Superiority of Blowfish Algorithm in Wireless Networks

Gurjeevan Singh
H.O.D - E.C.E
S.B.S.C.E.T, Poly Wing
Ferozepur

Ashwani Kr. Singla
H.O.D - E.C.E
G.T.B.K.I.E.T, Chappianwali
Malout

K.S. Sandha
Assistant Prof.
Deptt. Of E.C.E.
Thapar University , Patiala

ABSTRACT
Encryption algorithm plays a crucial role in information security which guarantees the recent growing internet and network applications. They are used to secure the data in wireless networks against malicious attacks but securing data also consumes resources such as C.P.U time, Memory, battery power, encryption time etc. In this paper, we evaluated the performance of four symmetric key encryption algorithms; AES, DES, 3DES and Blowfish which commonly used for data encryption in terms of encryption time, decryption time & throughput. In this research, we evaluated encryption time, decryption time and throughput for all four encryption algorithms in Visual Basic's environment using large size text data (.doc). Experimental results show that Blowfish encryption algorithm may be more suitable for wireless networks. Study reveals that Blowfish gives better performance than AES, DES and 3DES in terms of encryption time, decryption time & throughput.

Keywords
AES, Blowfish, DES, Encryption Algorithm, Security.

1. INTRODUCTION
Cryptography is a science of information security. It is the art of protecting the data. It stores and transmits the information safely over the insecure medium like Internet by encoding text data into a form non recognizable format with the help of various encryption algorithms and only the intended user will be able to convert it into original text. The process which converts original data into the unreadable form is called encryption process. The encrypted data is called cipher text. The reverse of data encryption is data decryption which converts the cipher text back into the original text. Original text is also called plain text. Cryptology is a combination of Cryptography (encryption) and cryptanalysis (decryption). Cryptography algorithms are classified as: Symmetric (private key) algorithm and asymmetric (public key) algorithm. In symmetric algorithms uses only one key for encrypt the data and same for decrypt the data. Asymmetric key algorithm uses two keys, one is used to encrypt the data and other is used to decrypt the data. Length of Key has an important place in Symmetric key encryption [1]. For the same algorithm, encryption using longer key is hard to cryptanalyze means more secure as compared to the one using shorter key. Asymmetric encryption techniques are almost one-thousand times slower than symmetric techniques as they require more computational processing power [2].

2. RESEARCH BACKGROUND
To give more perspectives of the performance of the compared algorithms this section discusses the results obtained from other resources:

Diaa Salama et.al (2011) paper presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. The selected algorithms are AES, DES, RC6, Blowfish, RC2 and 3DES. There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal it is found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod.

Simar Preet Singh et.al (2011) study reveals that Blowfish has better performance than other commonly used encryption algorithms. Since Blowfish has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm. AES showed poor performance results compared to other algorithms, since it requires more processing power.

M. Umaparvathi et.al (2010) discussed the comparison of the most commonly used symmetric encryption algorithms AES (Rijndael), DES, 3DES and Blowfish in terms of power consumption. A comparison has been conducted for those encryption algorithms at different data types like text, image, audio and video. Results showed that AES has a better performance than other common encryption algorithms used. Since AES has not any known security Weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. 3DES showed poor performance results compared to other algorithms since it requires more processing power.

Tingyuan Nie et.al (2010) discussed the performance of two symmetric key encryption algorithms: DES and Blowfish which commonly used for network data encryption. In this paper, they analyzed encryption security, evaluated encryption speed and power consumption for both algorithms. Experimental results show that Blowfish algorithm runs faster than DES, while the power consumption is almost the same. It is proved that Blowfish algorithm maybe more suitable for wireless network which exchanges small size packets.

Allam Mousa et.al (2006) paper Analyzing the RC4 parameters have shown that the speed of encryption or decryption time is directly related to the encryption key length and to the data file size if the data is large enough. Data type is also important since image data requires larger time to be processed than text or sound data mainly due to the larger file size. This relationship had been converted into equations to

model these relationships and so may be used to predict the performance of the RC4 under different conditions.

3. PROCEDURE TO EVALUATE PERFORMANCE

This section describes the simulation techniques which are used to evaluate the performance of various symmetric algorithms. In addition this section will discuss the methodology related parameter like experimental set-up and performance metrics.

3.1 Experimental Set-up

The various symmetric encryption algorithms have been implemented in Visual Basic language and the experiment has been carried out using a Laptop having 2.20 GHz Intel Pentium Core 2 Duo processor with 4 GB RAM on Windows 7 home premium, 32-bit operating system. In this experiment software encrypts & decrypts the text file of 98 MB.

