International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 26 Issue 3 – APRIL 2019.

ENHANCED PRIVACY PRESERVING USING MULTILEVEL ENCRYPTION TECHNIQUE

P.Anbazhagan[#1], M.Suruthisudar[#2], V.Madhumitha[#3], Dr.M.Ezhilarasan[*4]

[#,1,2,3]*Student, Department of Information Technology , Pondicherry Engineering College, Puducherry*

[*4] *Professor, Department of Information Technology , Pondicherry Engineering College, Puducherry*

***Abstract*— Data security in the delivery of online file becomes very important in the world of information itself. One way that can be done for the security of the data is to perform encryption before the data is sent This project proposes Multilevel Encryption System using BLOWFISH encryption algorithm and AES (Advanced Encryption Standard). Multilevel encryption system involves two or more encryption algorithm techniques to provide more security and efficiency. AES (Advanced Encryption Standard) is a symmetric cryptographic algorithms means that the key used in the encryption process is the same as the key to the decryption process. The analysis concludes theory, AES encryption process is designed to make the process of encoding in secret with no security level of complexity linear with time as efficiently as possible through the use of processes of transformation of light in the implementation. Aside from the AES algorithm, Blowfish algorithm is also a symmetric cryptographic algorithm. Theory analysis shows that BLOWFISH a cryptographic algorithm that uses a key with variable length. Here, we propose a two way secured data encryption system, which addresses the concerns of user's privacy and efficiency.**

Index Terms—***AES; BLOWFISH; Privacy Preserving***

I. INTRODUCTION

The development of communication over internet has more positive impacts and benefits but one of the most negative impact on the development of technology is the tapping or theft of data. The AES algorithm[1] has faster computation time and increase data security from attack and leakage[1]. when compared with the performance of the AES algorithm with DES stated that the AES algorithm for deriving time consumption or use a smaller computational time compared with DES and AES algorithms produce a higher level of security than DES. AES assign Federal Information Processing Standards (FIPS) approved cryptographic algorithms used to protect electronic data [1]. Other algorithms are also frequently used in securing digital data is BLOWFISH algorithm examined the implementation of the BLOWFISH algorithm on comparison computing speed and power consumption for some kind of symmetric algorithms are DES algorithm. The results showed that the BLOWFISH algorithm is superior in terms of speed and power consumption, especially in the delivery of data over a network without cables or wireless. The results of the study revealed that the BLOWFISH algorithm has a very good level of security. In this paper we will combine the AES algorithm and BLOWFISH algorithm which is the Multilevel Encryption Technique in order to make the data more secured and efficient.

II. BASIC TERMS

A. Symmetric Algorithm

Symmetric algorithms or also called secret key algorithm is an algorithm which can be calculated from the encryption key encryption key and vice versa. Symmetric algorithm[1] also called conventional algorithms, which can be determined decryption key from the encryption key, in other words the encryption key and decryption key together. Symmetric algorithms can be classified into two types, namely stream ciphers and block ciphers[1]. Stream ciphers operate bits per bit (or byte per byte) at a time. While block ciphers operate per group groups of bits called blocks (blocks) at a time. People often use mathematical notation to simplify the writing and analysis, so that modern cryptography[2] is always associated with mathematics. With original message M and the secret code C obtained from the encryption key K, we can be written as follows:

C = Ek (P)

In the decryption process, do the reverse operation, and can be written as follows:

P = Dk (P)

The process of encryption and decryption can be illustrated in the figure below

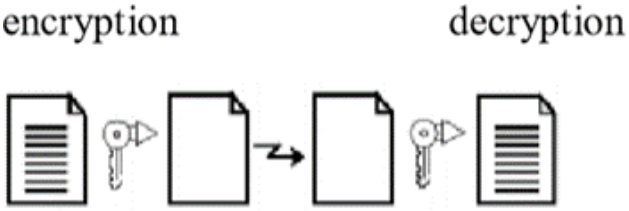

Fig.1.Encryption and Decryption process of symmetric algorithm

B. AES

Cryptographic algorithm AES (Advanced Encryption Standard) is a symmetric cryptographic algorithm. Input and output of the AES algorithm[2] consists of a sequence of 128 bits of data[3]. Cipher key of AES consists of a key with a length of 128 bits, 192 bits, or 256 bits[3].

