ISSN No:-2456-2165

Comparative Study of Blowfish

Malika Acharya
Masters of Technology, Department of Computer Science
Rajasthan technical University, Kota, Rajasthan.

Abstract:- With the growing data in transit, security has become utmost important issue to be addressed. Security of the data has given momentum to fields like cryptography. There are many cryptographic algorithms that have come in forefront in past decades. The application of each algorithm has grown in manifolds.

This paper reviews the cryptography algorithm blowfish and provides a fair comparison of it with DES. It has emerged a strong competitor to its contemporaries like AES and DES due to its compactness. Implementation of blowfish on supercomputers IMANC and also using MPI provided quintessential testimonial in the evaluation of blowfish in terms of speed, performance throughput and efficiency. The paper also reviews the modifications in the blowfish to support the security elements in the IoT. Although late in development blowfish has emerged in the scene as the best suited for the wireless networks, a nuance tested on variety of the data types.

Keywords:- *AES, Blowfish, Differential Analysis, Linear Cryptanalysis*

I. INTRODUCTION

Encryption involves the conversion of the plaintext into unreadable form called cipher text. There is broadly two heads of cryptography algorithm i.e. symmetric and asymmetric algorithm. Symmetric key algorithm uses only single key for both encryption and decryption. Whereas asymmetric key uses two separate keys for encryption and decryption, where the public key is established in the network while the private key is coveted and limited to the recipient.[1].There are many strong symmetric cryptography algorithms like AES,DES,IDEA, and Blowfish with a firm objective of coveting the information. The hardware implementation of each one of them is important in the narrative analysis. Isolated software implementations are seldom authentic as it provisions for the minimalistic security to key and even the Operating system can succumb to attacks. The implementation of the parallel blowfish sighting the time, speed, and parallel efficiency involves execution of MPI (Message Parallel Interface)on supercomputers. Also in today's world Internet of Things (IoT) has seen an unprecedented rise. With this development its important to provide a secure channel for transmission of data providing security to IoT. Blowfish has emerged has an efficacious tool for the same establishing its subtle modules. [2]. The advancement in the Function Module of the blowfish has widened the scope of the algorithm and the implementation of the same has been seen on Xilinx Virtex-5 XC5VLX50T FPGA using Verilog HDL[3]. The blowfish modification is an attempt to increase the throughput of the encryption by 18.7%. Using the comparative review of all, blowfish has emerged as the sound cryptographic algorithm that has been unbreakable since its introduction. The in-depth analysis of the algorithm shows that it can provide for the security of the parallel computing effectively.

As AES stands nowhere stand near broken, blowfish has passed the test of time and still unbreakable. The attacks could mangle the key near 4 rounds thereafter its compactness made it tedious and cumbersome. Advancement is tow fish that competes with AES in speed, block size, and key expansion. [4]

II. LITERATURE REVIEW

For the better and clearer comprehension of the work this section surfaces some of the eminent researches. Some selected algorithms are evaluated on their efficiency based on the criterion of authentication. There is huge disparity in the transmission time of data based upon whether it's an open key authentication or shared key authentication. The algorithm chosen for this are AES, DES, Blowfish, RC2, and RC6. [5]. AES performance showed a steep decline when evaluated in hardware implementation than blowfish due to its high power consumption. Blowfish passed the test as there are no weak points. 3DES had the lowest performance on the same. The proposition of use of algorithm on Graphical Processing unit (GPU) for parallel computing increasing the performance. It was demonstrated that with the increase in size of the files the time of the encryption and decryption is reduced. Also with the parallel execution of algorithm on FPGA the algorithm provided the high throughput and speedy especially in integrated pipeline technique. This was efficacious in reducing the critical path delay.[6]. The performance assessment of the algorithms also endows a different variation altogether with result being displayed in hexadecimal base encoding or in base 64 encoding. Blowfish being the highest performer followed by RC6 and others. But the same sequence goes reverse with image as a data type. Over here we observe a decrease in the performance of blowfish as far as time consumption is considered due to increase in key size.[7].As we can observe with the discussion above that there have been various approaches being used to evaluate the performance of these algorithms. The evaluation so done proves the mantle of blowfish as a stout security algorithm within accepted constraints of speed and time.