3.2 Description of the Snapshot

The fig. 1 shows the screen shot of the software which is used by the user. Firstly the drive has been selected then folder after the particular file (which is to be encrypt or decrypt) and at last when we press the encrypt key;

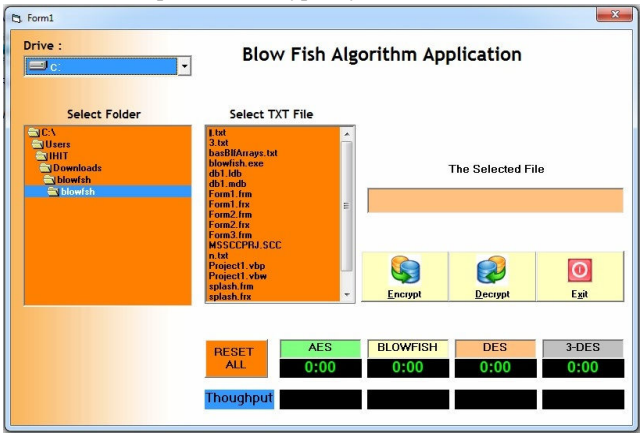

Fig. 1: GUI of the Software Used

the encryption time and the throughput of encryption time will be calculated automatically and displayed on the defined dialog box and to get the decryption and throughput of decryption time; first of all we reset it and again the same procedure is followed while selecting the file and similarly the value of decryption time and throughput of decryption time is calculated by pressing the decrypt key.

3.3 Performance metrics

The performance metrics are encryption time (milliseconds), decryption time (milliseconds) and throughput (Mb/sec.).

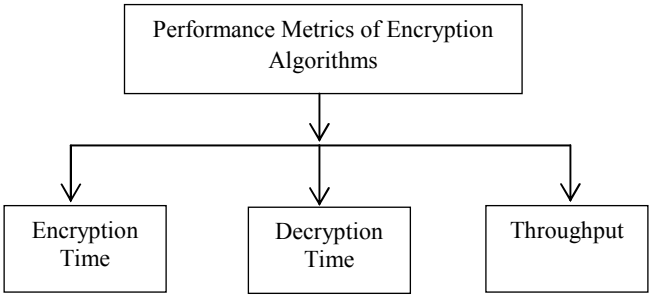

Fig. 2: Performance Metrics of Encryption Algorithms

The performance metrics analyzed and discussed by the researchers (as explained in the literature) regarding encryption algorithms are discussed below:

- Encryption Time: It is the time that an encryption algorithm takes to produce a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption process. In other words, it indicates the speed of the encryption process. The encryption time is generally calculated in milliseconds. It is the time taken by an encryption algorithm to encrypt the data. Less is the encryption time; more will be performance of that algorithm.

- Decryption Time: It is the time that an encryption algorithm takes to produce a plain text from a cipher text. Decryption time is used to calculate the throughput of a decryption process. In other words, it indicates the speed of the decryption process. The decryption time is generally calculated in milliseconds. It is the time taken by an encryption algorithm to decrypt the data. Less is the decryption time; more will be performance of that algorithm.

- Throughput: The throughput of the encryption scheme is calculated as the total plain text in encrypted in Kbytes divided by the encryption time in milliseconds. The unit of throughput is MB/Sec. More is the throughput; more will be the performance.

The throughput of the encryption scheme is calculated as the ratio of total plain text by encryption time [3].

$$\text{Throughput of Encryption Algorithm} = \frac{\text{Tp (Kbytes)}}{\text{Et (Milliseconds)}}$$

Where;
Tp: Total Plain Text (Kbytes)
Et: Encryption Time (Milliseconds)

4. RESULTS AND DISCUSSION

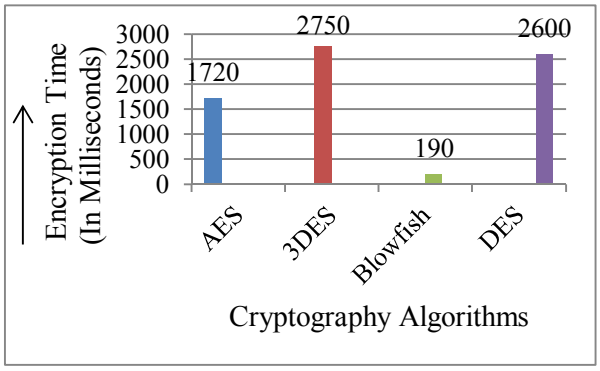

Fig. 2: Encryption time of Various Encryption Algorithms

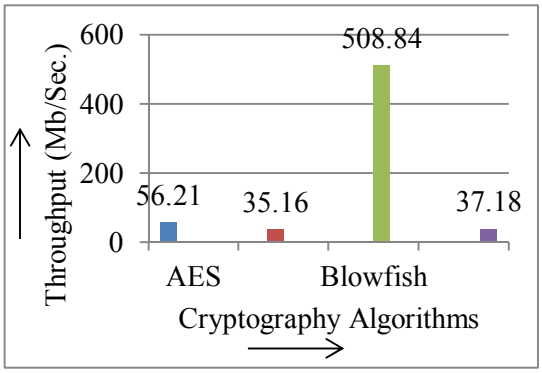

Fig. 3: Throughput (In Mb/sec.) of Encryption Process

4.1 Results & Discussion

We have taken four algorithms viz. AES, DES, Blowfish and 3DES. Firstly we have implemented them all, and then calculated their encryption time and finally the throughput of encryption time has been evaluated separately for each algorithm. Results conclude that the Blowfish is the best of all the four algorithms studied as it has minimum encryption time and maximum throughput due to its better performance followed by AES, DES and 3DES.