AES-128 encryption is done as much as 10 times (a = 10), as follows

1. Addroundkey
2. Round as a-1 times, the process undertaken in each round are: SubBytes, ShiftRows, MixColumns, and

AddRoundKey.

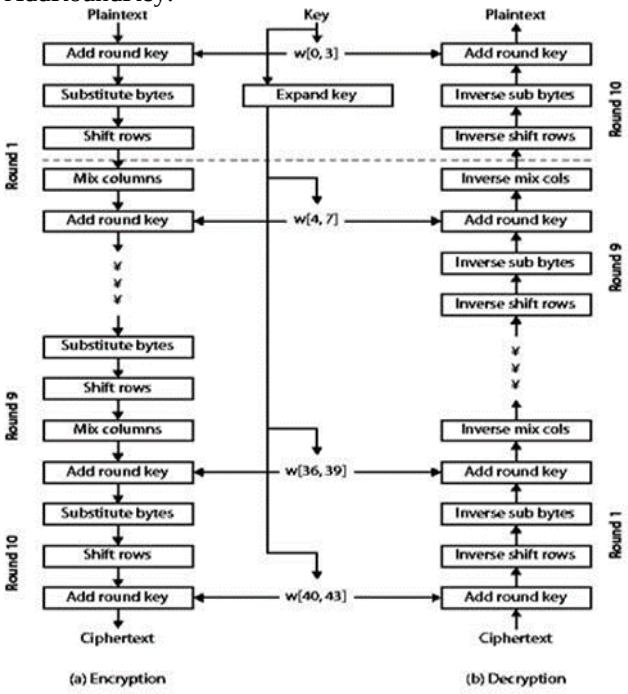

Fig.2. Working process of AES algorithm Process round

3. Final round, is the process for the last round which includes SubBytes, ShiftRows, and AddRoundKey.

While the AES-128 decryption process, the process of rotation is also done as much as 10 times (a = 10), as follows:

1. Addroundkey
2. The round as a-1 times, where in each round is done the process: InverseShiftRows, Inverse SubBytes, AddRoundKey, and Inverse MixColumns.
3. Final round, is the process for the last round which includes InverseShiftRows, InverseSubBytes, and AddRoundKey.

In encryption and decryption of AES-192 round process done 12 times (a = 12), while for AES-256 round process done 14 times (a = 14).

C. *BLOWFISH*

BLOWFISH is a symmetric key algorithm[4], BLOWFISH is also a block cipher, which means that during The process of encryption and decryption Blowfish will divide the message into blocks of equal size in length. The length of the block for the BLOWFISH algorithm[4] is 64-bit. Explains that the BLOWFISH was created by a cryptanalyst named Bruce Schneier, president of Counterpane Internet Security, Inc. (Company consultant on cryptography and computer security) and published in 1994. Created for use on computers that have a large microposesor (32- bits up with a large data cache).

The size of a block algorithm Blowfish length is 64 bits or 8 bytes. Key lengths ranging from 32 bits or 4 bytes to 448 bits or 56 bytes. Using as many as 16 rounds Feistel Cipher. BLOWFISH algorithm[5] has a P-array of size 18 each of which contains a 32-bit subkey, and four SBox with 256 entries[13]. Blowfish encryption process consists of a simple function iteration (Feistel Network) as many as 16 rounds (iterations), is a 64-bit input data element X.

Each round consists of a key-dependent permutation and substitution key- and data-dependent. All operations are addition (addition) and XOR on 32-bit variable. An additional operation is only four tables searches indexed array for each round. The steps are as follows.

