International Conference on Emerging Trends in Engineering, Science and Management
Sphoorthy Engineering College, Hyderabad, India (ESM-17)
17th and 18th March 2017 , www.conferenceworld.in ISBN: 978-93-86171-32-0

METRICS FOR PERFORMANCE EVALUATION OF ENCRYPTION ALGORITHMS

Mr.B.Bharathi[1], Mr.G.Manivasagam[2], Dr.M.Anand Kumar[3]

[1,2]Research Scholar, Department of Computer Science,
Karapagam University, Coimbatore,Tamilnadu, (India)
[3]Associate Professor, Department of Information Technology,
Karapagam University, Coimbatore, Tamilnadu, (India)

ABSTRACT

Network and internet applications are growing rapidly in the recent past. These applications are used by thousands of users and controlled by different administrative entities. It is mainly used as an efficient means for communication, entertainment and education. With the rapid growth of internet, there is a need for protecting confidential data. The Internet was however originally designed for research and educational purpose, not for commercial applications. So internet was not designed with security in mind. As the internet grows the existing security framework was not adequate for modern day applications. Cryptography plays a vital role in network security. Though, many cryptographic algorithms are implemented by the research community all over the world. But all the algorithms had some limitations such as the algorithms are implemented for specific applications, key size or block size limited to 64,128 and 256 bits. This paper presents various evaluation techniques and performance metrics that can be used to test any cryptographic algorithms. This work will be base for further research work especially in implementing new encryption algorithms.

Keywords*: *Cryptography, Blowfish, Encryption, Metrics, Performance, Idea

I. INTRODUCTION

Communication networks and Internet had a tremendous growth in the recent past years. Today most of the government sectors, financial institutions, corporations, military and others exchange huge amount of confidential information by using the Internet [1]. With the rapid growth and usage of Internet for commercial purpose, protection of confidential information ensuring data integrity and data origin authenticity is very important. The Internet was however originally designed for research and educational purpose, not for commercial applications. The increase in the users of Internet, the existing security framework was found inadequate for modern day applications and software [2].

Cryptography is the science of using mathematics to encrypt and decrypt data. It provides a way to store sensitive information or transmit it to the insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient [3]. This technique is widely used to protect data that traverses over open and unsecured networks. Many cryptographic algorithms have been implemented by the research organizations all over the world. But all the algorithms had some limitations such as the algorithms are implemented for specific applications, key size or block size limited to 64,128 and 256 bits. Though many cryptographic algorithms

 ISBN: 978-93-86171-32-0
available in market, it is very difficult to select appropriate algorithm for specific real time applications [4]. There is a need for mathematical model to evaluate the performance of the encryption algorithms. This work presents several mathematical models for the performance analysis of cryptographic algorithms. This work also uses Blowfish and IDEA algorithms to execute the mathematical models to show the performance analysis.

1.1 Blowfish

Blowfish: Blowfish [5] is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, a key and data-dependent substitution. All operations are EX-ORs and additions on 32-bit words Blowfish is successor to Twofish [8]

1.2 IDEA

The IDEA [6] is a 64-bit block cryptographic algorithm which uses a 128-bit key. This key is the same for both encryption and decryption. The algorithm consists of nine phases: eight identical phases and a final transformation phase. The encryption takes place when the 64-bit block is propagated through each of the first eight phases in a serial way where the block divided into four 16-bit sub-blocks is modified using the six sub-keys corresponding to each phase six sub-keys per phase and four sub-keys for the last phase). When the output of the eighth phase is obtained the block goes through a last phase the transformation one, which uses the last four sub-keys. . In terms of energy of key setup and encryption, IDEA is on par with AES. IDEA is supposed to have very good cryptanalytic properties, thereby combining efficiency with acceptable security [7].

