Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Secure Cloud File Storage System With Hybrid Cryptography Algorithm

[1]Dr. Ramalingam sugumar , [2]Srinivasan Thiruvengadam

[1]Professor & Director, PG & Research Department of Computer Science, Christhu Raj College (Affiliated to Bharathidasan University, Tiruchirappalli), Panjapur, Trichy, Tamilnadu.

[2]Ph.D Research Scholar, PG & Research Department of Computer Science, Christhu Raj College (Affiliated to Bharathidasan University, Tiruchirappalli), Panjapur, Trichy, Tamilnadu.

Abstract

Attention to the extent of the information used and also the growing use of cloud computing has become the delivery of several companies. And in many disciplines, investigators have placed great importance on cloud security over the past several decades. So information security is a big concern while keeping information in the cloud. Cryptography was one of the most critical methods of ensuring information security and privacy protection. As the number of institutions increases, so does the quantity of malicious activity. Malicious transactions can alter the information in a database, making it unusable for customers. Some ransomware was fairly efficient, and it demands money in exchange for data recovery. This paper presents a data protection strategy based on a number of cases of security risks using hybrid cryptographic algorithm. The methodology of encrypted message information would be discussed in this section as a security model. All information stored in cloud applications has been encrypted using the encryption technique. The method was tested using various file styles and sizes. It would be constructed so that it would work quickly an efficiently in a cloud infrastructure. A security of information approach was introduced in this study, in which information is stored using a hybrid cryptographic method. To be collected by Advanced

Encryption Standard (AES), BlowFish (BF), and Message-Digest algorithm (MDS). As a result, this architecture provides both speed and encrypted data.

Keywords: Cloud data storage; cryptography; Hybrid algorithm; Advanced Encryption Standard (AES), Blowfish and Message-Digest algorithm.

1. Introduction

Hybrid cryptography could be used to secure storage systems in the cloud. To distinguish between less safe and more protected by government, two different methodologies were used [1]- The first method uses the RSA and AES methods, the first being used for key encryption and the second for textual or encryption techniques [2]. The AES & Blowfish techniques were employed in the second, or perhaps safer, technique. These 2 techniques make it possible to double encrypt the information and password in this method, offering a higher security than the first [3]. Following the cloud computing adoption in several sectors, which include wellness, finance, property investment, army, and others, investigators' involvement in personal information cloud computing security has grown, as have their understanding of how to secure that information & how to increase the rate of its encrypted [4-5].

Its most important advantage of cloud services would be that the customer would be able to see the physical address of the service. All the client needs to do is make a connection to a gadget. Disaster recovery also benefited from cloud-based technology [6]. A single resource or device could also be distributed among these clients, allowing for more efficient use. A cloud administration is considered more secure if a specialized cloud organization has been tasked to reinforce [7].

Cloud management is considered more secure if a dedicated cloud organization has been tasked with strengthening [7]. Midway was responsible for data, and program and data security was increasing. By integrating modern operating systems, a cloud structure could deliver comparable functionality to all client [8]. Cloud computing technology comes with a set of drawbacks in addition to its many benefits. There's a lot of issues that come with cloud technology.

2. Related works

Cloud technology was one of the most frequently mentioned issues among investigators. Apart from cloud computing, interoperability, vendor blocking and membership may be other significant issues [9]. In any event, the threat of stability and compatibility has gradually faded away. Clients were often excluded from the provision of essential information in the fog as a result of the closure. Client data security would be an issue with cloud storage security . The research scientist demonstrated the security posture associated with the security y of data stored in the cloud [10]. A security portal, recovery template, assessment and visual modules were included. The security y techniques of cloud services were explained by the author. The RSA and MDS method were combined to ensure numerous security y features such as secrecy , integrin y of information, and not - repudiation [11-13] . User Input, Data Management and Users Output have been used to provide the Cloud Storage Security Service [14]. Three separate computers were used to ensure that all information was never damaged if one of them failed. The user input server stores user files and input data while ensuring user authentication and ensuring that information has never been accessed by unauthorized methods[15]. The data storage servers would be where AES cryptography was used to protect the input validation before the encryption keys were sent to the client output service. The user output server appears to be where the client obtains the output data or, encrypted document for future use [16]. Additional security could be another benefit of cloud services.