1. For X into two parts, each of which consists of 32bits: XL, XR.
2. For i = 1 to 16 XL = XL XOR pi XR = F (XL) XOR XR Swap XL and XR
3. After iteration sixteen, exchange XL and XR again to perform Undo the last exchange.
4. Then do XR = XR XOR P17 XL = XL XOR P1 5.Last , merge back XL and XR to get cipher text.

III. PROPOSED SYSTEM

ENHANCED ALGORITHM

The proposed enhanced AES is the improved form of existing AES algorithm. In proposed AES algorithm, to encrypt large amount of data, segmentation is done before encryption and after the decryption while transmission. The key expansion is also done to improve the security of the AES. Moreover, the nine rounds is completed in three blocks. This process is called pipelining which increase the operating speed of the entire system.

The algorithm for the enhanced AES is as follows:-

Step 1:- Input Data Matrix (d).

Step2:- Data Matrix Validation ・validate(d)・dM

Step3:-Data Matrix Segmentation ・segment((d M))・d mi

Step 4:- Input Security Key(Sk)

Step 5:- Key Expansion(Sk)

Step 6:- Initial Round ・AddRoundKey (Sk)

Step7:- Rounds For Loop

- SubBytes (d mi)
- ShiftRows (dmi)
- MixColumns (dmi)
- AddRoundKey(dmi)

Step 8:- Rounds

- End For Loop

Step 9:-Final Round

- MixColumns (False)
- SubBytes(dmi)
- ShiftRows (dmi)

- AddRoundKey (dmi)

Step 10:- Data Matrix Merger

- merge(dmi)
- dEM

Step11:-Data Matrix Reverse Validation — rvalidation (dEM)-dE

To encrypt 128 bit blocks of data. Data is fed as an input to the system. The Enhanced AES is combined with validation and segmentation algorithm. So the created data matrix (d) will be validated. As the amount of data to be entered into the system is validated using validation algorithm. After this, matrix will be segmented (dM) into fragments. This segmentation is done to increase the operating speed of the system. Now the secret key (Sk) is input which is used to encrypt or decrypt the data. After inputting the secret key, key expansion is done. This key expansion will make the AES algorithm more secure. Now the initial round AddRoundKey (Sk) will be performed. The nine rounds are divided into three parts, means every three parts will be processed as one block and these three blocks will complete the all nine rounds. After the completion of rounds the data matrix will be merged (dEm) and then data matrix reverse validation will be done. At the last we will get encrypted text. Then the blowfish algorithm is implemented in the encrypted text and decrypted as same as the encryption method.

IV. COMPARISON OF ALGORITHMS

TABLE -1: COMPARISON OF ALGORITHMS

Algorithm	Block Size	Rounds	Key
AES	128,192,256 Bits	10,12,14 Rounds	128 Bits
BLOWFISH	32-448 Bits	16 Rounds	64 Bits

The calculation for Encryption and Decryption speed of each algorithm for different packet sizes is done. Their implementation has tried to optimize the maximum performance for the algorithm[14]. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme The performance metrics are analysed by

(a) Encryption/decryption time.
(b) CPU process time

Table -2: Comparison of algorithms with respect to time in seconds

Algorithm	Encryption/decryption For 64 bits	CPU Time
AES	1.261816	1.54440990
BLOWFISH	0.850568721	0.07800050