1.3 SF Block

SF Block cipher [9] is a 512 bit block cipher. This Block cipher is based on a design principle known as a Substitution permutation network (SP Network). The algorithm is designed based on Advanced Standard Encryption (AES) algorithm. It takes a block of the plaintext and the key as inputs, and applies several alternating rounds or layers of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the cipher text block. In the case of SF Block Cipher the block size is 512 bit and the key size is also 512 bit. Message block and key can be realized as a 4*16 matrix (4 rows and 16 columns.). For encrypting and decrypting a single block, the SF Block cipher algorithm applies its Functions in N Rounds. The working principle of the algorithm can be found in [9]

The rest of the paper is organized as follows. Analytical model is described in section II that is followed by Performance metrics in section III. In section IV Mathematical model was presented that can be applied for various algorithms. Section V Presents the Performance evaluations of Blowfish and IDEA and SF Block cipher and Section VI finally concludes the research work

II. ANALYTICAL MODEL

Analytical modeling, measurement and evaluation have been identified as the three main approaches commonly used for evaluating the communication networks systems [9]. The result of the evaluation is used to set the network performance indices given a traffic workload and network configuration. In this research work, the network performance is evaluated after applying the proposed security algorithm for the TCP/IP Protocol Suite.

An analytical modeling is nothing but the rough representation of the real life behavior of a system. It is sometimes referred to as a mathematical model. Such representation is done using a set of mathematical symbols. Analytical model is built, solved and validated using analytical process modeling. Analytical modeling is predetermined for simple systems to the extent that it simplifies any complicated systems as the case may be whenever a complex system is involved. Measuring performance of the proposed system is made real time where the prototype of the protocol is presented for the evaluation. This method requires a prototype of the system to be developed by the researcher and tested within a particular network environment usually within the simulated environment [10]. The performance of the prototype is tested both during and after executing the prototype. The following figure shows the evaluation techniques of any cryptographic algorithms [11].

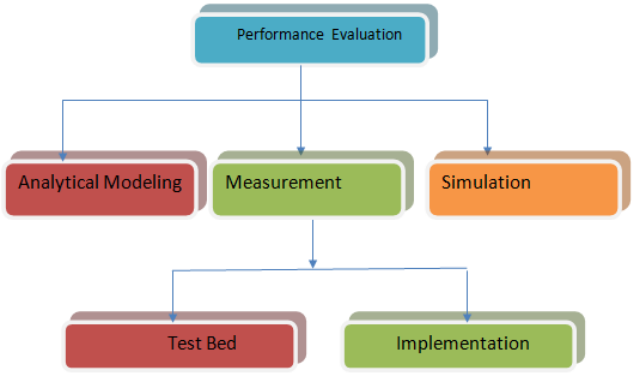

Fig. 1. Evaluation Technique

Computer simulation [10] is regarded as a technique used to examine a broad range of models presenting a kind of real-world systems using specific simulation application software primarily developed in order to imitate some basic features of the system. In the same manner, proposed simulation system involves the theory behind designing and executing a security model and finally analyzing the output using appropriate network simulation software. Such an approach supports easy modification of the design architecture by remodeling. The evaluation process is repeated each time and a modification is made until the desired level of performance is achieved.

III. PERFORMANCE METRICS

The setup for the proposed experiment is designed as two architectures such as wired architecture and wireless architecture. For wired architecture, Local Area Network (LAN) with eight Pentium IV systems is used as shown in the Figure 2. For wireless architecture two laptops are used in the experiment as shown in the Figure 3. The two laptops (sender and receiver) had windows XP professional installed on it.

The first laptop (sender) is connected to access point. In the experiments, the first laptop encrypts a different file size for different data types ranges from 321 Kilobytes to 7.139Megabytes for text data (.DOC files), from 33 Kbytes to 8,262 Kbytes for audio data (.WAV files), from 28 Kbytes to 131 Kbytes for pictures and Images

(.GIF and GPG files) using .NET environment, two commonly used encryption algorithm such as IDEA with different key sizes and Blowfish are selected and implemented.

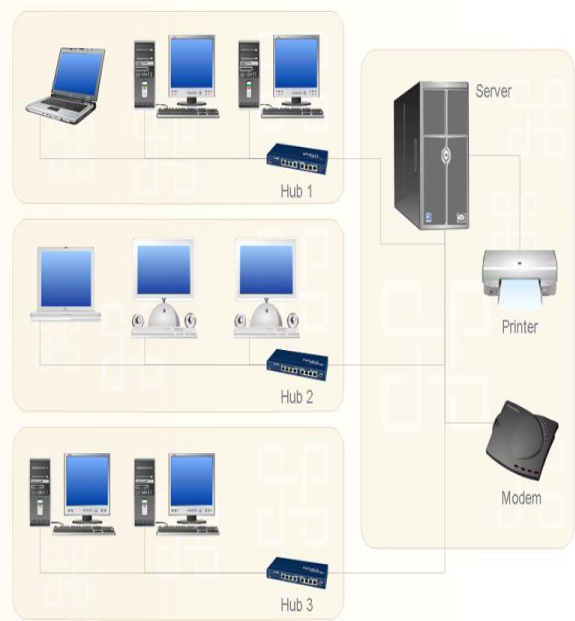

Fig. 2. Wired Architecture (Test Bed)

