iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XI **Month of publication:** November 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Audio Encryption with AES and Blowfish

Rashmi A. Gandhi[1] , Dr. Atul M. Gosai[2]
[1]MCA Department, Shri Sunshine College, Rajkot,Gujarat
[2]Department of Computer Science, Saurashtra University, Rajkot, Gujarat

Abstract: ***With the rapid growth of information and communication industry, data transfer, communication of information, storing of data in cloud, sharing of valuable information across networks, raised the need of security of data. With the technological advancements data transfer is not confined only between computers/laptops they are now with the hand held devices like mobiles/tabs. So along with data security, speed and power consumption will also need attention. For secure communication over networks Cryptography is the proven tool. The rapid growth of digital data and its security raises the concern for developing more advanced techniques in cryptography. Cryptography is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. Algorithms are there for different data types like text, image, audio, video etc. Throughputs, Speed, CPU time, Power Consumption and security are few parameters on which cryptographic algorithms are analyzed. The present paper analyses some common symmetric cryptographic algorithms like DES, 3DES, AES, and Blowfish on the above parameters. This paper provides a comparative analysis of the existing cryptographic techniques. Further an in-depth study of Blowfish algorithm and latest work done on it are also discussed.***

Keywords: Cryptography, AES, Blowfish, LFSR (Linear Feedback Shift Register), FPGA (Field Programmable Gate Array), VOIP (Voice over IP).

I. INTRODUCTION

In today's digital world everything like data, documents, designs and ideas are digitized. Along with digitization the growing need and demand for transferring data over internet/networks, storing in cloud also raises concern for its security. Every organization today must digitize to thrive. Every sector be it education, corporate, banking, manufacturing industry, IT, government, judiciary, service industry is rapidly falling behind digitization for its survival. Every industry must find its way out to deliver modern business operations as well as customer satisfaction along with good workplace environment and facilities to survive in the market place.

The digital transformation seeks new applications which are faster, quicker, simpler and most important is Secure. The quick development in computer technologies and internet had made the security of information as most important factor in information technology and communication [5].

Cryptography plays a crucial role in the field of network security.

It is the physical process that scrambles the information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. In other words a given message (plaintext) is coded into a secure message (ciphertext) by applying some substitution techniques, to make the input message unreadable by anyone during its transmission.

The message that needs to be protected and communicated is called as plaintext. The method of scrambling the plaintext to make it undetectable is called encryption. The output of encryption process is the ciphertext. The process of getting back plaintext from ciphertext is called decryption. A system that performs encryption and decryption is called cryptosystem. Security of any cryptosystem should depend on the security principle proposed by Kirchhoff. According to Kirchhoff, the security of the encryption system should depend on the secrecy of the encryption/decryption key rather than the encryption/decryption algorithm [11].

The key objectives of cryptography are confidentiality, Integrity, Non-repudiation, and Authentication. Cryptographic algorithms can be classified into three independent dimensions based on transformations used, number of keys used as well as the way the way in which plaintext is processed. Based on type of operation used for transforming plaintext to ciphertext, cryptographic algorithms can be known as Transposition and Substitution schemes. Private Key (Single key/Symmetric) and Public key (two keys/Asymmetric) classification is based on number of keys used. Again Block ciphers and Stream ciphers is another classification derived from the way in which plaintext is processed.

DES, 3DES, AES, Blowfish, RC4, Twofish, Threefish, RC6, CAST, IDEA are the most common symmetric key cryptographic algorithms. Digital Signature Algorithm (DSA), Diffie Hellman, Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystem (ECC) are the most common asymmetric key algorithms.

Encryption algorithms are compared on parameters like encryption/decryption speed, reversibility, security against unauthorized attacks, CPU cycles and energy consumption. It was found that for multimedia data AES and Blowfish are proved to be strong. 9F

In the present paper an overview of the different algorithms used for Audio Encryption is demonstrated. Structure of the paper is as follows: Section 2 gives an overview of previous research work done on AES and Blowfish algorithms and their performance with Audio files based on the above mentioned parameters. Section 3 gives a review of AES and its working. Section 4 provides a detailed working of Blowfish. Section 5 provides a comparative study of different encryption algorithms. Section 6 gives an insight of latest work done to improve security keeping blowfish as a base algorithm. Conclusion is provided by authors in section 7.