Chart -1: Comparison of AES and Blowfish

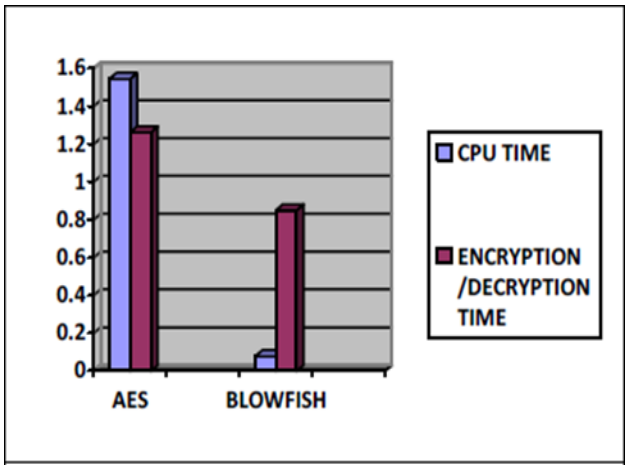

TABLE -3: COMPARISON OF ALGORITHMS

Parameters	DES	3DES	AES	Blowfish
Published	1977	1998	2001	1993
Developed by	IBM	IBM	Vincent Rijmen, Joan Daeman	Bruce Schneier
Algorithm Structure	Feistel	Feistel	Substitution Permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
Key Length	56 bits	112 bits, 168 bits	128 bits, 192 bits and 256	32 –448 bits
Flexibility or Modification	No	YES, Extended from 56 to 168 bits	YES, 256 key size is multiple of 64	YES, 64-448 key size in multiple of 32
Number of Rounds	16	48	10, 12, 14	16
Block size	64 bits	64 bits	128 bits	64 bits
Throughput	Lower than AES	Lower than DES	Lower than Blowfish	High

Level of Security	Adequate security	Adequate security	Excellent security	Excellent security
Encryption Speed	slow	Very slow	Fast	Fast
Effectiveness	Slow in both software and hardware	Slow in software	Effective in both software and hardware	Efficient in software
Attacks	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack

V. EXISTING SYSTEM

The existing system uses the attribute based encryption technique[11]. In order to protect the privacy of users and improve the efficiency of encryption, we propose a secure medical data sharing system, where sensors and mobile terminals can encrypt sensitive data of users, then send it cloud servers. And users who can satisfy access control structure can access data in this system. The contribution of this article is mainly three points below.

(a) Firstly, in our security system, when cipher text is uploaded to the cloud server, the access control structure will also be uploaded. If the attribute matching function is removed, attributes will be hidden into the access structure. The access control structure will also leakage user privacy. By using the attribute bloom filter (ABF), we can hide in the entire attributes in the anonymous access control structure. To this end, the data stored on the cloud server will be protected.

(b) Secondly, to generate the cipher text more quickly, we use online/offline encryption technology. Before the encrypted information is known, a large amount of work that is needed at the encryption stage will be done. When the encrypted information is known, the cipher text can be generated quickly. To this end, the efficiency of encryption will also be solved.

- Finally, in our scheme, the initialization stage of the system does not need to specify all attributes. When the overall attributes of the system users increase, the system does not need to be reinitialized, which will is also away to improve the efficiency.

VI. PROPOSED ARCHITECTURE

A. System Architecture

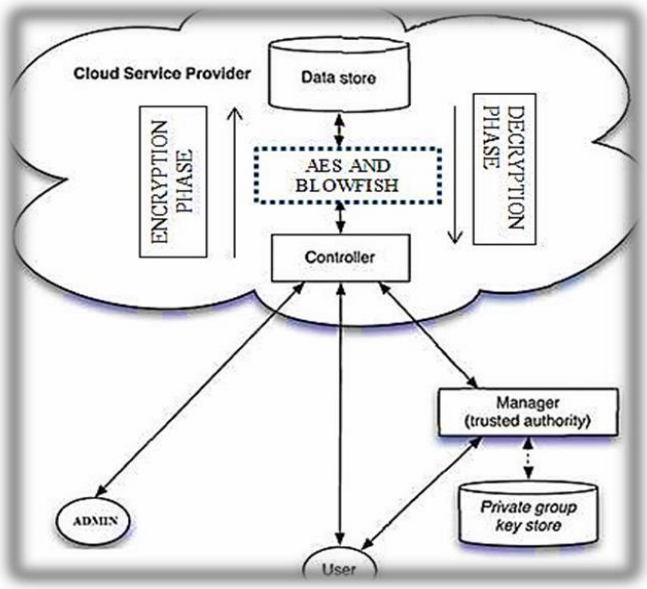

Fig.3. Architecture of Multilevel Encryption Technique

In this proposed architecture of Multilevel Encryption technique, the entire process is stored in a cloud based Database system. There are three entities named Admin, User, Manager (Trusted authority) is functioned under the main controller which manages the overall activities of them. The encryption and decryption process takes place between the controller and database where the data is saved in the encrypted format and retrieved after the decryption process. This process makes the data secured in multilevel techniques since we use AES[6] and BLOWFISH algorithm in the encryption and decryption stage.