Fig 3. Wireless architecture (Test Bed)

These implementations are thoroughly tested and are optimized to give the maximum performance for each algorithm. The results are checked and tested for AES Rijndael that supposed to be the best encryption algorithms by a different implementations program to give the maximum performance for the algorithms and make sure the results are the same using multiple platforms. Then for transmission of data, the two laptops are connected wirelessly. Data is transmitted from the first laptop to the second one through the wireless link using TCP/IP protocol.

The experiment are applied in two mode of wireless LANs connection (BSS and ad hoc mode).Using IEEE 802.11 standard, data is transmitted using the two different types of authentication. First, data is transmitted

without using the proposed algorithm. Then the data was transmitted with the proposed algorithm[11]. The results are compared with different parameters. The hardware specifications for the above mention architecture are as follows.

Performance is evaluated for the proposed algorithm based on the several metrics which are best suited for the cryptographic algorithms. The performance is evaluated separately for text data encryption and voice data encryption. The metrics [11] that are selected for the evaluation are encryption time, decryption time, throughput of encryption, throughput of decryption, diffusion analysis, CPU process time, and CPU clock cycles, power consumption and memory utilization.

- Encryption time: The encryption time is the total time taken to produce a cipher-text from plain-text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption.
- Decryption time: Decryption time is the total time taken to produce the plain-text from Cipher-text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption.
- Throughput of Encryption: The throughput of the encryption scheme defines the speed of encryption. When there is an increase in the throughput of the encryption algorithm, there is a decrease in the power consumption algorithm.
- Throughput of Decryption: The throughput of the decryption scheme defines the speed of decryption. When there is an increase in the throughput of the decryption algorithm, there is a decrease in the power consumption algorithm.
- CPU process time: The CPU process time is the time that a CPU is dedicated only to the particular process for calculations. It reflects the load of the CPU. More the CPU time used in the encryption process, the higher is the CPU load.
- CPU Clock: The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy.
- Power Consumption: It is the total power that required by the encryption and the decryption algorithm. It was estimated based on the throughput of the encryption and decryption algorithms. When there is an increase in the throughput of the encryption/decryption algorithm, there is a decrease in the power consumption algorithm.
- Memory utilization: The memory requirement for the encryption and decryption.

IV. MATHEMATICAL MODEL

Several experimental procedures are used such as different encoding techniques for encryption, different packet sizes of data, different data types and different key sizes. In the case of encoding two types are used such as Base64 encoding and hexadecimal encoding. Packet size range from 0.5 MB to 20MB is used. Different data types such as text or document and images are used for each selected algorithms. Different key sizes are employed to trace the performance of the selected algorithms specifically power consumption. The formula to calculate the average encryption time is given in the equation (1).

$$AvgTime = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{M_i}{t_i}(Kb/s) \quad (1)$$

Where

AvgTime = Average Data Rate (Kb/s), Nb = Number of Messages, Mi=Message Size (Kb)

Ti=Time taken to Encrypt Message Mi

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as in equation (3.2).

$$Throughput = \frac{Tp}{Et} \quad (2)$$

Energy consumption for encryption and decryption can be measured in several ways. The first method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery that can computed by equations. The battery life is consumed in percentage for one run.

$$OneRun = \frac{Change\_in\_Batterylife}{No\_of\_Runs} \quad (3)$$

Average battery Consumed per iteration

$$\sum_{1}^{N}\frac{Battery\_consumed/Iteration}{No\_of\_Runs} \quad (4)$$

The second method of security primitives can also be measured by counting the amount of computing cycles which are used in computations related to cryptographic operations. For computation of the energy cost of encryption, the equation 3.5 as shown below was used.

$$B\_cost\_Encryption(ampere-cycle) = \tau * I \quad (5)$$

$$Total\_Energy\_Cost = \frac{B\_cost\_encryption}{F(Cycles/Sec)} \quad (6)$$

$$Energy\_cost = Total\_Energy\_cost * V \quad (7)$$

Where

Bcost_Encryption: = basic cost of encryption

T = The total number of clock cycles.

