ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Raj and Ross

ARTICLE OPEN ACCESS

# ENHANCEMENT OF BLOWFISH ENCRYPTION IN TERMS OF SECURITY USING MIXED STRATEGY TECHNIQUE

**Joseph Raj[1] and Shamina Ross[2]**
[1]*Dept. of Computer Science, Kamaraj College, Thoothukudi-628003, INDIA*
[2]*Dept. of Computer Applications, Scott Christian College, Nagercoil-629001, INDIA*

## ABSTRACT

***Abstract***—*Encryption is the process of transforming plain text data into cipher text in order to conceal its meaning and preventing any unauthorized recipient from retrieving the original data.Cryptography has been around for several thousands of years. During this time, different forms of cryptosystems have been developed. Cryptographic algorithms can be divided into symmetric key algorithms and public key algorithms.In the symmetric cryptosystem, the encryption and the decryption keys are the same. Among symmetric cryptosystems, ciphers of different security levels have been developed, ranging from the substitution and transposition ciphers to block ciphers, such as the Blowfish. As of today, the Blowfish has no cryptanalysis.Thispaper proposed a new algorithm combining Blowfish and the Mixed strategy(MS), named as MS-Blowfish to improve the performance of the Blowfish cryptography algorithm by making modifications to the Feistel (F) function. The outcome of the Blowfish and MS-Blowfish algorithms are compared using Avalanche Effect to show the security enhancement of MS-Blowfish.*

**Published on:** 08th– August-2016

KEY WORDS

*Avalanche Effect;Blowfish; Cryptanalysis;Feistel Network;Mixed Strategy*

***Corresponding author: Email:** v.jose08@gmail.com; **Tel**.: 9443151625

## INTRODUCTION

Cryptography plays an important role for protecting data from destructive forces and the unwanted actions of unauthorized users. Cryptographic algorithms have mathematically become more and more complex with time due to the ever increasing need for data security. However, the increase in the complexity of such algorithms incurs more computation overhead, which in turn leads to more execution time and high energy consumption recent years; successful studies have been made to speedup the execution of cryptographic algorithms. The Blowfish algorithm was designed by Bruce Schneier to replace Data Encryption Standard, which was the Federal Information processing Standard Cryptography [1]. It is a symmetrical block cipher [2] having the advantages of secure, fast, easy to implement etc. The operation part of Blowfish consists of XORs and additions on 32-bit words, and only 4KB or even less memory is needed when it runs. The key length ofBlowfish is anywhere from 32 bits to 448 bits, which makes datum safe enough.The proposed MS-Blowfish algorithm enhances the performance over Blowfish by modifying the function F of the existing Blowfish. There are a lot of benefits from parallel computing. The advantage of this system is its ability to handle large and extremely complex computations. The basic idea of this research is to simplify complicated cryptographic algorithms by splitting up their tasks to run in parallel successfully so that they execute fast and consume less energy. Amdhal's law states that possible speed gains are limited by the fraction of the software that can't be parallelized to run on multiple cores simultaneously [3]. The Parallel processing, Blowfish and Mixed Strategy concept in Game Theory are combined so that the security is increased.The Avalanche effect is used to show that the proposed MS-Blowfish algorithm possess good diffusion characteristics as that of original Blowfish algorithm [2] [4].The objective of this research paper is to study the Blowfish algorithm and enhance its performance using Parallel Processing and Mixed Strategy technique.

## RELATED WORK

### System Specification

For this researcha Laptop with Intel Pentium T4500 @ 2.30GHz CPU, 4.00GB Dual-Channel DDR3 and Linux Mint 17.1 is used in which the performance data are collected. In this the software encrypts the text file size that ranges from 50 bytes to 208942 bytes.

THE IIOAB JOURNAL
ISSN: 0976-3104



Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The performance matrices are the encryption speed, decryption speed, execution time, encryption throughput, decryption throughput, execution throughput and avalanche effect.The Blowfish cryptosystem was implemented using the C programming language in gcc compiler.