The proposed method uses cryptographical techniques to secure the cloud service[17]. As a result, the proposed program seeks to enhance the protection of information transferred to the cloud using encryption technology. A hybrid method that combines methods to encrypt data by
downloading the application from the cloud, separating it into 3 parts, and then encrypting every one of the 3 parts with encryption, & finally combining the 3 secured parts into one document & re-uploading to the cloud[18]. Mixing the AES, DES and RC4 methods gave the fastest runtime, which would have been faster than executing the AES algorithm individually. Researchers employ the Triple-DES & Krishna hybrid method, and also AES

& Krishna as a proposed technique, & Triple DES & RSA like another method, and also Blowfish & Krishna [19].

According to the previous section hybrid methods, the hybrid method that mixes AES, Blowfish, & Krishna seems to be the better method because its encode efficiency & power have been demonstrated. A mechanism for securing the information security y of documents posted to the cloud by various customer [20]. This approach employs a hybrid encryption algorithm that combines the blowfish & MDS algorithms. The suggested product's experimental results demonstrate that the length of the encrypted file was reduced by about 7% when compared with the existing method. Moreover, the suggested MDS with blowfish approach takes around 42 percent less time to encode and decode a word document than the existing Diffie -Hellman with AES strategy.

A system for ensuring the confidentiality of papers uploaded to the cloud by diverse consumers [20]. This method uses a hybrid encryption method that incorporates both the blowfish & MD5 methods. When contrasted to the existing study, the size of the encryption key was decreased by around 7% using the proposed company's experimental data. Moreover, encoding & decoding a word processor with the proposed MDS with blowfish method takes roughl y 42 percent less time than the current Diffie -Hellman with AES method. The Hadoop cluster plans the encrypted management architecture using the MapReduce structure. To encode the video data, the inventor also has provided a comprehensive encryption plot, a specific encryption plot, & an unfinished encryption scheme [22]. As a result, it increases the rate of the video, encrypting while also streamlining the process. ln addition, the customer could select the encryption plot that best suits their needs [23]. The test findings reveal that the video encryption management humans provide could match the requirements of speed, safety, & other factors. To secure the information, the researchers use the Blowfish algorithm. For key generation, publicly key-Elliptic Curve Cryptography (ECC) had been employed. The ECC algorithm is a set of encrypting that uses elliptic curves. lt was a simplified method that relies on the elliptical bent encrypted message. The findings suggest that maintaining the safety & soundness of cloud services seems to be a viable option.

3. Proposed System

One of the symmetric block encryption methods was AES provides for an information length of 128 bits & separates it into four blocks. These blocks were patronized as an array of numbers & structured as a 444 matrix, which would be referred to as the state. AES performs four sorts of changes every round for every 128-bit plain text to most encrypted security. The Blowfish algorithm was a method of symmetric block encryption. Both encryption and decryption of information were done with almost the same private key. The BF method was divided into two parts: information encrypting & key multiplication. There have been four 32-bit S-boxes and furthermore. Festal network rounds, a swap operation, & 2 special actions have been used in the second stage of the Blowfish procedure, which involves encryption technology.

The system was set up in such a way that it functions as follows:

1. The user has logged in when they have already signed up, or registers by providing information such as their name, email address, mobile number, account passwords, and so on.

2. The client then navigates through the local store to find the document that would be uploaded.

3. The client then selects the encryption method to be used. The proposed solution makes it possible for users

to combine AES & RSA or AES & Blowfish.

4. The chosen document was downloaded after being secured using the combinations of encryption methods chosen.
5. The customer has the choice to view or download the items have presented.
6. When a user chooses a document to download, the decryption key was emailed to the e-mail address provided at the time of registration or registration.
7. It allows users to download the decrypted or source document with that password.
8. The program also compares the security y of two combinations of hybrid encryption algorithms, namely the hybrid combination of AES & RSA and AES & BF.