II. RELATED WORK

There are a basic set of cryptographic algorithms based on the method on which they are developed. Again lot many algorithms are developed by doing improvements/changes in the base algorithms like DES/AES/Blowfish/RSA/IDEA etc. All the algorithms are focusing on different data types, different parameters, and different hardware platforms. Each algorithm has its strength and weakness. In the previous research work authors [5] have considered different file types, wired and wireless media, number of keys, block cipher or stream cipher and parameters like throughput, speed, security, CPU time, memory and battery power. Since the research work is focused on audio files, block cipher and symmetric key algorithms will be in focus. Out of all the symmetric key algorithms AES and Blowfish are good candidates for further improvements.

Encryption Algorithms DES, 3DES, AES and Blowfish are compared on parameters like execution time and security [2]. Performance of a block cipher varies with the block size and the key size. Larger block size makes algorithm faster, whereas larger key size increases security. All the algorithms are tested on same platform keeping security as a secondary concern. The Blowfish came out as the fastest performing algorithm.

A Secure encryption algorithm is considered energy efficient if it uses a minimum number of CPU operations [1]. The amount of energy consumption for algorithms like DES, KBCP-M-DES, 3DES and AES are analyzed. Energy consumption is calculated in terms of number of instructions required for encryption including the memory access time. The work concluded that DES and KBCP-M-DES uses the least amount of energy.

A large number of cryptographic methods based on symmetric cryptographic algorithms have been compared based on their application area, advantages, limitations, and working pattern [3]. They ensure excellent data security but there are certain areas that remained open. Out of the tested algorithms, the conclusion came for the Blowfish as the fastest and efficient algorithm. It can be considered as a base algorithm for further enhancement.

RSA and Diffie-Hellman algorithms are used as base algorithm to design a new algorithm [4]. The newly developed algorithm is compared with common encryption algorithm like DES, 3DES, RC2, AES and Blowfish on parameters like CPU time, memory and battery power. The new algorithm gives better throughput both for encryption and decryption as well as consumes less time, which results in lower consumption of battery power. In their work we can analyze that next to the new algorithm, Blowfish is best performing among the existing conventional methods followed by AES on the above mentioned parameters.

Paper [7], compared DES, AES, 3DES, and Blowfish on different sizes of data blocks and different hardware and software platforms. The outcome is the Blowfish as the best performing algorithm under the security against unauthorized attack. Blowfish is fastest and provides great security with strong key size. It can be used in many applications like Bulk encryption, Random Bit Generation, Network security and packet encryption. But it suffers from weak key problem which need to be rectified and explored.

Paper [8] also evaluated the performance of Blowfish and DES on security, speed and power consumption parameters. Experimental results demonstrated that Blowfish is faster than DES with same power consumption. Blowfish was also found suitable for wireless network application security.

With the advancement of technology there is vast need for security even for small embedded devices. Issues like providing strong security at lower cost is of prime concern. Competitor cryptographic algorithms like AES and Blowfish are compared on parameters like processing time, speed and power consumption [9]. Researchers confirmed the superiority of Blowfish algorithm over AES in terms of throughput, processing time and also consume less power.

In paper [10] researchers analyzed the performance of DES, AES and Blowfish Encryption algorithm on parameters like Execution time, memory required and throughput. The output indicates that blowfish algorithm consumes less execution time, memory usage and produces more throughputs. Blowfish performed approximately 4 times faster than AES and 2 times faster than DES. Due to more time required for processing, AES showed poor performance results compared to other algorithms.

Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. ADVANCED ENCRYPTION STANDARD (AES)

Both DES and 3DES are not good candidates for long term security; NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard. Out of the proposal in first round, 15 algorithms were accepted, out of which in 2nd round 5 algorithms were shortlisted and out of them NIST selected Rijndael as the proposed AES algorithm [a]. AES uses block length of 128 bits and a key length that can be 128, 192 or 256 bits. It is iterative and not like Feistel Structure.

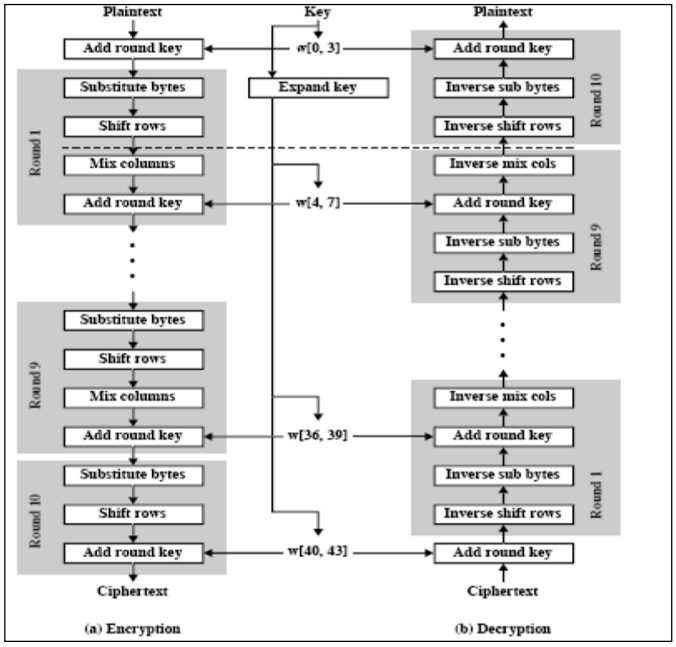


Figure 1: Overall Structure of AES

A. *Working Principle of AES*

In the following discussion we are taking a block length of 128 bits and a key length of 128 bits. Input to the encryption and decryption algorithm is a single 128 bit block which is a depicted as a square matrix of bytes. This block is copied into the state array which is modified at each stage of encryption and decryption. After the final stage, state is copied into an output matrix. 128-bit key is depicted as a square matrix of bytes. Key is then expanded into an array of key schedule words: each word is four bytes and the total key schedule is 44 words upto (4*44=176) 176-bits for the 128-bit key. Ordering of bytes is in column order.

AES is not following the Feistel structure but it processes the entire data block in parallel during each round using substitution and permutation. Four different stages are used, one is permutation and three is substitution.

1) *Substitute Bytes:* Uses S-box to perform byte by byte substitution of block.
2) *Shift Rows:* Simple permutation row by row.
3) *Mix columns:* Substitution that alters each byte in column as a function of all of bytes in column.
4) *Add Round Keys:* Simple bitwise XOR of current block with a portion of expanded key.

For both encryption and decryption, the cipher begins with an

1) *Add Round Key stage, followed by*
2) *Nine rounds that each includes all four stages,*
3) *Followed by a tenth round of three stages.*

Only the Add Round Key stage makes use of the key. For this reason, the cipher begins and ends with an Add Round Key stage.

The key feature of AES is each stage is easily reversible. The decryption algorithm makes use of the expanded key in reverse order. Decryption algorithm is not identical to the encryption algorithm. Since all the four stages are reversible, decryption can recover the original plaintext. The final round of both encryption and decryption consists of only three stages, and it is required to make the cipher reversible.

IV. BLOWFISH

Blowfish [5] is a keyed block cipher designed in 1993 by Bruce Schneier and widely used in a large number of cryptographic products. It provides good performance in software. Blowfish has 64 bit block size and a variable key length from 32 bit to 448 bits.