### Game Theory

The field of game theory and cryptographic protocol designare both concernedwith the study of interactions among mutually distrusting parties. These twosubjects have, historically, developed almost entirely independently within different research communities and, indeed, they tend to have a very different behavior. In Game Theoretic settings players are assumed to be rational. A great deal of effort was invested in trying to capture the nature of rational behavior, resulting in a long line of stability concepts.Cryptographic protocols are designed under the assumption that some parties are honestand faithfully follow the protocol, while some parties are maliciousand behave in an arbitrary fashion. The game-theoretic perspective, however, is that all parties are simply rationaland behave in their own best interests. This viewpoint is incomparable to the cryptographic one, although no one can be trusted to follow the protocol unless it is in their own best interests, the protocol need not prevent irrational behavior [5].

### Mixed Strategy

In the theory of games a player is said to use a mixed strategy whenever he or she chooses to randomize over the set of available actions. Formally, a mixed strategy is a probability distribution that assigns to each available action a likelihood of being selected. If only one action has a positive probability of being selected, the player is said to use a pure strategy. A mixed strategy profile is a list of strategies, one for each player in the game. A mixed strategy profile induces a probability distribution or lottery over the possible outcomes of the game.

One feature of mixed strategy equilibrium is that given the strategies chosen by the other players, each player is indifferent among all the actions that he or she selects with positive probability. In an interpretation advanced in 1973 by John Harsanyi, mixed strategy equilibrium of a game with perfect information is viewed as the limit point of a sequence of pure strategy equilibria of games with imperfect information. Specifically, starting from a game with perfect information, one can obtain a family of games with imperfect information by allowing for the possibility that there are small random variations in payoffs and that each player is not fully informed of the payoff functions of the other players. Harsanyi showed that the frequency with which the various pure strategies are chosen in these perturbed games approaches the frequency with which they are chosen in the mixed strategy equilibrium of the original game as the magnitude of the perturbation becomes vanishingly small. A very different interpretation of mixed strategy equilibria comes from evolutionary biology. To illustrate this, consider a large population in which each individual is programmed to play a particular pure strategy. Individuals are drawn at random from that population and are matched in pairs to play the game. The payoff that results from the adoption of any specific pure strategy will depend on the frequencies with which the various strategies are represented in the population. Suppose that those frequencies change over time in response to payoff differentials, with the population share of more highly rewarded strategies increasing at the expense of strategies that yield lower payoffs. Any rest point of this dynamic process must be Nash equilibrium. The long-run population share of each strategy corresponds exactly to the likelihood with which it is played in the mixed strategy equilibrium[6].

### Parallel processing

In parallel processing, each individual processor works the same as any other microprocessor. The processors act on instructions written in assembly language. Based on these instructions, the processors perform mathematical operations on data pulled from computer memory. The processors can also move data to a different memory location.

Processors rely on software to send and receive messages. The software allows a processor to communicate information to other processors. By exchanging messages, processors can adjust data values and stay in sync with one another. This is important because once all processors finish their tasks, the CPU must reassemble all the individual solutions into an overall solution for the original computational problem. There are two major factors that can impact system performance: latency and bandwidth. Latency refers to the amount of time it takes for a processor to transmit results back to the system. It is not good if it takes the processor takes less time to run an algorithm than it does to transmit the resulting information back to the overall system. In such cases, a sequential computer system would be more appropriate. Bandwidth refers to how much data the processor can transmit in a specific amount of time. A good parallel processing system will have both low latency and high bandwidth.