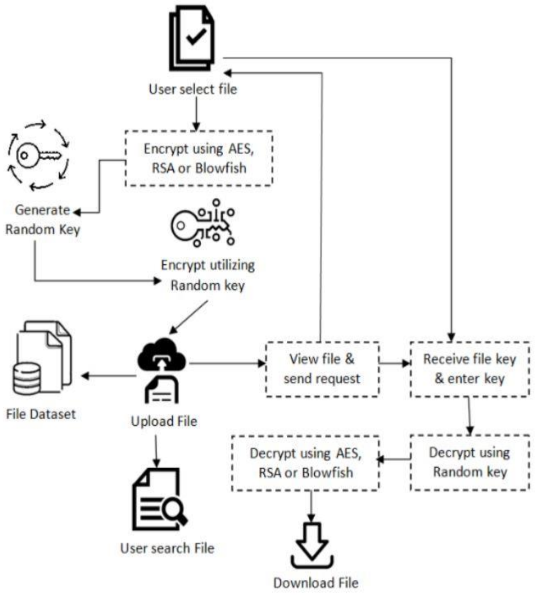


Figure 1: Proposed system architecture

3.1 Proposed Algorithm and the method

The need for a new method to make data storage more secure was highlighted in the preceding part. The stages of the proposed methodology were described as follows in Figure I . The method would be developed to function with plain text and ciphertext of 1024 bits. To make information safer, the method was regulated by a 1024-bit key. The encryption and decryption processes were similar. The production of keys seems to be the initial stage in the method. lt would generate a cryptographic value of 1024 bits. After that, it would be separated into 128-bit blocks. These eight blocks would serve as a starting point for generating new keys. A series identical to Random key AES was used to create the next keys.

3.2 Algorithm: Hybrid cryptography

Stage 1: A plaintext of 1024 bits is obtained.

Stage 2: The plaintext was separated into eight I 28-bit subs-blocks.

Step 3: Every I 28-bit sub-block would be joined to a key block produced by the Random Kay AES method.

Step 4: To use a replacement table, every bit would be changed by another bit.

Step 5: Results would be reorganized into 2D matrices.

Step 6: A mirror reflection of the matrix constructed.

Step 7: N time every bit would be relocated to the right. Thus N could be estimated as N= (number of steps) mod (number of steps) mod (number of steps) mod (number of steps) mcd (number

Step 8: To use the method previous step-key would be produced.

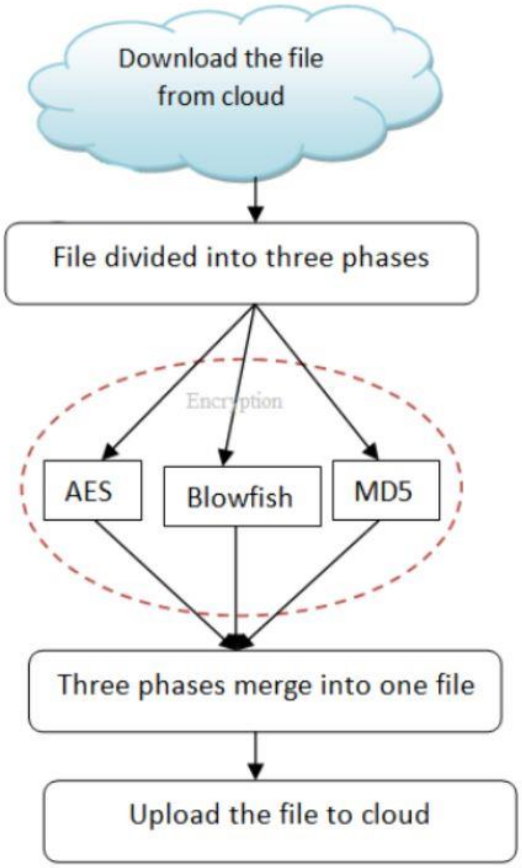
Step 9: lt would be included in the prior step's result.

Step 10: Repeat the iterations from step 2 to 9 until the file gets encrypted.

Step 11 : The same N number of iterations required to decrypt the file.

One of the encryption methods utilized in this study was hybrid encryption, which mixes 2 kinds of encrypted data. More than one procedure, whether of the same kind of various types, could be employed in this type, & this strategy was utilized to improve cloud computing systems. Symmetric & hashed encrypting were employed in this investigation, and several encryption techniques such as AES, BF and MD5.

The encrypting process has been carried out in a series of phases, as described in Figure 2, starting with downloading the application to be encoded and afterward separating it into 3 parts using the system files component. Every one of these portions was encoded using one of three different encryption algorithms. After then, the portions were merged into a single file & re- uploaded to the cloud.