The algorithm works in two parts: A key expansion part and a data encryption part. The key expansion part is to convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes. It uses key-dependent s-boxes, which provide more resistance to differential and linear cryptanalysis. The data encryption is by a 16 round Feistel structure and uses a large key dependent S-Boxes. Each round consists of a key dependent permutation and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

It is suitable for applications where the key does not change often, like communications link or an automatic file encryption. It is comparatively faster than most encryption algorithms when implemented on 32 bit microprocessors with large data caches.

It uses simple operations that are efficient on microprocessors like exclusive-or, addition, table lookup, modular- multiplication. It does not use variable length shifts or bit-wise permutations, or conditional jumps. It employs precomputable subkeys. On large-memory systems, these subkeys can be precomputed for faster operation.

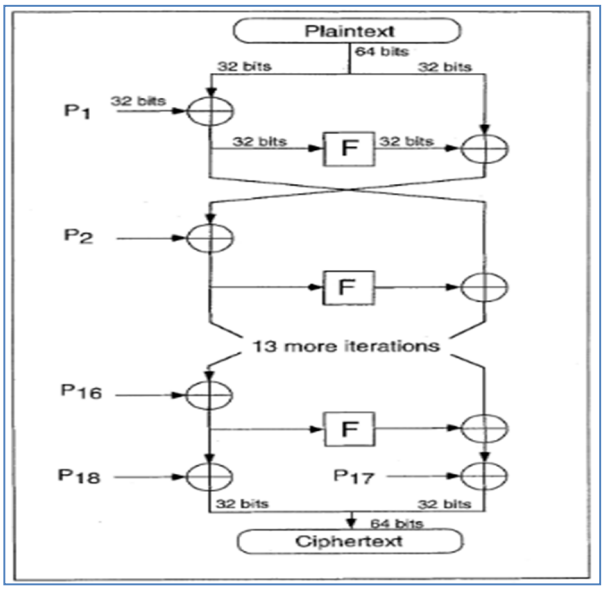


Figure 2: Structure of Blowfish Algorithm

A. Sub Keys of Blowfish Algorithm

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

1) The P-array consists of 18 32-bit subkeys:

P1, P2,..., P18.

2) There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

B. Calculation of Sub keys

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi(less the initial 3):

P1 =0x243f6a88, P2 = 0x85a308d3, P3 =0x13198a2e, P4 = 0x03707344, etc.

2) XOR P1 with the first 32 bits of the key,
XOR P2 with the second 32-bits of the key
And so on for all bits of the key (possibly upto P14).

Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. For every short key, there is atleast one equivalent longer key. For example if A is a 64-bit key, then AA, AAA, etc., are equivalent longer key.

3) Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described insteps (1) and (2).

4) Replace P1 and P2 with the output of step(3).

5) Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6) Replace P3 and P4 with the output of step(5).
7) Continue the process, replacing all entries of the P array, and then all four S-boxes in-order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required subkeys. Applications can store the sub-keys rather than execute this derivation process multiple times.

C. Encryption in Blowfish Algorithm

Blowfish has 16 rounds. The input is a 64-bit data element, x. It divides x into two 32-bit halves: xL, xR.

Then, for i = 1 to 16:

- xL = xL XOR Pi
- xR = F(xL) XOR xR

xL and xR are swapped. After the sixteenth round, swap xL and xR again to undo the last swap.

- xR = xR XOR P17
- xL = xL XOR P18.

Finally, recombine xL and xR to get the ciphertext. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. Implementations of Blowfish that require the fastest speeds should unroll the loop and ensure that all subkeys are stored in cache.