## BLOWFISH ALGORITHM

The Blowfish algorithm inputs a 64-bit plaintext and then outputs a 64-bit cipher text. It takes a variable-length key, from 32 bits to 448 bits [7], making it ideal for both domestic and exportable use. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The original sub key p-box and s-box are fixed. They are initialized in order with a fixed string that consists of hexadecimal digits of Pi (less the initial 3). Data encryption occurs via a 16-round Feistel network[8] after key expansion. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. The algorithm uses two boxes: key p-box [18] and key s-box [4] [256], and a core

ISSN: 0976-3104

Feistel function: The two boxes take up 18×32+256×32=4186 bytes memory. The sub keys must be pre-computed before any data encryption or decryption.
Function F is:Divide XL into four eight-bit quarters: a, b, c, and d

F(XL)=F(a,b,c,d)=((S1,a +S2,b mod2^32) XOR S3,c) + S4,d mod2^32

Herein, "+" is addition on 32-bit words, and XOR represents Exclusive OR; S1, a represents key s-box [1] [a], and similar of others.

Figure - 1 shows all operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. The process of decryption is the same as encryption, except that key p-box is used in the reverse order.

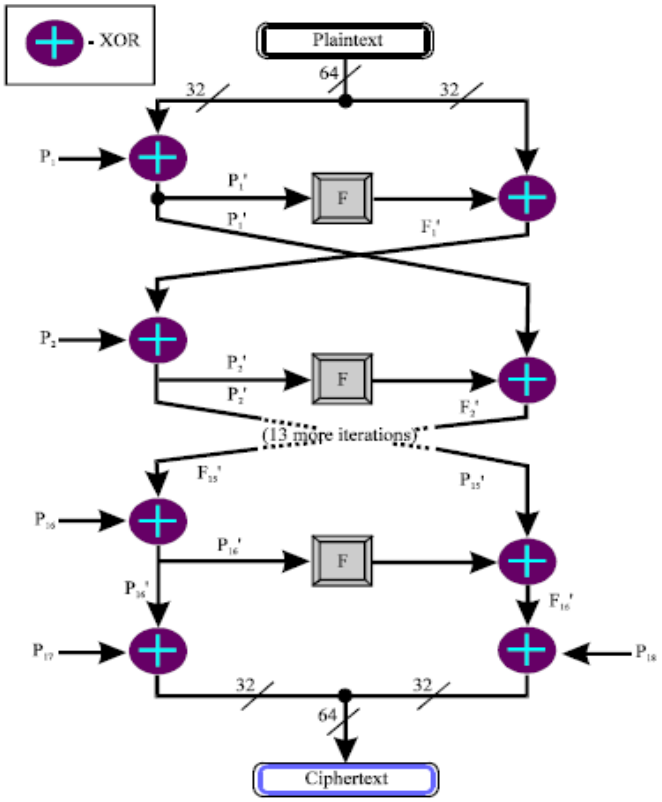



**Fig. 1: XORs and additions on 32-bit words**

The principle of Blowfish algorithm is both easy to understand and easy to implement. Different with other ciphers, all sub keys of Blowfish are influenced by every bit of the key, that makes the key and the data mingled together completely, which makes it quite difficult to analyze the key[9]. The function F gives the Feistel network a great avalanche effect.

Blowfish cipher is not only secure, but also fast, and suitable for different platforms, therefore, it has a high value of application in the field of information security.Blowfish is among the fastest block ciphersavailable[10]. Blowfish is used in wide range of applications such as bulk encryption of data files, remote backup of hard disk. Also multimedia applications use blowfish for encryption of voice and media files. It is now being used in biometric identification and authentication, using voice, facial or fingerprint recognition. Geographical information system uses blowfish for cryptographic protection of sensitive data. These applications run in high-end servers, workstations, process bulk amount of data and demand high speed encryption and higher throughput[11]. A study was conducted for different popular key algorithms such as DES, 3DES, AES and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The

ISSN: 0976-3104

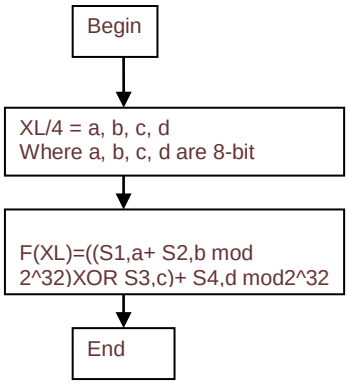


algorithms were tested on two different hardware platforms, to compare their performance. The results showed that Blowfish had a very good performance compared to the other algorithms [12]. Bruce Schneier made a block cipher speed comparison among Blowfish, RC5, DES, IDEA, 3DES algorithms[13]. The results showed the advantage of Blowfish among block ciphers in terms of speed. The results are shown in **Table-1**.From the **Table-1** it is clear that, the future of Blowfish as a secure algorithm is very promising. Blowfish algorithm is not only secure, but also fast, and suitable for different platforms. So it is widely used in the field of information security [14].