Download the file from cloud
File divided into three phases
Encryption
AES
Blowfish
MD5
Three phases merge into one file
Upload the file to cloud

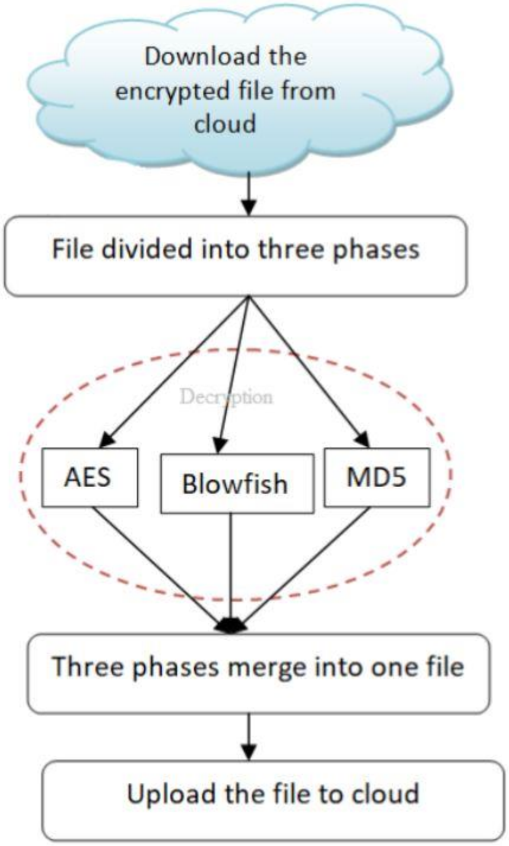

Download the encrypted file from cloud
File divided into three phases
Decryption
AES
Blowfish
MD5
Three phases merge into one file
Upload the file to cloud

Figure 2: Proposed hybrid method encryption

The decryption procedure involves the following steps in a reverse manner as the encryption method. The encoded downloaded file is firstly, then separated into three portions, each of which can be allocated for decryption according to the encryption method. The suggested technology's decryption procedure was depicted in Figure 3.

4. Result and Discussion

The proposed method was applied utilizing modular j's, MySQL, & java after the infrastructure had been established. The document & keys were stored in encrypted data in a MySQL database. RSA, AES, & Blowfish were therefore deployed on the same architecture as the suggested protocol. As a result, a correlation was obtained. Five parameters were used to evaluate the method. Encryption process,

Figure 3 Proposed hybrid method decryption

decryption, memory usage after decoding, avalanche impact, & entropy seem to be the five parameters. The streaming graphs compare the proposed encryption method to others. The RSA, AES, & blowfish methods were selected for the evaluation because they have been verified for encrypting. Figure 4 depicts the time it takes for a method to encrypt a document of various sizes. The proposed algorithm requires less time than other techniques such as RSA, AES, & BF. lt's also worth noting that the length of time it takes to encrypt a document grows in tandem with its size.

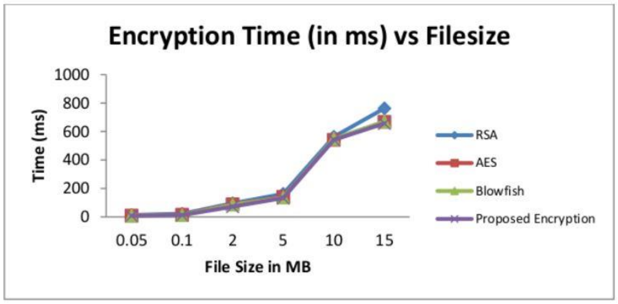


Figure 4: Comparison of proposed with existing system based on encryption

E j - Encryption time

Figure 5 depicts the time required for the technique to decrypt a document of various sizes. Decryption was performed on the same document that had been encrypted using a method. lt has been shown that the suggested encryption technique decrypts information faster than other methods such as RSA, AES, & BF. lt's also worth noting that the length of time it takes to decode a file grows with its size.