III. PEDAGOGY

A. *Blowfish Algorithm*

Bruce Schneier an eminent cryptologist propionate it in the year 1993 and since then it has not been cracked, primer reason being the compactness of this algorithm. It's a symmetric algorithm comprising of two steps: key expansion and data encryption. The algorithm converts the 441 bits key into arrays of 4168 bytes. The data encryption steps involve P array and S-boxes. As we know that the actual security of the algorithm is the onus of the S-box so here also the security is in the compactness of the operations of s-boxes that are in total of 256 entries each consolidated in 4 arrays each of 32 bit. With the 16-round Feistal Cipher the S-boxes used in this are key dependent resembling CAST-128.[8]. The process of s-boxes involves first the initialization of the input bits grouped in 32 bit subgroups. The second step is the XORing, i.e. XORing the 32 bits with the P_1 array, next 32 bit in P_2 and so on till near 448 bits have been XORed . Third step involves the encryption using P-array for the compact output of 64-bit block. After this we substitute these values in S-boxes and in order. With 4 32-bit S-boxes the operation above leads 256 entries in each S-box.

S1,0, S1,1,…….S1,255
S2, 0, S2,1,....., S2,255
S3, 0, S3,1,....., S3,255
S3, 0, S3,1,....., S3,255

This arithmetic operations involved in this algorithm are XOR's and four indexed array data lookups (per round) additions performed on 32-bit words. We use transformation function (F) at the final step to substitute the left and right half. This algorithm has the limited functionality in the places where the keys are stable for a long time i.e. keys does not change often.

B. *Analysis*

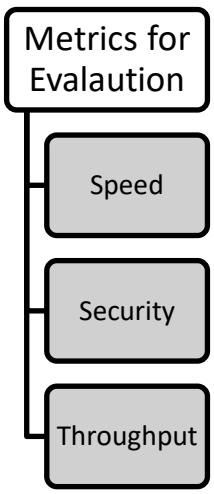

Fig 1

1. *Security Analysis*

The first analysis is a pure conceptual analysis based on the type of attack . The two approaches discussed here are:

i. Linear Cryptanalysis
ii. Differential cryptanalysis.

Introduced by Eli Biham and Adi Shamir differential cryptanalysis has been used to pit DES and Blowfish against each other. Bruce Schneier proposed that blowfish as in its proposed form with 16 rounds is unbreakable and to make differential analysis successful we need some piece of information unveiling the module function F. but on the whole it's the random generation of the boxes that makes blowfish attack resistance. On the other hand DES should its vulnerability with requirement of 237 DES operations for analysis. Differential attacks heavily depend upon the structure of S-boxes.

Mitsuru Matsui invented linear cryptanalysis though new in its advent yet showed some degree of effectiveness against DES with reduced number of rounds. With DES (16 rounds) there is need of 243 known plaintexts to break the algorithm. For the record it's important to note that it took 50 days to recover the DES key using 12HP9000735 workstation. [9]. AES in this respect also showed a great decline in performance since 5.8 million plaintext attack showed success rate of 84.16% . The success rate even varied with single-system and multi-system on the trial set of 1000.

Method	Success Rate
Single-system	91.8%
Multi –system	97.7%

Table 1:- Success Rate in 2 rounds

The substantial bias of 2-byte chosen texts attack were evaluated with theoretical ones in accordance with the Lemma 2 in (Matsui 1994).The algorithm further declined with the adoption of majority rule, multi-system attack as these increased the success rate of the 2-round AES attack involving Mix Columns.

Studies on avalanche effect allows us to juxtapose the AES and blowfish with ease. The researchers conducted the experiments primarily in CBC and EBC mode. If F_1 {i,j} is a function such that {I,j} is a set of data satisfying the avalanche criteria then , then avalanche equation goes as:

$$1/2\,(\sum \quad W(ae,j)) = (\frac{n}{2})$$

For assessing AES over here, first calculate the avalanche effect of S-box. The results provided that the algorithm was able to stand this with the success rate of .11. For the same effect blowfish was evaluated using the concept of hamming distance and flip –flops. The avalanche equation goes as

Avalanche Effect=
((hamming distance)/block Size)*100)

And the results were quite affirmative as the security of the algorithm was unbreakable. The reason for this is primarily the key dependent S-boxes. Owing to these blowfish shows 50% cipher text bits were different after every round[10]. Thus blowfish scores high in this respect too. The experiment is also conducted on other algorithms and the results have been tabulated as under:

Algorithm	% change in cipher text
AES	52.34
Blowfish	46.19%
DES	53.12
CAST-128	49.21

Table 2:- The experiment when conducted in ECB mode gave the following result.