**Table: 1. Block Cipher Speed Comparison**

| Algorithm | Clocks/round | No. of Rounds | Clocks/byte of output |
|---|---|---|---|
| Blowfish | 9 | 16 | 18 |
| RC5 | 12 | 16 | 23 |
| DES | 18 | 16 | 45 |
| IDEA | 50 | 8 | 50 |
| 3DES | 18 | 48 | 108 |

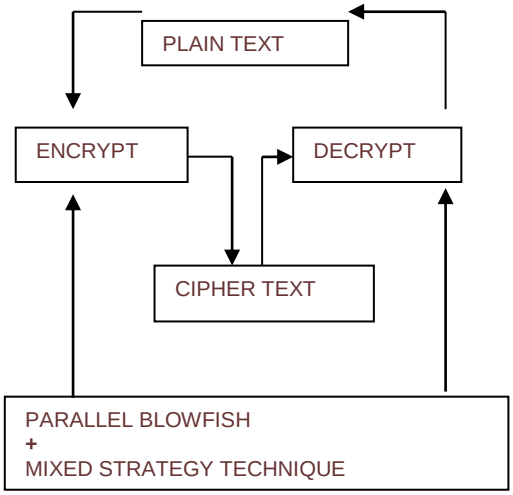
The following figure shows the calculation of the function F(XL) using Blowfish algorithm.




## PROPOSED MIXED STRATEGY-BLOWFISH ALGORITHM AND ANALYSIS

### MS-Blowfish

The block diagram shown below represents the structure of MS-Blowfish algorithm.

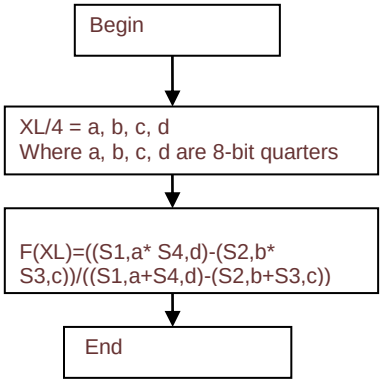



The proposed MS-Blowfishalgorithm is similar to the Blowfish algorithm with a modification in the F function. The modification shows parallel evaluation of different operations within the function. Without violating the security requirements, the Blowfish function F can be modified as follows:-

ISSN: 0976-3104

$$F(XL) = ((S1,a * S4,d) - (S2,b * S3,c))/((S1,a + S4,d) - (S2,b + S3,c))$$

This modification supports the parallel evaluation of two multiplication operations and two addition operations. Then parallel evaluation of twosubtraction operations. Finally,a division operation.All these operations take place in 3 steps.The following figure shows the calculation of F function using MS-Blowfish.




### Performance Comparisons

In this paper the performance metrics execution time, encryption time, decryption time, throughput, avalanche effect, power consumption are used to evaluate the blowfish algorithm and MS-Blowfish algorithm. The encryption time,the decryption time,the Execution time,is low for Blowfishalgorithm than MS-Blowfish algorithm. But the Avalanche Effect is high for MS-Blowfishthan Blowfish.MS-Blowfish is the best in terms of security.Blowfish algorithm by itselfis highly secure. But above all MS-Blowfish is unbreakable in any circumstances.