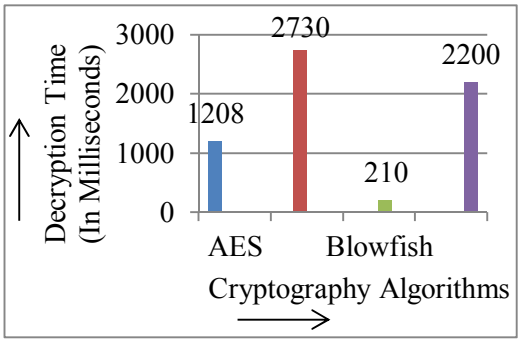

Fig. 4: Decryption time of Encryption Algorithms

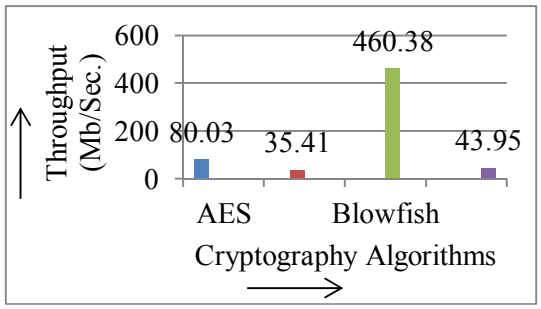

Fig. 5: Throughput (In Mb/sec.) of Decryption Process

4.2 Results & Discussion

The results suggest that the decryption time and the throughput of decryption time for Blowfish are better of all the four algorithms studied and due to its minimum decryption time and maximum throughput it gives better performance followed by AES, DES and 3DES.

5. CONCLUSION AND FUTURE SCOPE

We presented a fair comparison between AES, DES, 3DES and Blowfish in terms of Encryption time, Decryption time and Throughput. The presented simulations showed that Blowfish has better performance in terms of Encryption time, Decryption time and Throughput. Second point can be noticed here that AES has advantage over the other 3DES and DES in terms of throughput & decryption time except Blowfish. In third point at the same conditions 3DES has the least performance in terms of throughput of decryption process. In future the work may be extended by including the schemes and techniques by studying the different data packet sizes over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and minimum energy consumption.

6. REFERENCES

[1] William Stalling, "Cryptography and Network Security Principles and Practice 5th Edition", Pearson.

[2] Hardjono, "Security in Wireless LANs and MANs", Architect House Publishers, 2005.

[3] Diaa Salama, Hatem Abdual Kader and Mohiy Hadhoud (2011), "Studying the Effects of Most Common Encryption Algorithms", International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011, pp 1-10.

[4] SimarPreet Singh, and Raman Maini (2011), "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127.

[5] A.Rathika, Parvathy Nair and Parvathy Nair (2011), "A High Throughput Algorithm for Data Encryption" International Journal of Computer Applications (0975 – 8887) Volume 13, No.5, January 2011 pp 13-16.

[6] Lavanya P and M Rajashekhara Babu (2011), "Performance Analysis of Montgomery Multiplication Algorithm for Multi-core Systems Using Concurrent

Java", Journal of Advances in Applied Science Research, 2011, 2 (3), pp 567-573.

[7] M.Umaparvathi, Dr.Dharmishtan and K Varughese (2010), "Evaluation of Symmetric Encryption Algorithms for MANETs", Proceedings of 2010 IEEE International conference on Computational Intelligence and Computing Research (ICCIC-2010), 28-29 Dec. 2010, pp 1-3.

[8] Tingyuan Nie, Chuanwang Songa and Xulong Zhi (2010), "Performance Evaluation of DES and Blowfish Algorithms", Proceedings of 2010 IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), 23-25 Apr 2010. pp 1-4.

[9] Mingyan Wang, Yanwen Que (2009),"The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm", International Forum on Computer Science-Technology and Applications, 2009. pp 24-28.

[10] Allam Mousa and Ahmad Hamad (2006), "Evaluation of the RC4 Algorithm for Data Encryption", International Journal of Computer Science & Applications Vol. 3, No.2, June 2006, pp 44-56.

[11] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud (2008), "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS, VOL.8 No.12, December 2008, pp 280-286.

[12] Challa Narasimham , Jayaram Pradhan (2008), "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology, pp 254-259.