I = The average current drawn by each CPU clock cycle.

Total_Energy_Cost= The total energy cost (amp seconds).

F: clock frequency (cycles/sec).

Energy_cost = The energy cost (consumed).

So the amount of energy consumed by program P to achieve its goal (encryption or decryption) is given by

$$E = VCC * I * N * \tau \quad (8)$$

Where N = The number of clock cycles.

τ = The clock period.

VCC = The supply voltage of the system

I = The average current in amperes drawn from the power source for T seconds.

Several cryptanalysis methods are used to evaluate the security strength of the proposed system such as cipher-text only attacks, chosen plain-text attacks, adaptive chosen plain-text and cipher-text attacks, side channel attacks, brute force attacks and meet in the middle attacks. Other than this, autocorrelation analysis and the frequency distribution analysis were done to evaluate the security weakness of the algorithm.

The auto-correlation test [14] .mainly tests a line of auto-correlation. If {an} = {a0, a1, a2,…} is any binary sequence, the auto-correlation C(τ) is defined as

$$C(\tau) = \frac{1}{p} \sum_{n=1}^{p} a_n a_{n+\tau} \quad (9)$$

Here, τ can be treated as a phase shift of the sequence {an}. C (τ) measures the amount of similarity between the sequence and its phase shift. This is always highest for τ =0, and if {an} is random, C(τ) is quite small for most other values of τ. The autocorrelation analysis gives the randomness of data after every round of encryption process, by which the security strength is evaluated for the proposed system.

V. PERFORMANCE ANALYSIS

The performance measure of encryption and decryption schemes [17] was conducted using several performance metrics such as energy consumption, changing data types such as text or document and images, changing packet size and changing key size for the selected cryptographic algorithms. The experiments are performed several times to assure that the results are constant and are valid to compare the different algorithms.

The encryption time was calculated for the Blowfish with three different key sizes and SF Block cipher with different key size. It is the total time taken to produce a cipher-text from plain-text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. Different file sizes ranging from 40 Kb to 8000 kb is used for the evaluation. It gives the rate of encryption.

Table 1. Time Consumption for Encryption (Different Keys)

S.No	File Size (KB)	Time Consumption(Encryption)					
		Blowfish (Bits)			SF (Bits)		
		128	256	448	128	256	512
1	49.00	21.61	46.40	55.2	22.01	45.2	56.0
2	59.10	32.11	36.93	45.7	32.13	35.7	38.0
3	100.09	49.61	63.42	63.2	49.12	62.2	90.0
4	247.12	79.11	88.95	92.7	76.12	87.7	112.0
5	321.24	121.01	130.87	134.6	121.31	129.6	164.0
6	694.45	211.47	255.31	256.1	209.41	254.1	210.0
7	899.12	276.67	324.52	321.3	279.17	323.3	258.0
8	963.09	342.57	378.44	387.2	312.57	377.2	208.0
9	5345.15	834.67	880.26	879.3	721.13	879.0	1237.0
10	7310.39	877.07	909.07	921.7	856.01	907.8	1366.0

It can be seen that going from 128 bits key to 256 bits causes increase in power and time consumption about 8% and to 256 bit key causes an increase of 16%.

ISBN: 978-93-86171-32-0

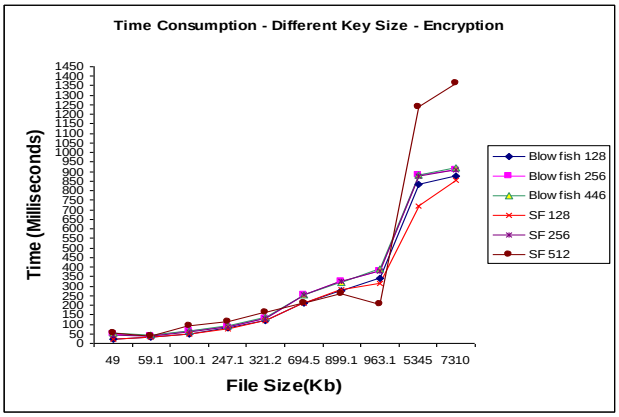

Fig 4. Time Consumption for Encryption (Different Keys)