## EXPERIMENTAL RESULTS

### Encryption Time

Encryption Time is one of the performance metrics which is defined as the amount of time required for converting plaintext message to cipher text at the time of encryption[15]. Tabulation of results of encryption time with different packet size for Blowfish algorithm and MS-Blowfish algorithm are shown in **Table- 2**.and **Table-3.**The encryption time ofMS-Blowfish algorithm is slightly more than Blowfish algorithm.

### Decryption Time

Decryption Time is one of the performance metrics which is defined as the amount of time required for converting the cipher text into the plain text at the time of decryptionTabulation of results of decryption time with different packet size for Blowfish algorithm and MS-Blowfish algorithm are shown in **Table- 2**.and **Table-3**.The decryption time forMS-Blowfish algorithm is slightly more than Blowfish algorithm.

### Execution Time

Execution time of an algorithm directly depends on the functionality of the algorithm and it clearly defines that more complex structure originates poor execution time. Higher the key length provides higher security but increases execution time. The speed of the algorithm is determined by the execution time of the algorithm. Tabulation of results of execution time with different packet size for Blowfish algorithm and MS-Blowfish algorithm are shown in **Table- 2**. and **Table- 3**.Theexecution time forMS-Blowfish algorithm is slightly more than Blowfish algorithm.

THE IIOAB JOURNAL
ISSN: 0976-3104



## Throughput

The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in.

*Throughput= Total Plaintext in MegaBytes/ Encryption Time*

The higher the value of throughput more is the efficiency of encrypting any text with an encryption algorithm. Tabulation of results of throughput with different packet size for Blowfish algorithm and MS-Blowfish algorithm are shown in **Table-2** and **Table-3**.for Blowfish and MS-Blowfish algorithms respectively.

**Table: 2. Speed Analysis of Blowfish Algorithm**

| Data size | Encryption | Decryption | Execution |
|---|---|---|---|
| 50 | 0.7586 | 0.7602 | 0.8875 |
| 60 | 0.7709 | 0.7722 | 0.9058 |
| 100 | 0.7919 | 0.7934 | 0.9543 |
| 250 | 0.8962 | 0.8978 | 1.1592 |
| 325 | 0.9486 | 0.9497 | 1.2615 |
| 700 | 1.2776 | 1.2005 | 1.7646 |
| 900 | 1.3354 | 1.3364 | 2.0352 |
| 965 | 1.3741 | 1.549 | 2.29 |
| 5350 | 4.5246 | 4.4654 | 8.3683 |
| 7400 | 5.9181 | 5.8499 | 11.146 |
| 9000 | 6.9128 | 5.1447 | 11.4318 |
| 51202 | 20.9473 | 16.2216 | 36.5376 |
| 61442 | 23.8123 | 19.2313 | 42.4173 |
| 102402 | 37.7555 | 31.5148 | 68.651 |
| 208942 | 63.2736 | 63.159 | 126.085 |
| Average Time(millisec) | 11.41983333 | 10.25639333 | 21.05967333 |
| Throughput(MB/sec) | 2.500233162 | 2.783848579 | 1.3557782 |

**Table: 3. Speed Analysis of MS-Blowfish Algorithm**

| Data size | Encryption | Decryption | Execution |
|---|---|---|---|
| 50 | 1.0458 | 1.0482 | 1.1875 |
| 60 | 1.0562 | 1.0586 | 1.2071 |
| 100 | 1.0908 | 1.0932 | 1.2794 |
| 250 | 1.2321 | 1.2342 | 1.5609 |
| 325 | 1.3014 | 1.304 | 1.7002 |
| 700 | 1.6517 | 1.7891 | 2.5419 |
| 900 | 1.8431 | 1.9559 | 2.8977 |
| 965 | 1.9028 | 1.8738 | 2.8709 |
| 5350 | 6.1375 | 4.9518 | 10.1801 |
| 7400 | 7.2244 | 5.4114 | 11.7265 |
| 9000 | 8.2606 | 5.172 | 12.5251 |
| 51202 | 26.807 | 23.4668 | 48.2796 |
| 61442 | 30.7288 | 26.6701 | 56.5023 |
| 102402 | 45.6741 | 43.9294 | 88.5926 |
| 208942 | 87.9248 | 88.0193 | 175.5779 |
| Average Time(millisec) | 14.92540667 | 13.93185333 | 27.90864667 |
| Throughput(MB/sec) | 1.912996184 | 2.049422439 | 1.023060807 |