D. Pseudo-code for Blowfish Algorithm

Input:
T: 64 bits of plain text
P1, P2, ..., P18: 18 sub-keys
F(): Round function
Output:
C: 64 bits of cipher text
Algorithm:
(xL, xR) = T, dividing T into two 32-bit parts
Loop on i from = 1 to 16
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
End of loop
Swap xL and xR
xR = xR XOR P17
xL = xL XOR P18
C = (xL, xR)

E. The Round Function

Input:
A: 32-bit input data
S1[], S2[], S3[], S4[]: 4 S-box lookup tables, 256 long each
Output:
B = f(A): 32-bit output data
Algorithm:
(a, b, c, d) = A, dividing L into four 8-bit parts
B = ((S1[a] + S2[b] mod 2**32) XOR S3[c]) + S[d] mod 2**32

Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

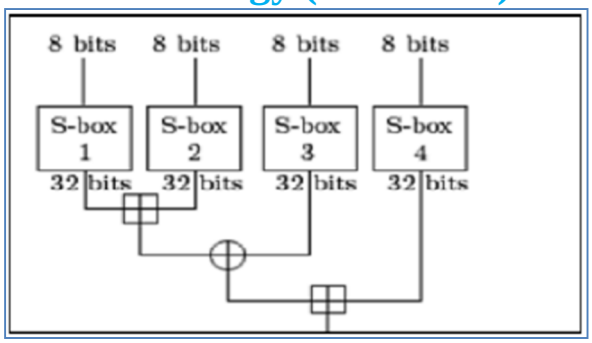


Figure 3: The Round Function

F. Blowfish Key schedule Algorithm

Input:
K: The key - 32 bits or more
PI: The binary representation of the fractional portion of "pi“
= 3.1415927... - 3.0
= 2/16 + 4*/16**2 + 3/16**3 + 15/16**4 + ...
= 0x243f6a8885a308d313198a2e03707344...
Output:
P1, P2, ..., P18: 18 32-bit sub-keys
S1[], S2[], S3[], S4[]: 4 S-boxes, 32-bit 256-element arrays
Algorithm:
(P1, P2, ..., P18, S1[], S2[], S3[], S4[]) = PI
K' = (K, K, K, ...), Repeat the key to 18*32 bits long
(P1, P2, ..., P18) = (P1, P2, ..., P18) XOR K'
T = (0x000000, 0x000000), Setting initial clear text
T = Blowfish(T), Applying Blowfish algorithm
(P1, P2) = T, Updating first two sub-keys
T = Blowfish(T), Applying Blowfish again
(P3, P4) = T
.....
T = Blowfish(T)
(P17, P18) = T
T = Blowfish(T)
(S1[0], S1[1]) = T
T = Blowfish(T)
(S1[2], S1[3]) = T
.....
T = Blowfish(T)
(S1[254], S1[255]) = T
T = Blowfish(T)
(S2[0], S2[1]) = T
.....
T = Blowfish(T)
(S4[254], S4[255]) = T

Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. COMPARATIVE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS

Algorithm	Block Size	Key Size	Rounds	Structure
DES	64	64	16	FIESTEL
3DES	192	64	16	FIESTEL
AES	128,192,256	128	10,12,14	NON- FIESTEL
BLOWFISH	64	32-448	16	FIESTEL

Table 1: Settings of Symmetric Encryption Algorithms

From the earlier work done by researchers as discussed in the previous section a comparative analysis can be done on parameters like Energy consumption, Execution speed, Security, Encryption/Decryption time and Throughput.

Algorithm	DES	3DES	AES	BLOWFISH
Energy Consumption [1]	Low	Highest	Medium	Lowest
Execution Speed [2,4,6,7]	Slow	Slowest	Medium	Fastest
Security	Cracked	Not cracked, but very slow	Not Cracked	Not Cracked
Encryption/ Decryption time [6]	High	Highest	Moderate	Lowest
Throughput [4,6]	Low	Lowest	High	Highest

Table 2: Comparative analysis on different parameters

From the table it can be observed that Blowfish algorithm is superior to other symmetric encryption algorithms in terms of energy consumption, execution speed, security, encryption/decryption time and throughput.

VI. RECENT ADVANCES IN BLOWFISH ALGORITHM

Researchers in paper [12] implemented Blowfish Algorithm in VHDL and provided a simple, robust implementation of the algorithm in hardware. The algorithm is already proved to be relatively secure and high speed over the competitors in the block and stream ciphers. The new implementation provides 590 Mbits/sec maximal throughputs which is 204% as fast as the leading pipelined competitors. Again it consumes only 63 mW of power during its operation.