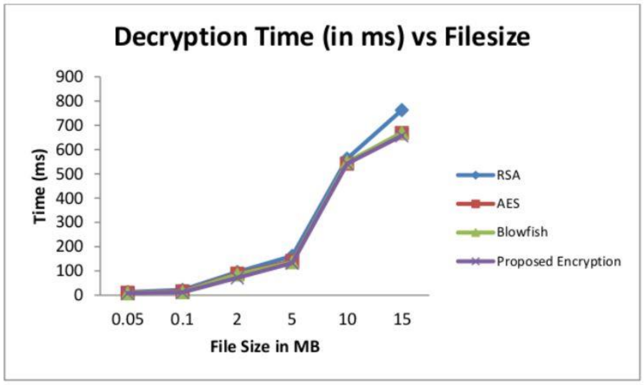


Figure 5: Comparison of proposed with existing system based on decryption

D j - Decryption time

The entropy calculation for the method is shown in Figure 6. The level of randomness in the information can be collected by entropy. Every important piece of information establishes a link between the facts. For effective encryption techniques, the entropy should have been high. The suggested encryption methods, have a similar entropy to RSA & Better than AES & BF.

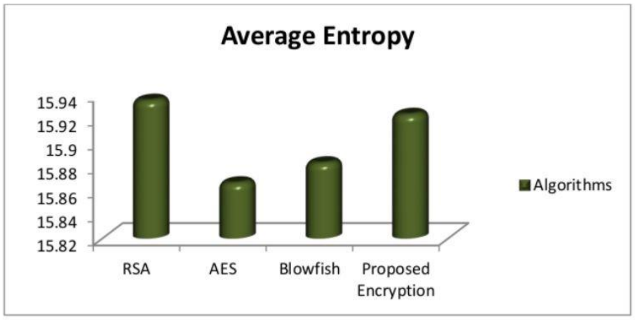


Figure 6: Median entropy of proposed and existing methods

The avalanche impact for methods was depicted in Figure 7. The effect of the cascade effect would be that a small change in the value causes a massive change in the output. Figure. 7 shows that the suggested encrypting system's avalanche impact was comparable to AES & stronger than Blowfish. RSA has a stronger avalanche impact than other methods.

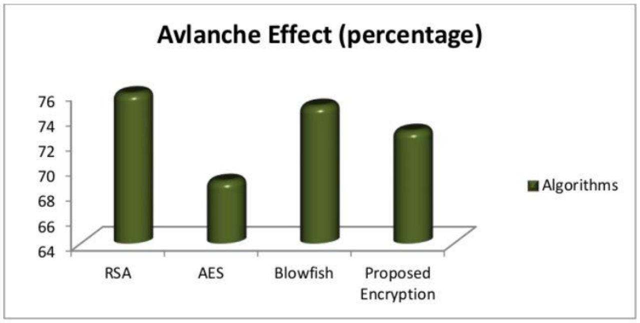
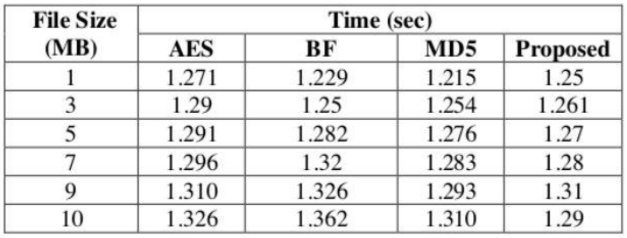


Figure 7: Avalanche effects comparisons of proposed and existing methods

4.1 Security Network

There has been no doubt that safety y should not be the only issue of cloud services customers; the use of systems that enable information security of data might slow information flow because encryption and decryption take a little time, therefore the time limit has become crucial when using encryption technologies. Techniques were selected for this study based on their capacity in terms of encryption performance & decoding. To demonstrate the suggested program's functionality, documents of various sizes were encoded using the AES, BF, & MDS techniques, and the new method, as shown in Table I . Table I compares the results of encryption execution time for documents using methodologies and also the proposed method.