THE IIOAB JOURNAL
ISSN: 0976-3104



### Avalanche Effect

A change in one bit of the plain text or one bit of the key schedule will produce a change in many bits of the cipher text. This change in number of bits in the cipher text whenever there is a change in one bit of the plain text or one bit of the key is called Avalanche Effect [16]. A desirable feature of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text. If the changes are small, this might provide a way to reduce the size of the plain text or key space to be searched and hence makes the cryptanalysis very easy. For a cryptographic algorithm to be secure it should exhibit strong Avalanche effect. Tabulation ofresults observed by changing one bit of plain text in the sample is shown in **Table-4**. **Figure- 2**. represents the Avalanche effect of Blowfish algorithmandMS-Blowfish algorithm.In the bar chart Blowfish is represented as BF and MS-Blowfish as MSBF.

**Table: 4. Comparison of Avalanche Effect**

| Algorithm | BF | MSBF |
|---|---|---|
| Avalanche | 57.1 | 62.1 |
| | | |

The Blowfish algorithm has the lowest Avalanche effect when compared to the MS-Blowfish algorithm discussed here. So it is clear that MS-Blowfish algorithm is more secure than Blowfish algorithm.

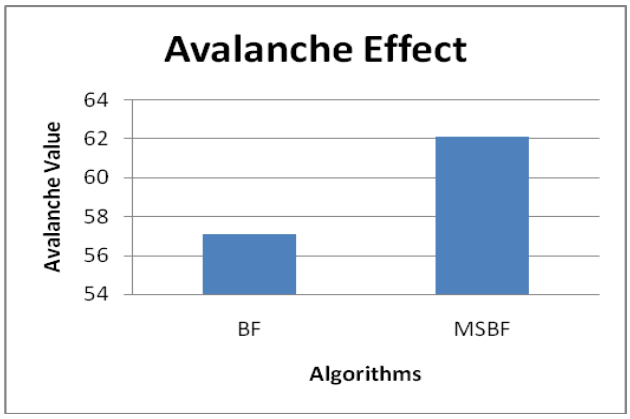



**Fig: 2.Comparison of Avalanche Effect**

## CONCLUSION

This paper gives a detailed study of the most popular symmetric key encryption algorithm that is Blowfish and discussed about its advantages. Based on the benefits of Blowfish algorithm we have proposed and implemented a new approach to further enhance the existing algorithm to achieve better results in terms of security. The striking feature of Blowfish encryption algorithm is that for the same input plaintext the cipher text generated at each time will be different. This is because every time a new random number gets generated and this as a result gives difference in the application of F function over each round. The advantage of different cipher text generated for the same input is it will greatly enhance the security aspect ofblowfish algorithm. The above results clearly indicate that the Avalanche effect of MS-Blowfish is much better than Blowfish algorithm.So it is clear that MS-Blowfish algorithm is very strong, secure and unbreakable than the Blowfish algorithm.The research work can be further extended with other optimization techniques which have potential capacities

## ACKNOWLEDGEMENT

None

THE IIOAB JOURNAL
ISSN: 0976-3104



## CONFLICT OF INTEREST

No conflict of interest

## FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

## REFERENCES

[1] US National Bureau of Standards.[1977]Data encryption standard,"U.S. Fed. Inform. Processing Standards Pub., FIPS PUB 46,January.

[2] Bruce Schneier.[1996] Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition, New York, John Wiley and Sons Inc, 21-27.

[3] Gene M. Adahl.[1967] Validity of the single processor approach to largescale computing capabilities, in proceedings of the April 18-20, 1967, spring joint computer conferenceAFIPS'67(spring) ACM,Newyork,NY, USA, pp.483-485.