Table 2. Time Consumption for Decryption (Different Keys)

S.No	File Size (KB)	Time Consumption(Decryption)					
		Blowfish (Bits)			SF (Bits)		
		128	256	446	128	256	512
1	49.00	21.84	57.21	55.44	22.15	45.27	56.01
2	59.10	32.34	42.15	45.94	32.27	35.77	38.24
3	100.09	49.84	69.09	63.44	49.26	62.27	90.31
4	247.12	79.34	96.07	92.94	76.26	87.77	112.52
5	321.24	121.24	135.56	134.84	121.45	129.67	164.21
6	694.45	211.7	275.09	255.89	209.55	254.17	210.34
7	899.12	276.45	345.08	321.09	279.08	323.37	258.21
8	963.09	342.35	402.34	386.99	312.48	377.11	208.04
9	5345.15	834.45	921.03	879.09	721.04	878.91	1237.09
10	7310.39	876.85	946.78	921.49	855.92	907.71	1366.14

Fig 5. Time Consumption for Deccryption (Different Keys)

The throughput of the encryption scheme defines the speed of encryption. When there is an increase in the throughput of the encryption algorithm, there is a decrease in the power consumption algorithm.

Table 3. Throughput(Encryption)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	IDEA	SF Block Cipher
1	49	59	78	56
2	59	39	46	38
3	100	94	104	90
4	247	121	134	112
5	321	167	198	164
6	694	234	267	210
7	899	254	342	258
8	963	213	456	208
9	5345	1324	1521	1237
10	7310	1432	1743	1366
Average		**393**	**488.9**	**374**
Throughput		**4.06**	**3.26**	**4.27**

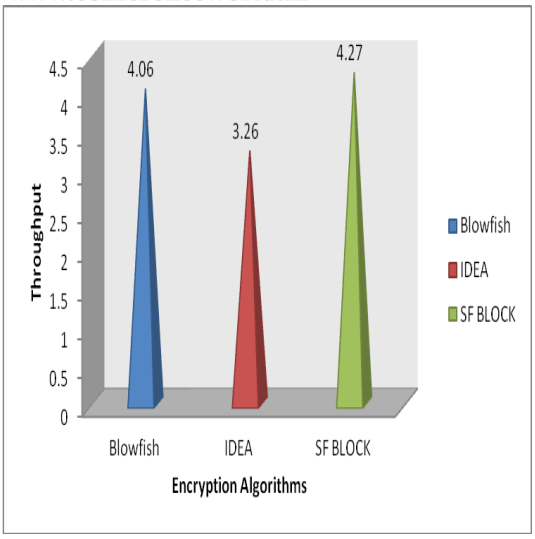

Fig 6. Throughput (Encryption)

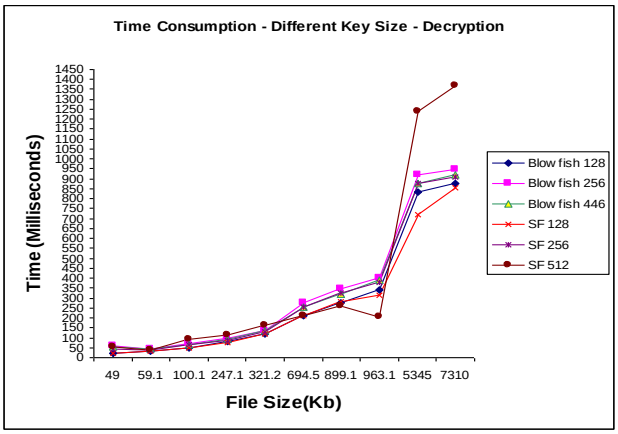

Table 4. Throughput(Decryption)

S.No	Packet Size (KB)	Time Consumption(Decryption)		
		Blowfish	IDEA	SF Block Cipher
1	49	65	78	61
2	59	45	56	43
3	100	89	97	79
4	247	120	131	112
5	321	167	198	168
6	694	243	301	212
7	899	223	378	259
8	963	334	423	309
9	5345	1224	1676	1216
10	7310	1435	1943	1363
Average		**394**	**528**	**382**
Throughput		**4.05**	**3.02**	**4.18**