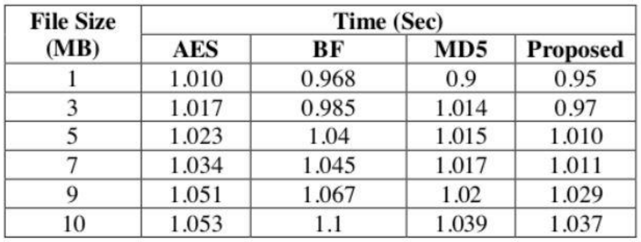
Table I Encryption efficiency



File Size (MB)	Time (sec)			
	AES	BF	MD5	Proposed
1	1.271	1.229	1.215	1.25
3	1.29	1.25	1.254	1.261
5	1.291	1.282	1.276	1.27
7	1.296	1.32	1.283	1.28
9	1.310	1.326	1.293	1.31
10	1.326	1.362	1.310	1.29

Researchers evaluated the validity of three methods, AES, Blowfish, & MDS, and also a hybrid approach suggested with varying large files, in this research. Humans ran the indicated methods on documents with sizes of 1.3.5.7.9 &10 Megabytes to see how fast they ran. The hybrid method and other methods were developed in Java, & tests have been performed on a machine with an Intel Core i5 CPU running at 2.50GHz & 8GB of RAM. Whereas the decoding method must have been implemented in documents to encrypt in cryptographic processes of various sizes using the AES, Blowfish, & MD5 methodologies, & also the proposed model, Table 2 compares the results of the decoding processing time for encryption keys using methodologies and also proposed method.

Table 2 Decryption efficiency



File Size (MB)	Time (Sec)			
	AES	BF	MD5	Proposed
1	1.010	0.968	0.9	0.95
3	1.017	0.985	1.014	0.97
5	1.023	1.04	1.015	1.010
7	1.034	1.045	1.017	1.011
9	1.051	1.067	1.02	1.029
10	1.053	1.1	1.039	1.037

5. Conclusions

Security is a major concern in cloud computing file storage, prompting academics to develop several technologies that enable increased performance & security of data encryption in the cloud. This study propose an encryption technique for encrypting shows significantly to cloud service. The discussion showed that the suggested encryption method provides greater encryption. In comparison to RSA, AES, & Blowfish the suggested technique takes less time to encrypt & decode documents, according to the findings. The structure of the ciphertext formed by the proposed method was comparable to industry norms, as demonstrated by avalanche impact & entropy numbers. As shown in previous portions, the key attribute of the suggested encryption method is that it would be hard to break shortly. Moreover, the trend of the encryption method is that it would be hard to break shortly . Moreover, the trend of the encryption time indicates that the suggested approach would become increasingly beneficial as the data size grows. The AES, BF and MD5 methods were combined to provide hybrid cryptography. This hybrid cryptography, which combines symmetric & hash encrypting, improves the encrypted communication procedure's performance and effectiveness.

References

[1] S.Bruce, "Description of a new variable-length key, 64- bit block cipher (Blowfish),"In Fast Software Encryption Second International Workshop, Leuven, Belgium, December 1993, Proceedings, SpringerVerlag, ISBN: 3-540-58108-1, pp.191- 204, 1994.

[2] K..Russell Meyers, and H.Ahmed Desoky, "An implementation of the Blowfish cryptosystem," Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, Sarajevo, Bosnia and Herzegovina, pp. 346-351, December 16-19, 2008.

[3] M.Allam,"Data encryption performance based on Blowfish," 47th International Symposium ELMAR, Zadar, Croatia, 2005,pp. 131-134.

[4] T. Jawahar and K. Nagesh "DES, AES and Blowish: Symmetric key cryptography algorithms simulation based performance analysis,". Int. J. Emerg. Technol. Adv. Eng., 1:pp. 6-12, 2011.

[5] G.S.Srikantaswamy," An analysis of the design factors affecting the performance of cryptosystems," Indian Journal of Computer Science and Engineering (IJCSE), pp.684-686, ISSN : 0976-5166, 2(5), Oct-Nov 2011.

[6] M. Stamp , "Information Security: Principles and Practice," San Jose: San Jose State University. John Wiley & Sons, Inc,2006.

[7] J.Alfred Menezes, C. Paul Oorschot and A. Scott Vanstone , Handbook of applied cryptography: CRC Press, ISBN 0-8493- 8523-7,1997.

[8] M. Alexander ,"Some Words on Cryptanalysis of Stream Ciphers," Lund University, PH. D. thesis,2006.

[9] A. Siva Rapeti,"Nlfs: A New Non-Linear Feedback Stream Cipher," master thesis, 2008.

[10] O. Mohammad Awad Al-Hazaimeh," New cryptographic algorithms for enhancing security of voice data," Universiti Utara Malaysia, UUM, PH. D. thesis.