B. Proposed Encryption Architecture

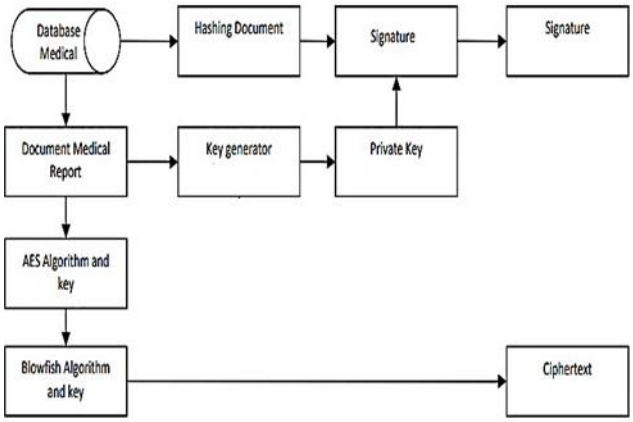

Fig.4 The Proposed Encryption Architecture

It is a proposed multilevel encryption process, medical record data will be encrypted using AES and Blowfish, follows the process used: Generate data of medical record into a format portable document file (PDF), Apply a hashing document with the method of AES 256 resulting signature, Generate a private key by Encryption[7] of patient's medical record file with AES and Blowfish uses key,

Sends files,

(1) encrypted file
(2) encrypted key and
(3) the signature to the recipient.

C. The Proposed Decryption Architecture

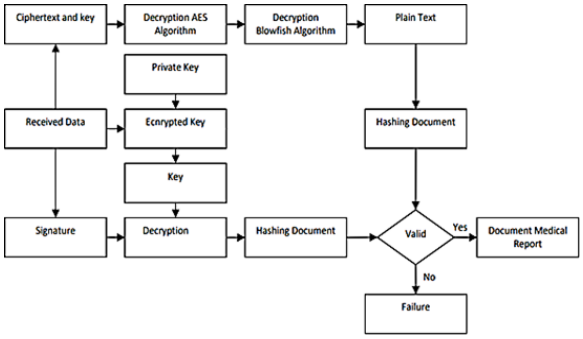

Fig.5 The Proposed Decryption Architecture

It describes the multilevel decryption process proposed, patient record data which has been already encrypted[8] will be decrypted again so that it can be read by the recipient, the following decryption process:

The recipient will receive a three-block file password:

(1) block key
(2) signature block and
(3) the encrypted file

Implement private key, apply the private keys to open the file signature. Enter AES[8] key and Blowfish key to unlock the encryption file so that it results Hashing document file. Then it is compared with the result of hashing signature by hashing the document, if it works then your medical record file will perform normally. If not, then the files will appear in encrypted.

D.Modules

1. AUTHENTICATION MODULE

This module makes the normal user to login if the user not registered already they can sign up and login, this process will be operated by admin.

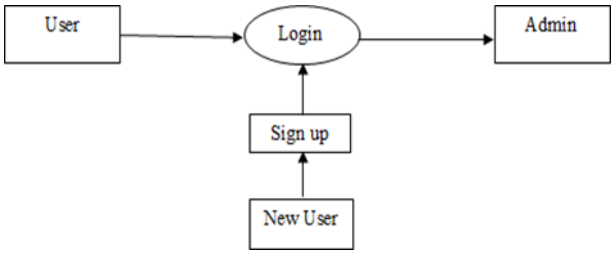

Fig.6. Login

2. THIRD PARTY OWNER MODULE

This module helps the doctor to approve the request given by the patient, admin handles the patient registration process, generate OTP and makes the patient to view the report.

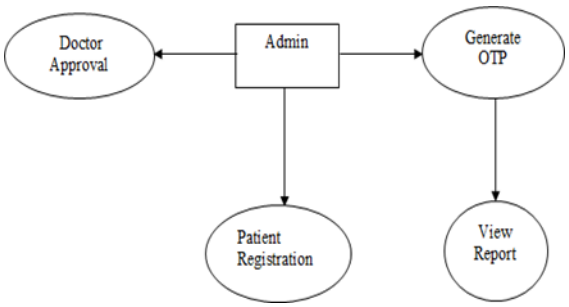

Fig.7. Data owner design

3. PATIENT RECORD MODULE

This module is the patient record module were patient can give appointment request, wait for the admin to generate OTP and to view the report.

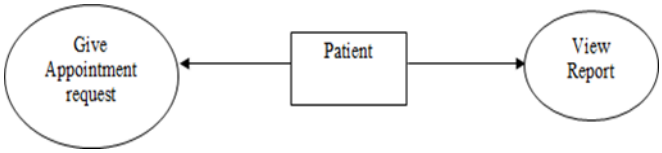

Fig.8. Patient Access

4. DOCTOR ACCESSING MODULE

This module is used to accept the appointment request and emergency case then doctor will generate OTP and makes the patient to view the report.

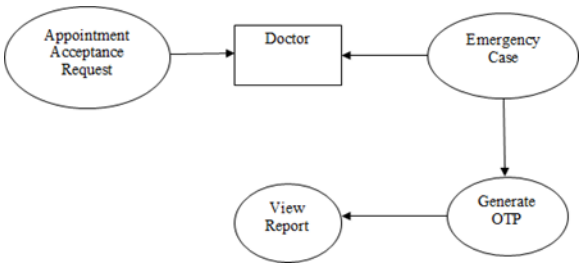

Fig.9. Doctor Access

5. PDF ENCRYPTION MODULE

In this module the patient's record is generated as Pdf file format and it is encrypted. Then the key is generated and a private key is sent as signature.

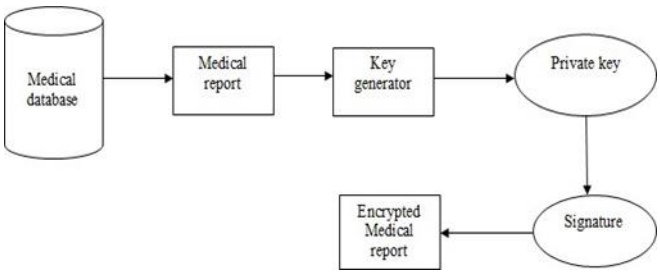

Fig.10. Pdf Encryption process

6. PDF DECRYPTION MODULE

In this module, the generated patient's record will be decrypted and the patient can access the report.

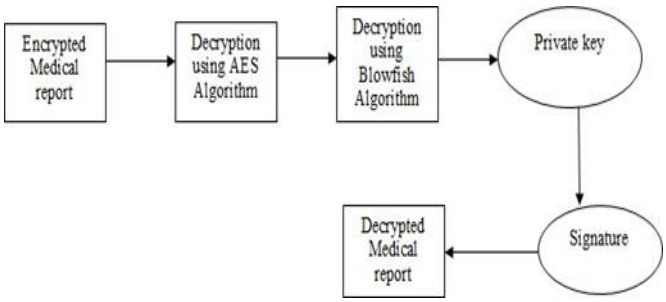

Fig.11. Pdf Decryption process

VII. EXPERIMENTAL RESULTS

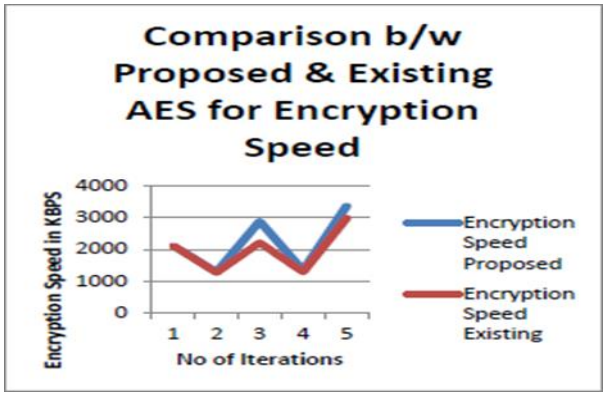

Fig.12. Encryption Speed comparison between Enhanced and existing algorithm.

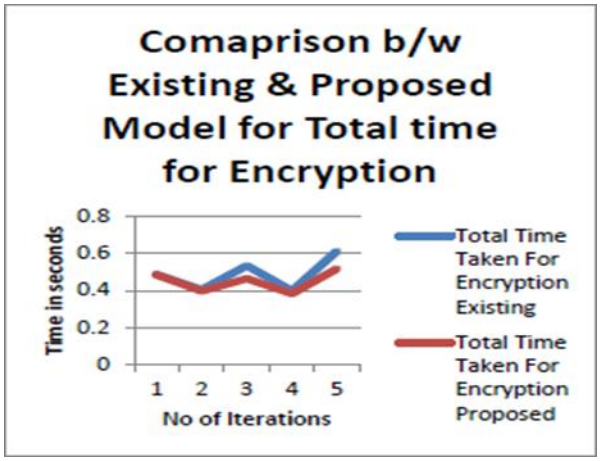

Fig.13.Comparison between Existing and Enhanced model for total time taken for encryption.

TABLE 4: ENCRYPTION SPEED BETWEEN EXISTING AND ENHANCED AES.

ENCRYPTION SPEED	
ENHANCED	EXISTING
1292.6	1265.4
2880.5	2207.6
3350.2	2973.5

TABLE 5: COMPARISON BETWEEN TOTAL TIME TAKEN FOR ENCRYPTION.

TIME TAKEN FOR ENCRYPTION	
EXISTING	ENHANCED
0.404559	0.396174
0.533234	0.463851
0.611303	0.516567

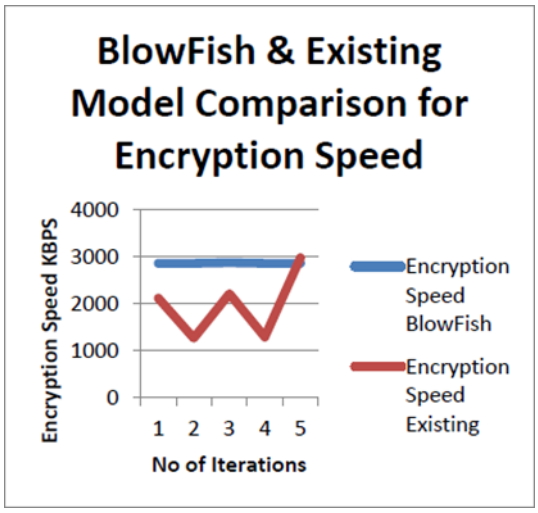

Fig.14. BlowFish & Existing Model Comparison for Encryption Speed

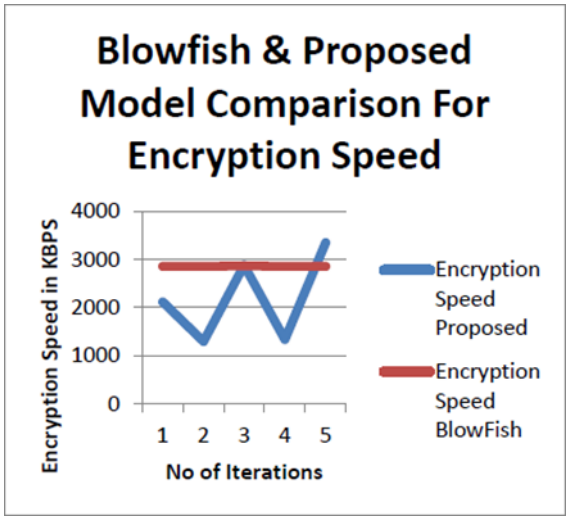

Fig.15. BlowFish & Enhanced Model Comparison for Encryption Speed

.

TABLE 6: TABLE SHOWING ENCRYPTION SPEED COMPARISON BETWEEN BLOWFISH AND EXISTING AES TABLE.

ENCRYPTION SPEED	
BlowFish	**EXISTING**
2855.210611	1265.4
2869.677519	2207.6
2854.997706	1286.8

TABLE 7: ENCRYPTION SPEED COMPARISON BETWEEN BLOWFISH AND ENHANCED AES TABLE.

ENCRYPTION SPEED	
BlowFish	**ENHANCED**
2855.210611	1292.6
2869.677519	2880.5
2854.997706	1338

VIII. CONCLUSION

In this paper, an Enhanced AES has been proposed which will be more secure and good in performance as compared to existing AES. The data to be encrypted is pipelined to increase the speed and time to encrypt the text data. AES is combined with Validation and Segmentation. Key Expansion is done to make the data more secure. Also, the blowfish is compared with this enhanced version of AES. But as a result the BlowFish is fast and more secure encryption algorithm as compared to the proposed AES. The future scope of this project can be that the AES can be made more secure and reliable and can be made faster and good than blowfish algorithm. By using the of AES algorithm and BlowFish algorithm the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices and processing time is reduced. Multilevel data encryption technique reduces the theft of data by performing secret key formation in the relevant data field.

REFERENCES

[1] Dong Zheng, Axin Wu, Yinghui Zhang, Qinglan Zhao, " Efficient and Privacy-Preserving Medical Data Sharing in Internet of Things With Limited Computing Power ", IEEE Transaction, Vol 6, 2018.

[2] Joan Daemen, Vincent Rijmen, "The Rijindael Block Cipher-AES Proposal ",Vincent Rijmen Katholieke Universiteit Leuven, 2001.

[3] Douglas Selent, "Advanced encryption standard ", Rivier academic journal, Vol 6, no. 2, 2010.

[4] Padate R & Patel A, "Encryption and decryption of text using AES algorithm", International Journal of Emerging Technology and Advanced Engineering, 2014.

[5] Ashwak A Labaichi, Faudziah Ahmad , "Security Analysis of Blowfish algorithm", Information Technology Department University Utara Malaysia Kedah, 2013.

[6] Rajan Patel and Pariza Kamboj, "Security Enhancement of Blowfish Block Cipher", Faculty of Technology, RK University, Rajkot 360020, Gujarat, India, 2016.

[7] Faheem Gul, Aaqib Amin, Suhail Ashraf, "Enhancement of Cloud Computing Security with Secure Data Storage using AES ", IJCSMC , 2016.

[8] B.Anjani Kumar, G.Jaswanth Varma, Fazal Noorbasha, Harikishore Kakarla, M. Manasa, "Data encryption and decryption cryptography using AES algorithm ", International Journal of Pure and Applied Mathematics , 2017.

[9] Muhammad faheem musta,Sapiee Jamel, Abdulkadir Hassan Disina, "A Survey on the Cryptographic Encryption Algorithms ",IJACSA, Vol 8,no. 11,2017.
[10] Garcy C.Kessler, "An Overview of Cryptography", Handbook on Local Area Network, Vol.10, No.24, pp- 234-240, 2016.
[11] E. Thambiraj,G. Ramesh,Dr. R. Umarani , "A survey on Various Most Common Encryption Technique " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012,pp226-233 I.S.
[12] MilindMathur, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", National Informatics Center Network NICNET, Vol. 1, No.3, pp. 143-148, 2013.
[13] S. Manku and K. Vasanth, "Blowfish encryption algorithm for information security," ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 10, pp. 4717–4719, 2015.
[14] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," International Conference on Information and Communication Technologies, pp. 84–89, 2005