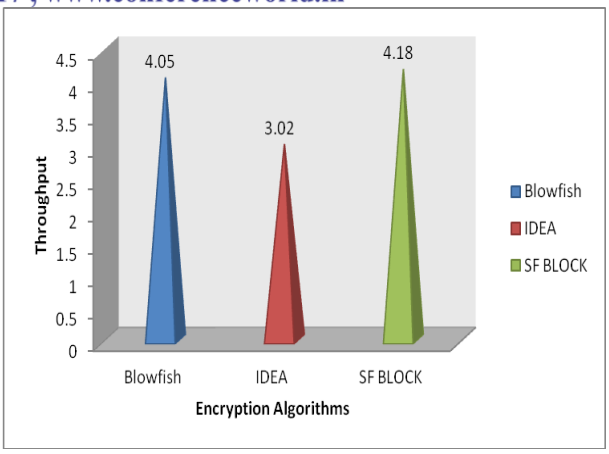

Fig 7. Throughput (Encryption)

Figure 6 denotes the throughput of encryption and figure 7 shows the throughput of decryption. From the analysis it shows that the SF Block cipher has better throughput than that of blowfish and IDEA algorithms.

VI . CONCLUSION

This paper presented the performance evaluation of three commonly known symmetric cryptographic algorithms. These algorithms are tested with different performance metrics. The simulation results shows that SF Block Cipher has better performance than Blowfish almost all the test cases. It is also identified that there is change in performance when there is a change in key size of SF Block cipher algorithm. Overall it is identified that SF can be used in circumstances where there is need for high security.

Journal Papers

[1]. Saleh, A. M. , and J. M. Simmons, 2011. Technology and architecture to enable the explosive growth of the internet, IEEE Communications Magazine, 49(1): 126-132.

[2]. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A., "Security in Software Defined Networks: A Survey," in Communications Surveys & Tutorials, IEEE , vol.17, no.4, pp.2317-2346

[3]. Kartalopoulos, S.V. , 2006. A primer on cryptography in communications, IEEE Communications Magazine, 44(4): 146-151.

[4]. Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar and Mohsin Iftikhar, 2011. A Survey about the Latest Trends and Research Issues of Cryptographic Elements, International Journal of Computer Science Issues, 8(3): 140-149.

[5]. Alabaichi, A.; Ahmad, F.; Mahmod, R., "Security analysis of blowfish algorithm," in Informatics and Applications (ICIA),2013 Second International Conference on , vol., no., pp.12-18, 23-25 Sept. 2013

[6]. Sandipan Basu., 2011. International Data Encryption Algorithm (Idea) – A Typical Illustration, Journal of Global Research in Computer Science, 2(7): 116-118.

[7]. M. Anand Kumar, Dr. S. Karthikeyan (2011), “Security Model for TCP/IP Protocol Suite”, Journal of Advances in Information Technology, 2[2], 87-91.

[8]. Potlapally, N.R., S. Ravi, A. Raghunathan, and N.K. Jha, 2006. A study of the energy consumption characteristics of cryptographic algorithms and security protocols, IEEE Transactions on Mobile Computing, 5(2): 128- 143.

[9]. Purnima Gehlot, S. R Biradar, B. P. Singh 2013, Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL, International Journal of Computer Applications,70(13):37-42.

[10]. Anand Kumar.M and Dr. S. Karthikeyan 2011)," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", 4[11]: 55-61.

[11]. Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

[12]. Anand Kumar M.and Dr. S. Karthikeyan (2011)," Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" International Journal of Computer Network and Information Security", 4[2] : 22-28

[13]. S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,PP 20-25.

[14]. Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E," Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect", International Journal of Computer Science and Network Security, 8(3), 2008.

[15]. Diaa Salama Abdul Minaam, Hatem M. Abdual- Kader Mohiy Mohamed Hadhoud (2010),"Evaluating the Effects of Symmetric Cryptogr aphy Algorithms on Power Consumption for Diferent Data Types", International Journal of Network Security, Vol.11, No.2, Sept. 2010, pp 78–87.

[16]. Peng Zhang; Chuang Lin; Yixin Jiang; Yanfei Fan; Xuemin Shen, "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks," in Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.9, pp.2211-2221

[17]. M. Anand Kumar.and Dr. S. Karthikeyan (2013)," An Enhanced Security for TCP/IP Protocol Suite" International. Journal of Computer Science and Mobile Computing, 2[11]:331-338.