Blowfish cryptosystem is implemented for different file types and also undergone different attacks [13]. Besides the well known brute force cryptanalysis attack, the linear and differential cryptanalysis is also examined. If the plaintext alphabet of characters is relatively evenly distributed and the key is chosen at random, little knowledge of plaintext and key can be gained from the cipher text. Only 12 rounds are necessary and enough to provide security. Significance weakness is yet to discover when the full 448 bit key and 16 rounds are used.

The throughput of blowfish cipher is further enhanced by designing a pipelined architecture in FPGA (Field Programmable Gate Array) [14]. It had been observed that Blowfish runs faster than DES and AES where frequent key changing is not needed. It is also suitable for wireless network applications which exchanges small size packets like any type of emergency control signal.

The Blowfish encryption algorithm have been proposed and implemented to encrypt the audio communication between the VoIP (Voice over Internet Protocol) clients [15]. It was also compared with earlier implementation of AES for VoIP. The output shows that blowfish is faster and offers better throughput. Experiments also show that RC2 as the fastest algorithm but it is vulnerable to related key attack and can be broken with one related key query and about 234 chosen plaintexts.

A modified Blowfish algorithm for speech encryption using LFSR (Linear Feedback Shift Register) is presented in [16]. The problem with the basic blowfish algorithm is the time required to initialize the algorithm with the key. The modified algorithm introduces a new method for generating S-boxes and P-arrays. This new method leads to a reduction in time complexity for generating S-boxes and P-arrays and produce good avalanche effect. An Avalanche effect shows that for a small change in one bit of plain text or key, it should produce significantly different cipher text by many number of bits. The modified blowfish algorithm offers the same level of security as the original blowfish with less computational overhead in key generation.

The Blowfish algorithm is implemented for mobile devices by taking the help of Render Script from Android Platform [17]. To provide improved mobile security, a new language technology, Render script on Android platform is used to utilize the power of parallelism to increase the efficiency of Blowfish algorithm. Mobile applications are also taking the help of Blowfish algorithm for providing security.

In their recent work researchers in paper [18] implemented Blowfish Algorithm on FPGA using VHDL programming language. Monitoring was done on the number of FPGA resources used. The Blowfish algorithm is analyzed on parameters like security, encryption time, avalanche effect and throughput from multiple testing scenarios for system reliability. Reducing the rounds of fiestels reduce total encryption time, give greater throughput, and not affect avalanche effect significantly. Larger key length demands more resource to be implemented on FPGA. The output shows Blowfish as a good alternative to propose a network security on internet of things.

The security of Blowfish Algorithm is analyzed in [20]. Cryptographic tests like randomness test, avalanche criteria and correlation coefficient must be conducted to test the algorithm. Non-Random block cipher is vulnerable to any type of attack. In their present work researchers had taken randomness of the output into consideration. Authors have investigated the blowfish algorithm on the statistical tests of National Institute of Standard and Technology (NIST). Blowfish Algorithm with the ECB (Electronic Codebook) and CBC (Cipher Block Chaining) modes were conducted for these tests. The output of the tests says that Blowfish algorithm with ECB mode is inappropriate with text and image data, while CBC mode can be a better alternative.

In paper [21] authors had continued with their earlier work for security of Blowfish Algorithm as discussed in [20]. In the present work they had analyzed the security of the algorithm using Avalanche criteria and correlation coefficient. The results obtained from the analysis of correlation coefficient showed that Blowfish algorithm gives a good non linear relation between plaintext and cipher text. The results of avalanche effect indicate that the algorithm presents good avalanche effect from the second round.