[11] C. Jeyamala, B. Subramanyan, & S.G Raman,"Ensemble of Blowfish with Chaos based S box design for text and image encryption," International Journal of Network Security & Its Applications (IJNSA). 3(4), pp.165-173, doi : 10.5121/ijnsa.2011.3415, 2011.

[12] W. Jason Cornwell, Blowfish Survey. Department of Computer Science, Columbus State University Columbus,GA.,2012.

[13] S.V.Bagad and A. I. Dhotre , "Cryptography and Network Security," 2nd Revised Edn., Pune, India: Technical Publications, ISBN-13: 9788184313406, Pages: 202, 2008.

[14] V.Tilborg Henk C.A. and J. Sushil ," Encyclopaedia of cryptography and security," 2nd edition, Springer Science and Business Media, ISBN 978-1-4419-5906-5, 2011.

[15] S.Bruce, " Applied Cryptography: Protocols, Algorithms and Source Code in C," 2nd edition, New York: Wiley, ISBN 10: 0471117099, 1996.

[16] A Suriyani, "A human immune system inspired byte permutation of block cipher, " PH.D. thesis, UPM.,2012.

[17] J. Julia, M. Ramlan, S. Salasiah " A Proposal for improving AES S-box with Rotation and Key-Dependent, " In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference on, pp. 38- 42. IEEE, 2012.

[18] S. Salasiah, M. Zaiton, J. Julia, "The New Approach of Rijndael Key Schedule , " In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference on, pp. 23-27. IEEE, 2012.

[19] M. Eman Mahmoud, A. Ahmed, A. Talaat .Elgarf, Z. Abdelhalim,"Dynamic AES-128 with Key-Dependent S-box, " International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 , 3(1), January -February 2013, pp.1662-1670.

[20] E. Dawson, H. Gustafson and A. N Pettitt," Strict Key Avalanche Criterion," Australasian Journal of Combinatorics, vol.6 147-153, 1992

[21] C. Julio Hernandez Castro, M. Jos´e Sierrab, S. Andre, I. Antonio , R. Arturo, " The strict avalanche criterion randomness test," Mathematics and Computers in Simulation," vol. 68, doi:10.1016/j.matcom.2004.09.001, 2005.

[22] D. Ali, E. Barıs, K. Onur, and S. Fatih,"Cryptographic randomness testing of block ciphers and hash functions,"Cryptologye. Print Archive, Report 2010/564, 2010.

[23] A. Himani and S. Monisha,"Implementation and analysis of various symmetric cryptosystems," Indian Journal of Science and Technology, 3 (12), SSN: 0974- 6846,pp.1173-1176,2010.

[24] S. H. Mohan.and R.A Reddy ,"Performance Analysis of AES and MARS Encryption Algorithms,"IJCSI International Journal of Computer Science Issues, 8(1), ISSN (Online): 1694-0814,2011,pp.363-368.

[25] R. Sriram and K. Marimuthu,"Designing an algorithm with high Avalanche Effect," IJCSNS International Journal of Computer Science and Network Security, 11(1),2011. [26] A. Fahmy, M. Shaarawy, K. El-Hadad, G. Salama and K. Hassanain ,"A Proposal For A Key-Dependent AES," SETIT 2005,3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 27-31, 2005 – TUNISIA 2005.

[26] A. Suriyani, M. Ramlan, J. Azmi, R. Muhammad Kamel Ariffin," An Immune System-Inspired Byte Permutation Function to Improve Confusion Performance of Round Transformation in Symmetric Encryption Scheme, "in Computer Science and its Applications: springer, pp.339-351, 2012.

[27] [27] Y. Faiz Mohammad, E. Alaa Rohiem, D. Ashraf Elbayoumy ,."A Novel S-box of AES Algorithm Using Variable Mapping Technique",13th International Conference on

AEROSPACE SCIENCES & AVIATION TECHNOLOGY,ASAT- 13, May 26 – 28, 2009.

[28] S.R.Kumar, E. Pradeep, K. Naveen and R. Gunasekaran, "A Novel Approach for Enciphering Data of Smaller Bytes", International Journal of Computer Theory and Engineering, 2(4), 1793-8201, pp. 654- 659,2010