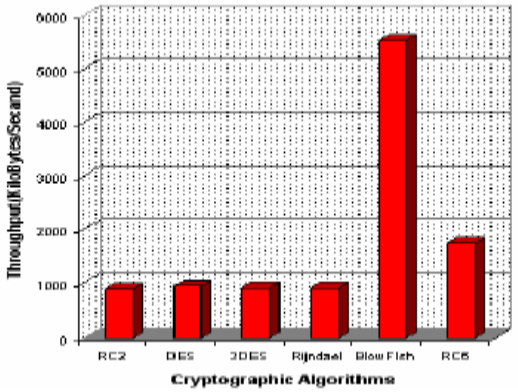

Fig-(G):-Throughput of each encryption algorithm

3) **Power Consumption:-**The result of power consumption for video files shows the same result as we measured result in text data and from that we conclude that Blowfish is the superior algorithm among all the algorithms because during encryption of video file with Blowfish and AES we found Blowfish requires approximately16% of power consumed in AES [16].When we encrypt data using RC6 and AES we found AES consume 50% more power than RC6.Finally we conclude that RC2 has low performance and low throughput than all other algorithms.

4.2.2) Decryption of Different Video file

1)CPUWorkLoad:-

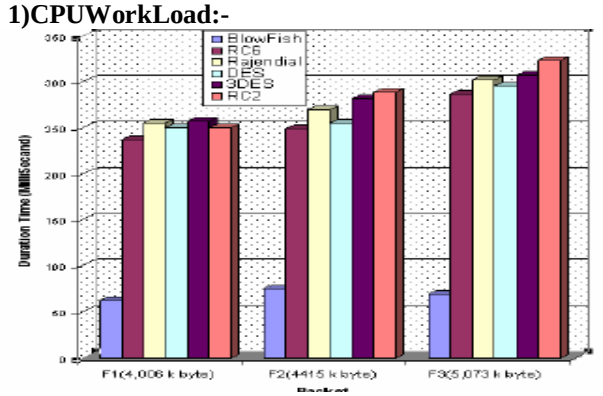

Fig – (H) Time Consumption for decrypting different video files

2)DecryptionThroughput:-

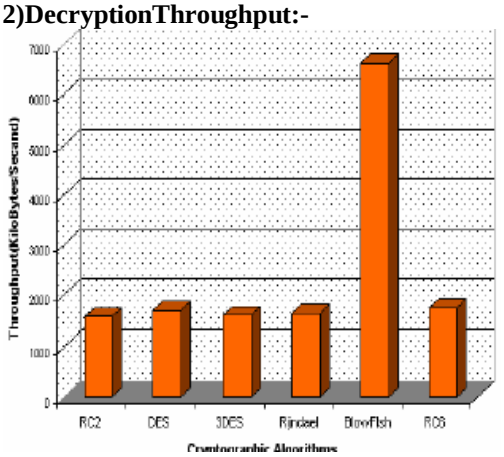

Fig-(I):- Throughput of each encryption algorithm (KB/sec)

3) **Power Consumption:-**

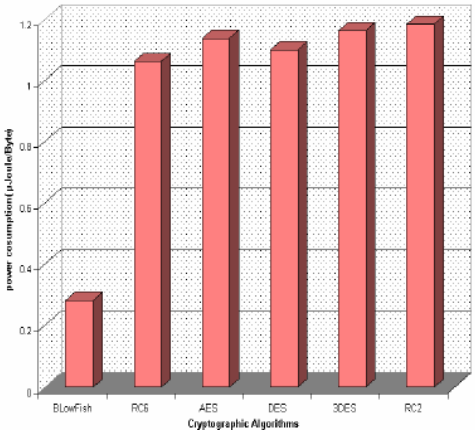

Fig-(J):- Power Consumption for decrypt different video files in micro- joule/byte

With the help of the graphs of encryption and decryption we found that the results is same as in the encryption process for video files and text data .During decryption process and when we decrypt the data using Blowfish and AES we found that Blowfish requires approximately 24% power which is consumed for AES[16] and when we decrypt data using RC6 and AES we found that RC6 approximately 93% of the power which we consumed for AES.

V. CONCLUSION AND FUTURE RESEARCH

This paper presents a performance evaluation of different symmetric algorithms .The selected algorithms are AES,DES, 3DES,RC6,Blowfish and RC2.Several points can be conclude from the simulation results and it is found that Blowfish provides the best performance among all algorithms then after that the best algorithm which consumes less power and less time is RC6 and the worst approach among all the algorithms in terms of CPU load is RC2 because it leads to heavy workload of CPU as it is very time consuming factor. In future the same approach we apply on audio files and images and as well as suggest three approach to reduce energy consumption or power consumption on security protocols and apply it to (WLAN's) to provide energy efficient schema for 802.11WLANS and as well as tried our best to replace all standard security protocol primitives that consumes high energy while maintaining the same security level. Finally we will conclude a new design of security protocol where energy is our main concern or main focus

.REFERENCES

[1]J Daeman and V.Rijmen. AES proposal: Rijndael, National Institute of Standards and Technology.

[2]R.Chandramouli,"Battery Power aware encryption,"ACM transactions on information and system security (TISSEC), vol 9 no 2 pp.162-180

[3]J.Daeman and V.Rijmen," Rijndael: The Advance Encryption Standard" Dr. Dobb's Journal pp.137-139

[4]D.Coppersmith,"The Data Encryption Standard (DES) and its strength against attacks,"IBM Journal of Research and development pp.243-250.

[5]A.Nadeem and M.Y.Javed,"A performance comparison of data encryption algorithms," Information and communication technologies2005, pp-84-89

[6]S.Hirani, EnergyConsumption of encryption schemes in wireless devices thesis.

[7]W.S Elkilani and H.M. Abdul –Kader,"Performance of encryption techniques for real time Video streaming"IBIMA Conference pp-1846-1850

[8]N.El.Fishawy,"Quality of Encryption measurement of bitmap images with RC6, MRC6 and Rijndael block cipher algorithms," International Journal of Network Security pp-241-251

[9]N.Ruangchaijatupon & P.Krishnamurthy," Encryption and power consumption in wireless LAN's"The Third IEEE workshop on Wireless LANs pp.148-152.

[10]S.Z.S. Idrus, S.A Aljunid and S.M. Asi,"Performance analysis of encryption algorithms text length size on web browsers".

[11]http://www.eskimo.com/weidai/benchmark.html.

[12]K.Naik and D.S.L Wei,"Software implementation Strategies for power conscious systems" Mobile Networks and Applications vol-6 pp no-291-305.

[13]A.Sinha and A.P Chandrakasan,"Joule Track –A Web based tool for software energy profiling"

[14]A.A.Tamini Performance Analysis of data encryption algorithms ;(http://www.cs.wust1.edu/jain/cse56706/ftp/encryption-perf/index.html).

[15] W.Stallings ,Cryptography & Network Security 4th edition p.p. 58-309,Prentice Hall,2005

[16]B.Scheneier, The Blowfish Encryption & decryption Algo