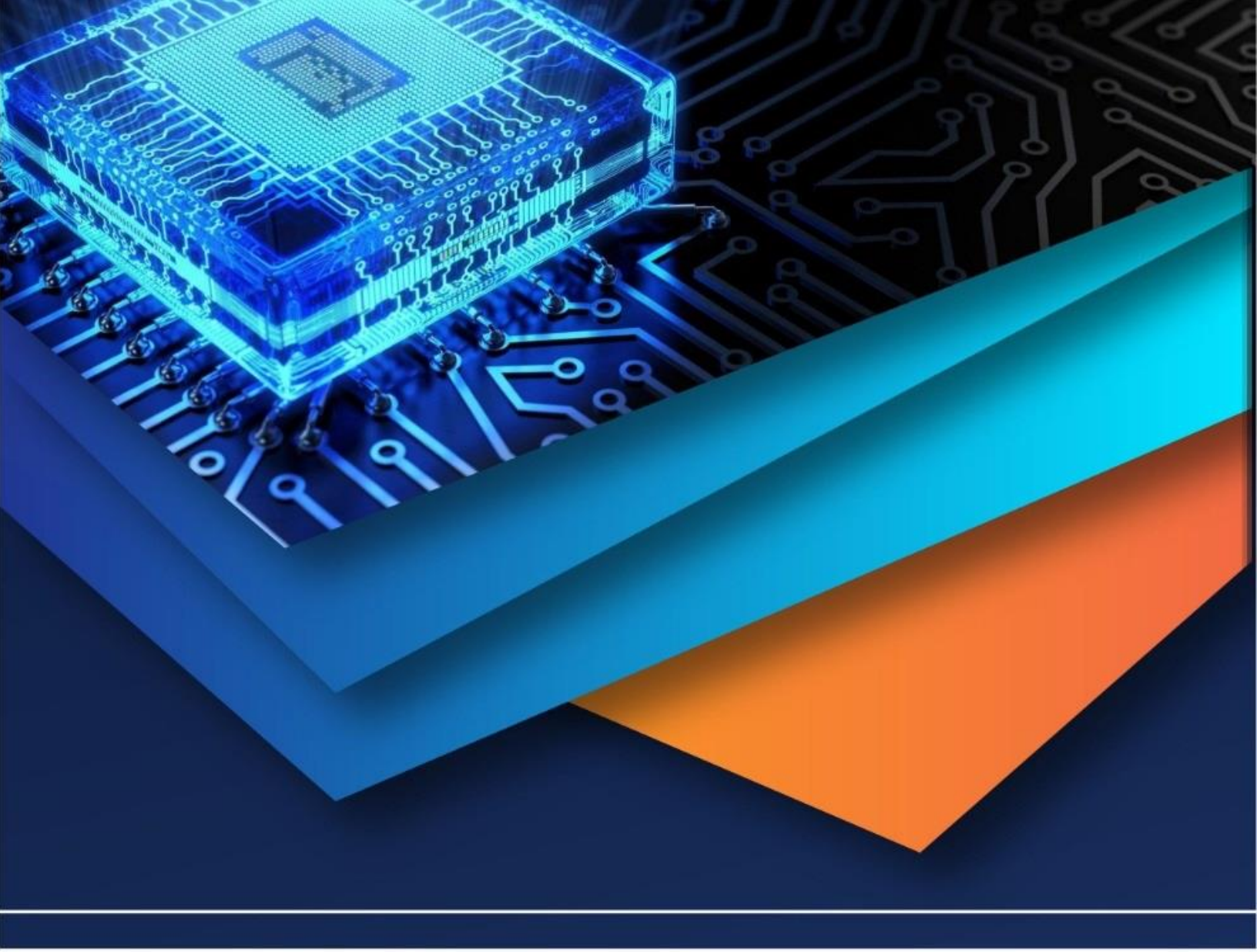
VII. CONCLUSION

In the present paper, the most common symmetric key algorithms were compared and analyzed on parameters like throughput, power consumption and security based on the work done by researchers. It is found that for multimedia files AES and Blowfish are better solutions. Further a detailed study on Blowfish algorithm is conducted. Some improvements in the algorithm are suggested. Researchers have taken the help of different techniques like pipelining with FPGA, VHDL, and LFSR to improve performance as well as provide more security. Yet enough scope is left for improvements. A proposed direction for future work could be to analyze the throughput and security parameters in detail. The algorithm with more number of rounds and more complex key proved to be more secure, but it will be slow. As a result throughput will be down. Again power consumption will be more. So the new algorithm should be designed keeping a balance of all the three factors i.e. Throughput, security and power consumption.