Similar results table has been constructed for CBC mode also. The output was mapped to the statistical tests of NIST and the results clearly showed that blowfish was not much effective in ECB mode as it was in CBC mode.

As seen, blowfish gives higher avalanche effect than AES and also scores high. Thus blowfish has a strong immunity against differential cryptanalysis but in CBC mode only.

C. *Speed Estimation.*

Speed is time in computing. Nie,T.&Zhang, (2009) [11].made an effort to pit DES and blowfish in terms of speed with the following architecture:
1. Windows XP Os
2. PC with CPU Pentium® 43.00 Ghz

Blowfish gave a higher speed up than DES but it varied from memory size to memory size. As per my comprehension I would like to propose a scale up view of the analysis:[12].

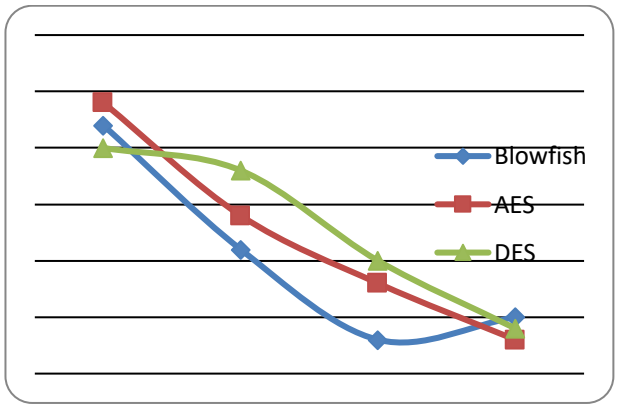

Fig 1:- Thoroughput of DES, AES, Blowfish

D. Advancement in Blowfish

1. IoT Security using Blowfish

IoT has gained recent recognition in IT industry. But the major concern is the interconnection of these that can lead to hijacker eavesdrop the information.

For providing the security to IoT's there is modification done in the blowfish. The S-box addition output in modified blowfish is in parallel which is then XORed to get the function output. The addition done here is modulo addition. Dr. J.deny (2016) attempted a hardware implementation for the same. The experiments expatiates that blowfish efficiency was on rise by 16.9% and throughput by 18.7%.

2. Linear Feedback Shift Register(LFSR)

Basic blowfish sufferrs from the demrit of requirement of large time to initialize the algorithm . this is because of the key dependent S-boxes that are generated in the consecutive rounds by imploying the blowfish itself. But the researches in [12] paper have proposed a modified algorithm to generate the S-boxes and P-arrays . this method even substantiates the avalanche effect as provided by the basic blowfish. The benefit of this system cam eup in the application of blowfish algorithm in speech encryption using LFSR. This aided the secure transmission of speech message over large channels with limitation that the key is seldom changed.

3. FPGA using VHDL

Blowfish is a fiestal cipher with 16 rounds. The researchers in paper [13] proposed the system to implement the blowfish on FPGA using VHDL programming language. The output of this experiment was complementary to the usage of the blowfish fot internet of things.(IoT). The researches evaluated the algorithm on the following criteria:
a. Security
b. Encryption time
c. Avalanche effect
d. Throughput

To make a note that the fiestal network allows the reduction in time with the reduction of number of rounds and also assists in higher throughput . this implication was deployed in using number on FPGA resources. The results from multiple test stations provided a testimonial for the blowfish
.

4. Render Script

Today's era is the era of mobile devices. Android security is need of the hour. Researchers in paper[14] have implemented the algorithm on Android devices using Render Script. Blowfish is itself a compact algorithm and thus a new language Render script was used on Android devices to enhance the security features of blowfish.