[4] William Stallings. [2011] Cryptography and Network Security, *Fifth Edition, Pearson Education*,.119-120.

[5] YevgeniyDodis, ShaiHalevi, Tal Rabin. [2000]A Cryptographic Solution to a Game Theoretic Problem, Advances in Cryptology Crypto 2000, Springer-Verlag Berlin,Heidelberg-, 113-130.

[6] International Encyclopedia Of The Social Sciences, 2nd Edition, pp.290-292.

[7] Bruce Schneier[1993] Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), in Cambridge Security Workshop on Fast Software Encryption, Cambridge, UK, December 9-11:191-204.

[8] Bruce.Schneier[1994] The Blowfish Encryption Algorithm, *Dr. Dobb's Journal*, 19( 4): 38-40.

[9] Bruce Schneier. [1994]Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 191-204.

[10] on a Pentium.Retrieved 08:04:58, August 27, 2010 from http://www.schneier.com/blowfish-speed.html.

[11] T Srikanthan et al. Drill – A Flexible Architecture for BlowfishEncryption Using Dynamic Reconfiguration, Replication, Inner-Loop, Pipelining, Loop Folding Techniques, Springer- *Verlag Berlin Heidelberg*.6256-639.

[12] AamerNadeem, M YounusJaved.[ 2005] A Performance Comparison of Data Encryption Algorithms,*IEEE, Information and Communication Technologies*, 2005, ICICT 2005.First International Conference, -02-27:84-89.

[13] https://www.schneier.com/cryptography/blowfish/speed.html

[14] Mingyan Wang,YanwenQue, The Design and Implementation of Password Management System Based on Blowfish Cryptographic Algorithm,IEEE Xplore, International Forum on Computer Science- Technology and Applicatioins,2009, IEEE Computer Society, 978-0-7695-3930-0/09.

[15] R. Mohan, C.Rajan, Dr. N.Shanthi, "A Stable Mobility Model Evaluation Strategy for MANET Routing Protocols." International Journal of Advanced Research in Computer Science and Software Engineering. vol. 2, p.p.58-65, December 2012.

[16] Krishnamurthy GN, V.Ramaswamy, Leela GH, Ashalatha ME.[2008] Performance enhancement of Blowfish and CAST-128 algorithms and Security Analysis of Improved Blowfish Algorithm Using Avalanche Effect, *IJCSNS*,.8 (3): 244-250.

## ABOUT AUTHORS

***Dr.V. Joseph Raj*** *received the Ph.D. degree from ManonmaniamSundaranar University, Tirunelveli, India and P.G. degree from Anna University, Chennai, India. He worked as an Associate Professor of Department of Computer Engineering in European University of Lefke, North Cyprus for two years. He has been working as a Professor and HOD of Computer Science in Kamaraj College, Thoothukudi, affiliated to ManonmaniamSundaranar University, Tamilnadu, India. He is serving as Chairman of Computer Applications (P.G.) Board of Studies and Chairman of Computer Science Board of Examinations of ManonmaniamSundaranar University. He has been guiding Ph.D. scholars in various Indian Universities and many of his Ph.D. scholars were awarded Ph.D. degree. He has a vast teaching experience of about 29 years and research experience of 21 years. His research interests include Artificial Neural Network, Digital Image Processing, Wireless Networks, Operations Research and Biometrics. He has published several articles in International Journals and Conferences and National Journals and Conferences.*

***Mrs. Shamina Ross B****. received the M.Phil. degree from Vinayaka Mission University, Salem, India, P.G. degree from Annamalai University, Chidambaram, India and U.G. degree from ManonmaniamSundaranar University, Tirunelveli, India. She is presently working as Assistant Professor in the Department of Computer Applications in Scott Christian College, Nagercoil, affiliated to ManonmaniamSundaranar University, Tamilnadu, India. She has more than 7 years of teaching experience and research experience of 5 years. She has published papers in International Journals. Her area of interest in research includes Network Security and Artificial Intelligence.*