REFERENCES

[1] Walid Y. Zibideh, Mustafa M. Matalgah, “Energy Consumption Analysis for a class of Symmetric Encryption Algorithm”, IEEE 2014.
[2] Aamer Nadeem, Dr M. Younus Javed, “A Performance Comparison of Data Encryption Algorithms”, IEEE, 2005.
[3] Sourabh Chandra, Siddhartha Bhattacharyya, Smita Paira, Sk Safikul Alam, “A Study and Analysis on Symmetric Cryptography”, IEEE, 2014.
[4] Bijoy Kumar Mandal, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, “Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm”, IEEE,2013.
[5] Rashmi A. Gandhi, Dr. Atul M. Gosai “A Study on Current Scenario of Audio Encryption ”, International Journal of Computer Applications, Volume 116, No.7, April 2015.
[6] Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud, “Evaluating the effects of Symmetric Encryption Algorithms on Power Consumption for different Data Types”, International Journal of Network Security, Vol.11, No.2, Page.78-87, Sep 2010
[7] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi, “Performance Analysis Of Data Encryption Algorithms”, IEEE, 2011.
[8] Tingyuan Nie, Chuanwang Song, Xulong Zhi, “Performance Evaluation of DES and Blowfish Algorithms”, IEEE,2010.
[9] Chaitali Haldankar, Sonia Kuwelkar, “ IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM “, International Journal of Research in Engineering and Technology , Volume:03, Issue:03, May 2014.
[10] Ramesh .A, Suruliandi.A “ Performance Analysis of Encryption for information security”, IEEE 2013

[11] [b] S. Pavithra, E.Ramadevi, "Throughput Analysis of Symmetric Algorithms", International Journal of Advanced Networking and Applications, Volume-4, Issue-2, Pages:1574-1577, 2012.
[12] Brian Cody, Justin Madigan, Spencer MacDonald, Kenneth W. Hsu, "High Speed SOC Design for Blowfish Cryptographic Algorithm", IEEE, 2007.
[13] Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", IEEE, 2008.
[14] Swagata Roy Chatterjee, Soham Majumder, Bodhisatta Pramanik, Mohuya Chakraborty, "FPGA Implementation of Pipelined Blowfish Algorithm", Fifth International Symposium on Electronic System Design, IEEE, 2014.
[15] Khelf Mohamed, Ouslim Mohamed, Hamoudi.M, Masmoudi.M, "QoS evaluation in VoIP software with and without Blowfish encryption module", IEEE.
[16] Amaal A. Abd El-Sadek, Talaat A. El-Garf, Mohammed M. Fouad, "Speech Encryption Applying a Modified Blowfish Algorithm", IEEE, 2014.
[17] Spencer Davis, Brandon Jones, Hai Jiang, « Portable Parallelized Blowfish Via RenderScript", IEEE, 2015.
[18] 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", 2nd International Conference on Information and Communication Technology, IEEE, 2014.
[19] Jiali Bian, Bei Lu, Jian Kuang, " A New Hierarchical File Encryption System Based On Smartphone", 2nd International Conference on Computer Science and Network Technology, IEEE, 2012.
[20] Ashwak Alabaichi, Faudziah Ahmad, Ramlan Mahmod , Mohmood S. Mechee, "Randomness Analysis on Blowfish Block Cipher using ECB and CBC Mode", Journal of Applied Sciences, Asian Network for Scientific Information, 2013.
[21] Ashwak Alabaichi, Faudziah Ahmad, Ramlan Mahmod , " Securtiy Analysis of Blowfish Algorithm", IEEE, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY