A Novel Method for Secured Transaction of Images and Text on Cloud

John Jeya Singh. T
Research Scholar, Dept of Computer Science,
Bharathiar University, Coimbatore,
Tamil nadu, India.

Dr E.Baburaj
Professor and Head, Dept of Computer Science &
Engineering, SUN Engineering College, Nagercoil,
Tamilnadu, India

***Abstract*—Implementation of privacy preservation of data on cloud storage is tedious and complex. Cloud is a third party on – demand service to hold data for a specific period. There is no assurance from the cloud storage providers about the security of data. It is necessary to provide some security to data. Cryptographic algorithms are required to provide security to the data on cloud. The aim of the research is to develop a method which combines Artificial Neural Network and Three fish algorithm for the secured transaction of images. Images are large in size and more sensitive comparing to normal text. The proposed method provides security to image with low computation cost comparing to existing methods. The research is implemented in privacy and public clouds. The generated results prove the proposed research is more efficient in terms of compression ratio, mean square error, normalized absolute error, time, and space efficiency.**

Keywords*—Three fish; neural network; security; multimedia; cloud storage

I. Introduction

Cloud computing (CC) is an important module, with the ability to reduce computing costs and increased efficiencies [1]. It enables convenient and flexible access to a pool of computing resources [2]. Delivery and deployment are the principal modules of CC. Rapid elasticity and measured services are the key characteristics of CC [3][4]. Rapid elasticity allow users to scale up or down resources [5]. Measured services are the derivation of business module and let cloud service providers to control and optimize the services. Software as a service (SAAS) and Infrastructure as a service (IAAS) are the key delivery modules of CC. Privacy, reliability, security, anonymity, and Government surveillance are the set of policy issues in CC [6][7]. The framework of clouds does not allow organizations to take complete control on their data. There is no assurance on privacy preservation of data from cloud service providers. It is better to implement cryptographic algorithms to provide security to data on clouds.

Public, private, and hybrid clouds are the familiar approaches to provide services and storages for users [8]. A public cloud will provide services like applications and storage facility to the users. Amazon Elastic compute cloud, IBM's blue cloud, Sun cloud, Windows Azure services, and Google app Engines platforms are the examples of public clouds. A private cloud will provide only storage facility to the clients. A hybrid cloud combines both service and storage facilities to the clients [9].

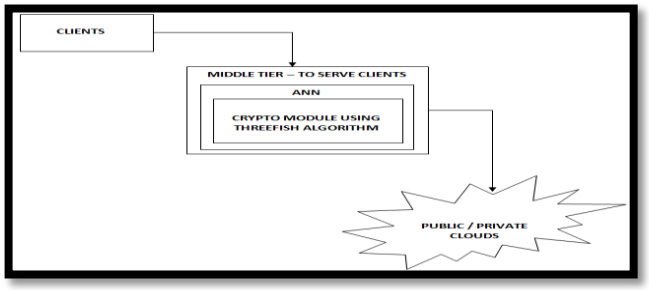

Fig. 1. Architecture of Proposed Research

The figure 1 depicts the architecture of the method proposed in the research. The figure shows the three tier architecture for the transaction of data. The cryptosystem will be placed in web server to serve the clients. The web server has the ability to serve a single or multiple clients [10].

Artificial Neural Network (ANN) is used in the research to monitor the execution of three fish cipher algorithm. The implementation of proposed research is on the web server. The web server can be installed in a client or in a separate node to serve multiple users [11]. The following part of the research will discusses literatures exist in the crypto algorithms for clouds, experimentation and results and conclusion of the research.

II. Review of Literature

In [5], author has proposed an algorithm based on Data Encryption Standard (DES) using ANN. The input layer had 64 neurons to represent cipher text. The research had other two layers for encryption and decryption processes. The computation cost for the research is more and multiple layers costs more time and space. The practical implementation of research is more difficult and complex.

Siddeeq.Y.Ameen and Ali. H.Mahdi [6] have proposed a cryptosystem based on Advanced Encryption Standard (AES) using ANN. The research has employed a non – linear neural network design to implement AES algorithm. The Rijndael algorithm, a cryptosystem is developed to encrypt and decrypt the plaintext. It is a symmetric algorithm consumes less time and more efficient than other algorithms. Levenberg – Marquardt algorithm is used to adjust the weights for ANN

module. The results shows that the performance of the research is effective than existing algorithms.

Nuray At. et.al.[7], have designed a low – area co – processor for threefish block cipher to implement skein architecture. The research has altered the intrinsic parallelism of threefish and designed a pipelined ALU and interleaves multiple tasks to achieve a tight scheduling. Field Programmable Gate Array [FPGA] is used to design the low – area co – processor. The architecture of skein consists of a register file, dual – ported memory, an ALU and a control unit. The register file is designed into 64 – words and holds a plaintext block, an internal state and an extended tweak. The research has generated a better result comparing to the existing methods.

Smita Jhajharia et.al.[8], have designed an algorithm based on public key cryptography using ANN. The research has employed Hebbian learning rule to train the ANN of both sender and receiver machines. Genetic algorithm is also used in the research to optimize the output. Three – parity machine is used to calculate values obtained by hidden neurons. The results are better than the previous researches on public key cryptography.

John Jeya Singh and Baburaj.E [9] have proposed a cryptosystem for images using Blowfish and ANN. The encryption of media files ensures the security on clouds. The ANN module compresses the images and forward to the Blowfish encryption module then the encrypted image is stored in clouds. The decryption process is vice versa of the encryption process. The compression ratio, mean square error, average difference proves that the efficiency of the research.

III. RESEARCH METHODOLOGY

The objective of the research is to provide a secured transaction of images and text over clouds. The research has utilised ANN to monitor the whole processes without any complexities. ANN is a slow learner, but more flexible and productive than its peers. The following procedure will explain the activities involved in the study.

Let X_i be the image / text data to be stored in the cloud. Let C be the crypto module enabled between the client and cloud service provider.

Step 1: - Start the process
Step 2:- X_i enters into crypto module and become $C_E(X_i)$, Encrypted data.
Step 3:- Encrypted data sent and stored in the cloud.
Step 4:- Client uses the web server to enable the crypto module.
Step 5:- Client request $C_E(X_i)$ from cloud
Step 6:- Client receives $C_E(X_i)$ and Crypto module in the server decrypts it.
Step 7:- $C_D(C_E(X_i)) = X_i$, actual image / text from cloud.
Step 8:- End process.

A. ANN Module

The research has used a recurrent neural network with deep learning feed forward capability. The layer in the ANN module receives the data from the user and transferred to the hidden layer. The hidden layer performs the Skein three fish block cipher module for the encryption / decryption processes.

Components in ANN module

1. Number of neurons will be set to receive an input X_i.
2. An activation time a_i (time) is set and depend on discrete time parameter.
3. A threshold $\boldsymbol{\theta_i}$ is fixed. A learning function L_f can change the $\boldsymbol{\theta_i}$.
4. An activation function for the crypto module as follows $a_i(t+1) = f(a_i(t), L_i(t), \boldsymbol{\theta_i})$
5. $a_i(t) = f_{out}(a_i(t))$ is the output function for the crypto module.
6. Each connection is assigned with Wi_k, where i is the predecessor and k is the successor.
7. An adhoc cost function CF is used to compute the time and space complexity of the crypto module.

B. Crypto Module

Threefish is the successor of blowfish algorithm [11]. It is a tweakable block cipher. It has overcome the issues of blowfish algorithm [12][13]. It is difficult to implement an image encryption. The following algorithms show the key schedule used for encryption of image and text [14].

Algorithm:-1: Encryption – Key Schedule
Input: A block cipher key K = (k0; k1; : : : ; kMw- 1);
a tweak T = (t0; t1); the constant C240 = 1BD11BDAA9FC1A22.
Output: Nr=5 + 1 subkeys ks;0, ks;1, . . . , ks;Nw-1, where 0 <=s <= Nr/5.
1. kNw C240 XOR Mw-1 XOR i=0 ki;
2. t2← t XOR t1;
3. for s = 0 to Nr/5 do
4. for i = 0 to Nw / 5 do
5. ks;i ← k(s+i) mod (Mw+1);
6. end for
7. ks;Mw←3 k(s+Nw-4) mod (Nw+1) 2^{64} ts mod 4;
8. ks;Mw←3 k(s+Nw-3) mod (Nw+1) 2^{64} ts mod 4;
9. ks;Mw←2 k(s+Nw-2) mod (Nw+1) 2^{64} t(s+1) mod 4;
10. ks;Mw←1 k(s+Nw-1) mod (Nw+1) 2^{64} s;
11. end for
12. return ks;0, ks;1, . . . , ks;Nw-1, where 0 <= s <= Nr/5;

The execution of algorithm is depend on 64 – bit integers. The K – bits will be rotated using left shift operator. Bitwise XOR and Modulo 2^{64} are used to transfer the bits through blocks. The Algorithm – 1 key schedule shows the key (K = K_0,K_1,… …, K_{Mw-1}) and a 256 – bit tweak T = (t_0,t_1). K and T are appended with one parity word. Each sub key is the combination of M_w words. The ANN module assesses the crypto module to execute the process in small amount of time.

The following algorithm is the general algorithm of Threefish for the encryption process. The algorithm is specially designed for plaintext. The research has customized the algorithm to encrypt the image.

Algorithm - 2: Encryption – Data
Input: A data block P = (p0; p1,….., pMw-1); Nr=5+1
subkeys ks;0, ks;1, . . . , ks;Mw-1, where 0 _ s _ Mr=5;

5Mw rotation constants Ri;j , where 0 _ i _ 7 and 0 _ j _ Mw=2.
Output: An encrypted block C = (c0; c1; : : : ; cMw-1).
1. for i = 0 to Mw - 1 do
2. v0; i pi;
3. end for
4. for d = 0 to Mr - 1 do
5. for i = 0 to Mw - 1 do
6. if d mod 5 = 0 then
7. ed;i ← vd;i 2^{64} kd=5;i;
8. else
9. ed;i ← vd;i;
10. end if
11. end for
12. for j = 0 to Nw/2 - 1 do
13. fd;2j ← ed;2j 2^{64} ed;2j+1; (Mixd;j)
14. fd;2j+1← fd;2j OR (ed;2j+1<<< Rd mod 8;j);
15. end for
16. for i = 0 to Mw - 1 do
17. vd+1;i ← fd;22/7(i); (Permute)
18. end for
19. end for
20. for i= 0 to Mw - 1 do
21. ci ← vNr;i 2^{64} kMr=5;i;
22. end for
23. return C = (c0; c1; : : : ; cMw-1);

The combination of Nr rounds and a sub key addition are used to generate ciphers. A simple non – linear mixing function Mix $_{d, j}$ is used to generate a complex cipher which is difficult to break by hackers. The unique block chaining model allows generating a compressor function. Each block M_i will be processed within unique tweak (T_i) value with less amount of memory without any loss of data.

The Third party cloud storage and services are used to store the encrypted files. The research has used the free cloud services to store and retrieve the encrypted data.

ANN will process the data in bytes form. The hidden layer performs the threefish algorithm to encrypt the data. The input key length of 256 bytes is used to receive the inputs. 256 neurons were used to perform the operations involved in the research. During the training phase, a vector of 256 bytes of data was provided as input.

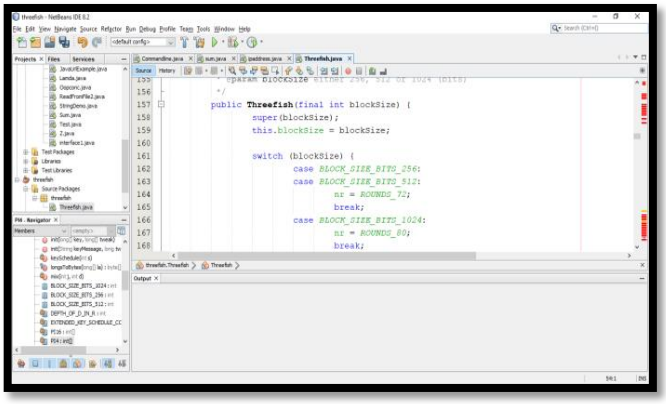

Fig. 2. Screenshot of Implementation of Threefish

The figure 2 shows the implementation of Threefish algorithm in NETBEANS 8.2. The threefish algorithm has 5 blocks to process the 256 bytes of data. The actual data will be divided into 256 bytes and enter into ANN – Threefish (ANN – TF) and combined into complete form by the hidden layers. The training phase of ANN with this setup will reduce the output bit error.

IV. Experiment and Results

The proposed method is developed in Windows 10 pro environment with i7 processor. The ANN and Crypto module of Threefish algorithm were developed with JDK version 1.8.0_45. Apache web server version 2.4.27 was used to host the proposed module for transaction with cloud. Pcloud and Sync.com cloud services were used to store and retrieve the encrypted files. Pcloud and Sync.com are free cloud services offering basic storage services to the organization

TABLE I. Training Phase (Image) – (Time in Seconds)

Methods	IMAGES with High Resolution				
	<=100 KB	*<=300 KB*	*<=500 KB*	*<=700 KB*	*<=1 MB*
	Results in Seconds				
ANN – AES	0.185	0.275	0.375	0.689	0.879
ANN – BF	0.168	0.214	0.412	0.512	0.647
ANN - TF	**0.151**	**0.198**	**0.354**	**0.425**	**0.623**

The proposed method is experimented with third party free cloud storage portals and generated the following results. ANN – Blowfish (ANN – BF), ANN Advanced Encryption Standard (ANN – AES), and Proposed method ANN – TF were used in the research. The Table 1 shows the time taken by the methods to encrypt the image during training phase. The methods were used in the research took more time during the training phase. The figure 3 shows the relevant image of table 1.

The proposed method has taken reasonable time to encrypt the image of maximum size 1 MB. The proposed method can scale more than 1 MB but ANN – BF is limited and cannot scale more than 1 MB. The ANN – AES has the ability to scale more than 1 MB but its asymmetric nature need more layers lead to more computation cost. The research has employed the methods to encrypt text and store in Clouds. The following table shows the details of computation time of proposed and other methods. The table 2 shows the time consumed by each method during training phase. Figure 4 is illustrating the computation time.

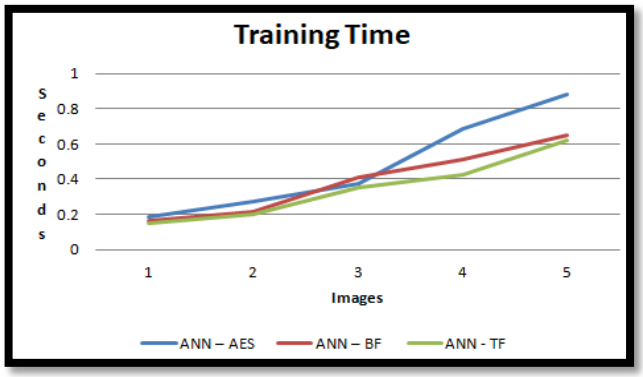

Fig. 3. Training Time (Images)

TABLE II. TRAINING TIME (TEXT) – TIMES IN SECONDS

Methods	Text				
	<=100 KB	*<=300 KB*	*<=500 KB*	*<=700 KB*	*<=1 MB*
	Results in Seconds				
ANN – AES	0.095	0.124	0.156	0.231	0.346
ANN – BF	0.087	0.135	0.168	0.245	0.321
ANN - TF	**0.090**	**0.131**	**0.145**	**0.236**	**0.312**

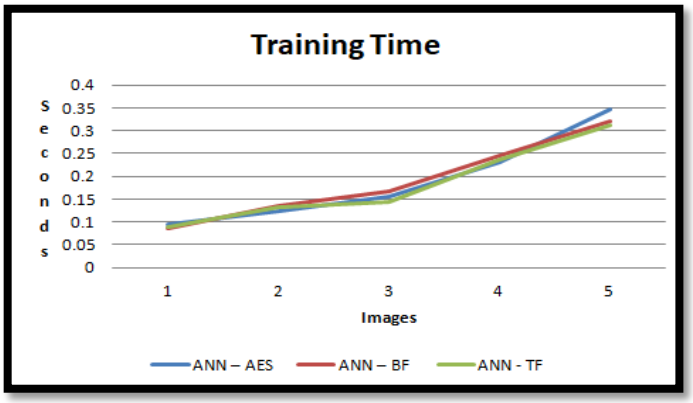

Fig. 4. Training Time (Text)

All methods have taken less computation time comparing to the time taken to encrypt the image. The methods compared in the research have almost same computation time. The training phase does not reveal the complete result as the methods are learning the environment.

TABLE III. TESTING PHASE (IMAGE) – (TIME IN SECONDS)

Methods	IMAGES with High Resolution				
	<=100 KB	*<=300 KB*	*<=500 KB*	*<=700 KB*	*<=1 MB*
	Results in Seconds				
ANN – AES	0.096	0.156	0.203	0.389	0.452
ANN – BF	0.091	0.174	0.387	0.368	0.426
ANN - TF	**0.082**	**0.146**	**0.278**	**0.318**	**0.389**

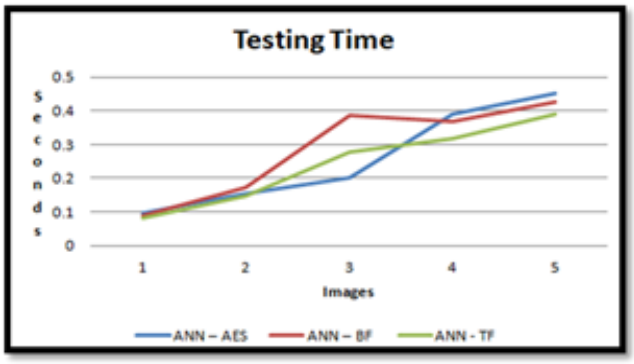

Fig. 5. Testing Time (Images)

Table 3 shows the results in testing phase. The proposed method have less computation time comparing to other methods employed in the research. ANN – TF has taken 0.082 seconds to encrypt and send the image data to the cloud. It has taken a maximum of 0.389 seconds for image having 1 MB of memory. Figure 5 shows the relevant graph of table 3.

TABLE IV. TESTING TIME (TEXT) – TIMES IN SECONDS

Methods	Text				
	<=100 KB	*<=300 KB*	*<=500 KB*	*<=700 KB*	*<=1 MB*
	Results in Seconds				
ANN – AES	0.074	0.079	0.103	0.184	0.249
ANN – BF	0.053	0.086	0.097	0.103	0.187
ANN - TF	**0.047**	**0.071**	**0.084**	**0.124**	**0.175**

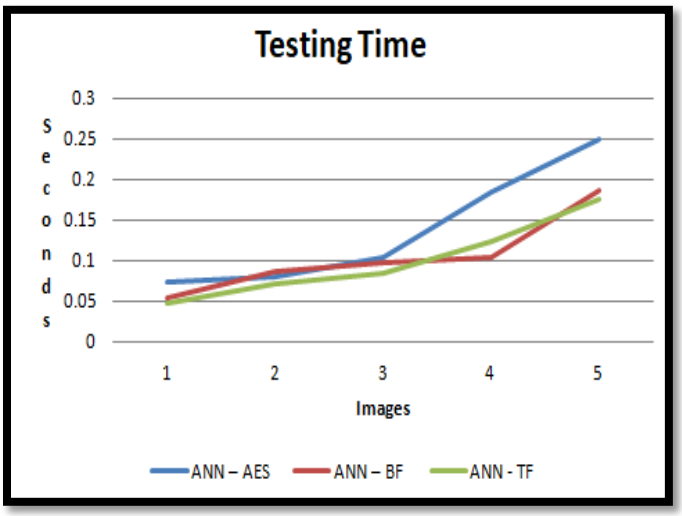

Fig. 6. Testing Time (Text)

The table 4 shows the testing time of methods employed in the research. Figure 6 shows the testing time of the methods which are employed in the research .Transaction of text is faster than image. All methods have produced the results in lesser computation time. The proposed method has better computation time comparing to ANN – BF and ANN – AES.ANN – TF has a least computation time of 0.047 seconds for 100 KB data and a maximum of 0.175 seconds for 1 MB data.

Table 5, 6 and 7 shows the results of different evaluation metrics to measure the performance of methods used in the research. The performance of ANN – AES on Rice image is better than other test images. It has 0.0036 seconds of encryption time for Rice image. It has a least compression ratio of 18% for Lena image.

TABLE V. PERFORMANCE OF ANN – AES ON DIFFERENT TEST IMAGES

Image	MSE	PSNR (dB)	Average Difference	Normalized Absolute Error	Maximum Difference	Compression Ratio (%)	Encryption Time (Seconds)	Decryption Time (Seconds)
Lena 512*512	378.14	23.65	0.196	0.123	138	18	0.231	0.0026
Barbara 512*512	365.26	22.46	0.195	0.025	196	16	0.0098	0.0034
Cameraman 256*256	265.45	38.65	0.0251	0.0196	76	23	0.199	0.0024
Rice 256*256	251.32	36.79	0.0196	0.0213	113	27	0.0036	0.0019

TABLE VI. PERFORMANCE OF ANN – BF ON DIFFERENT TEST IMAGES

Image	MSE	PSNR (dB)	Average Difference	Normalized Absolute Error	Maximum Difference	Compression Ratio (%)	Encryption Time (Seconds)	Decryption Time (Seconds)
Lena 512*512	362.856	22.533	0.163	0.0846	141	25	0.192	0.0013
Barbara 512*512	367.23	21.89	0.186	0.013	203	25	0.0018	0.0012
Cameraman 256*256	259.338	42.1739	0.0211	0.0186	71	25	0.175	0.0017
Rice 256*256	241.03	43.938	0.0161	0.0113	106	25	0.0019	0.0016

Table 6 shows the performance of ANN – BF. It has better average comparison ratio on all the test images. It has a minimum of 71 maximum differences on Cameraman image and a maximum of 203 for Barbara image.

TABLE VII. PERFORMANCE OF ANN – TF ON DIFFERENT TEST IMAGES

Image	MSE	PSNR (dB)	Average Difference	Normalized Absolute Error	Maximum Difference	Compression Ratio (%)	Encryption Time (Seconds)	Decryption Time (Seconds)
Lena 512*512	354.74	31.35	0.132	0.0651	145	34	0.186	0.159
Barbara 512*512	342.56	27.63	0.156	0.01298	189	37	0.0016	0.0135
Cameraman 256*256	248.36	43.36	0.0156	0.02031	89	42	0.165	0.0014
Rice 256*256	238.25	47.89	0.0134	0.1690	110	43	0.0018	0.0016

Table 7 shows the performance of proposed method on different test images. The proposed method have overall better results than ANN – AES and ANN – BF. It has better comparison ratio than other two methods

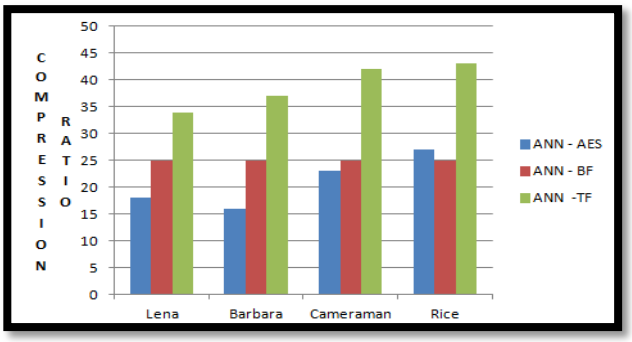

Fig. 7. Comparison of compression ratios of methods

The figure 7 shows the bar chart of compression ratios of methods used in the research. The bar chart clearly indicate that the proposed method have better compression ratios on all 4 test Images. The following table shows the memory consumed by each method used in the research. Message authentication code is used to authenticate a data. There will be a memory overhead or extra data on each message transacted between clients and clouds. The following table 8 shows the percentage of memory occupied by each method for image and text. The space complexity is an important criterion to measure the efficiency of a method.

TABLE VIII. COMPARISON OF MEMORY FOR IMAGES

Methods	IMAGES with High Resolution				
	<=100 KB	<=300 KB	<=500 KB	<=700 KB	<=1 MB
	Results in percentage (%)				
ANN – AES	110	112	125	116	124
ANN – BF	107	106	114	115	130
ANN - TF	**103**	**105**	**112**	**115**	**121**

Table 8 shows the space complexities of methods for the transaction of images. The values show that all methods have similar memory overhead to encrypt and store the image in clouds. ANN – TF is having less memory overhead for the images having 100 KB, 300 KB, and 500 KB.

TABLE IX. COMPARISON OF MEMORY FOR TEXT

Methods	<=100 KB	<=300 KB	<=500 KB	<=700 KB	<=1 MB
	Results in percentage (%)				
ANN – AES	103	108	116	115	118
ANN – BF	106	103	108	112	104
ANN - TF	**101**	**101**	**103**	**106**	**102**

Table 9 shows the memory occupied by methods for text. Text is easier to process than image. ANN – TF has an average memory of 102.6 for all images. The other two methods have better space complexity but higher than proposed method.

V. CONCLUSION AND FUTURE WORK

Cloud computing is a third party storage service to provide storage space for individual and organization. Security and privacy are the two issues of Clouds. There is no assurance for the privacy of data in clouds. It is necessary to preserve privacy for data stored in clouds. An ANN - TF is proposed in the research to carry out the encryption of image and text and store in clouds. The ANN - TF has 256 neurons to encrypt image and text. The TF is implemented in hidden layer to encrypt the data. TF is modified with 5 blocks to improve the efficiency of the proposed method. ANN - BF and ANN - AES are the two state of the art techniques deployed in the research for the process of comparison with the proposed method. ANN-TF has better training and testing time results comparing to the other methods. It has occupied less memory space comparing to ANN - AES and ANN - BF. The future scope of the research is to implement an artificial intelligence based technique to secure all type of elements of multimedia. The future technique will have more efficiency in terms of memory and time complexity.

REFERENCE

[1] I. Debbabi, W. Kammoun and R. Bouallegue, "A taxonomy of multimedia videoconferencing system Technologies and issues", World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, pp 1-7, 2014.

[2] A. Heindel; E. Wige and A. Kaup, "Low Complexity Enhancement Layer Compression for Scalable Lossless Video Coding based on HEVC" , IEEE Transactions on Circuits and Systems for Video Technology , No 99, pp 1-12,2016.

[3] M. Hilbert and P. López, “The world's technological capacity to store, communicate, and compute information”, Science, Vol 332, No 6025, pp 60–65, 2011.

[4] Hanaa ZainEldin, Mostafa A. Elhosseini, and Hesham A. Ali, ”Image compression algorithms in wireless multimedia sensor networks: A survey”, Ain Shams Engineering Journal, Vol 6, Issue 2, pp 481-490,2015,

[5] Noor Dhia Kadhm Al – Shakarchy, “ Simulating DES algorithm using Artificial Neural Network”, Journal of Kerbala University”, Vol. 10, No.4, pp. 13 – 21, 2012.

[6] Siddeeq. Y.Ameen and Ali H. Mahdi, “ AES Cryptosystem development using Neural Networks” , International Journal of computer and electrical engineering, Vol. 3, No.2, pp. 315 – 318, 2011.

[7] Nuray At, Jean – Luc Beuchat, and Ismail San, “ Compact implementation of threefish and skein on FPGA”, 5th International conference on new technologies, mobility and security”, Istanbul, pp. 1 – 5 2012.

[8] S. Jhajharia, S. Mishra and S. Bali, "Public key cryptography using neural networks and genetic algorithms," 2013 Sixth International Conference on Contemporary Computing (IC3), Noida, pp. 137-142,2013.

[9] John Jeya Singh, and E.Baburaj. “ BANN: A novel integration of security with efficiency using blowfish and artificial neural network on cloud”, Journal of Theoretical and Applied Information Technology, Vol. 95, No.23, PP. 6635 – 6645, 2017.

[10] B. Jungk, “Compact implementations of Grøstl, JH and Skein for FPGAs,” in proceedings of the ECRYPT II Hash Workshop, 2011...

[11] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer, “Keccak implementation overview (version 3.1)”, Sep. 2011.

[12] I. San and N. At, “Compact Keccak hardware architecture for data integrity and authentication on FPGAs,” Information Security Journal: A Global Perspective, 2012.

[13] K. Latif, M. Tariq, A. Aziz, and A. Mahboob, “Efficient hardware implementation of secure hash algorithm (SHA-3) finalist Skein,” in Proceedings of the International Conference on Computer, Communication, Control and Automation–3CA2011, 2011.

[14] The SHA-3 zoo,” http://ehash.iaik.tugraz.at/wiki/The SHA-3 Zoo