5. Audio Communication

RC2 is one of the fastest algorithm with a considerable immunity to linear attacks. But its vulnerable to related key attacks. With 234 chosen plaintexts and just one key query this cipher can easily be broken. The algorithm is used heavily in audio communication over VOIP(Voice Over Internet Protocol) clients just next to AES. Blowfish algorithm has been modified to implement in the same and showed a more secure and faster results with a better throughput. [15]

IV. FUTURE SCOPE

The algorithm is a Fiestal structure based algorithm with 16 rounds. This many number of rounds although provide more security , and compactness to algorithm thereby making it a strong symmetric cipher yet also lowers the performance because of the initialization cost in terms of time. The higher he time it will take it will become slower and initial throughput will decrease although overall throughput will remain steady.

Also power consumption is another cause of concern as it reduces the performance and also depreciates the liking in public domain.AES often scores high due to the same. Thus it is required to develop the algorithm based on the 3 factors:

1. Throughput
2. Security
3. Power consumption.

V. CONCLUSIONS

The present paper compares and analyses the common symmetric algorithms with blowfish using the work purported by the researchers. It was comprehended that although 2nd order differential attack tend to rock the algorithm but overall the algorithm is quite secure in the places where the key is not changed often. AES is furnished to be the best for multimedia files and in ECB mode but in CBC mode it stands second to blowfish. the researchers have gone far way to implement blowfish in various fields like IoT, FGPA, VHDL,LFSR, etc. These technology have been quite successful in demonstrating the security and robustness of the blowfish and also proposed a modified version of blowfish. though much of the work has been done in this field yet there is still a lot of scope and venues left to be explored and brought to the forefront.

REFERNCES

[1]. Asassfeh, Mahmoud & Qatawneh, Mohammad & Alazzeh, Feras. (2018). Performance Evaluation of Blowfish Algorithm on Supercomputer IMAN1. International journal of Computer Networks & Communications. 10. 43-53. 10.5121/ijcnc.2018.10205.

[2]. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud3, “Performance Evaluation of Symmetric Encryption Algorithms,” in IJCSNS International Journal of Computer Science and Network Security, vol.8 No.12, December 2008, pp. 280-286

[3]. Nie, T., & Zhang, T. (2009). A study of DES and Blowfish encryption algorithm. TENCON 2009 - 2009 IEEE Region 10 Conference.

[4]. IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83

[5]. Brian Cody, Justin Madigan, Spencer MacDonald, Kenneth W. Hsu, “High Speed SOC Design for Blowfish Cryptographic Algorithm”, IEEE, 2007

[6]. Singh, Gurjeevan & Singla, Ashwani & Sandha, Karmjit. (2012). Superiority of Blowfish Algorithm in Wireless Networks. International Journal of Computer Applications. 44. 23-26. 10.5120/6308-8632.

[7]. Tingyuan Nie, Chuanwang Song, Xulong Zhi, “Performance Evaluation of DES and Blowfish Algorithms,” 2010 International Conferenceon Biomedical Engineering and Computer Science, 23-25 April, 2010.

[8]. haitali Haldankar, Sonia Kuwelkar, “ IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM “, International Journal of Research in Engineering and Technology , Volume:03, Issue:03, May 2014.

[9]. E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Advances in Cryptology-CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 487- 496.

[10]. Himani Agrawal and Monisha Sharma, “Implementation and analysis of various symmetric cryptosystems,” in IJST Indian Journal of cience and Technology, vol.3 No. 12, December 2010, pp.1173-11

[11]. TingyuanNie; Teng Zhang; , "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Con-ference , vol., no., pp.1-4, 23-26 Jan. 2009

[12]. S. Pavithra, E.Ramadevi, “Throughput Analysis of Symmetric Algorithms”, International Journal of Advanced Networking and Applications, Volume-4, Issue-2, Pages:1574-1577,

[13]. Kuraniawan Nur Prestyo ST., Yudha Purwanto, ST., MT., Denny Darlis, S.Si, MT., “An Implementation of Data Encryption for Internet of Things Using Blowfish Algorithm on FPGA”, 2ndInternational Conference on Information and Communication Technology, IEEE, 2014.

[14]. Spencer Davis, Brandon Jones, Hai Jiang, «Portable Parallelized Blowfish Via RenderScript”, IEEE, 2015.

[15]. Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M. Fouad, “Speech Encryption Applying a Modified Blowfish Algorithm”, IEEE, 2014..