Algorithm Design and Analysis for RSA and Blowfish Encryption using Fuzzy Logic

Amit Verma [1*], Karamjeet singh [1], Ranjeeta Kaushik,Bharti[2] Chhabra [3]

[1*] *Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[1]*M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[2 and 3]*Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

Abstract: In daily life, we use internet or access information from various sources. Some of the method requires us to sending our own information. The goal of the project is to explore the methods of encryption to improve some aspects of the existing algorithms, and find way to create better security. In the proposed work, encryption has been implemented on the text in order to make it secure. For that matter, encryption techniques such as RSA, Blowfish and combination of both are used. The RSA algorithm, allows a message sender to generate a public keys to encrypt the message and the receiver is sent a generated private key using a secured database. Blowfish algorithm has also been implemented as it is a very strong weapon against hackers and cyber-criminals. Blowfish uses a unique form of key generation. Blowfish generates a really large key (think of a very robust cereal box decoder ring), and this alone is a huge benefit to security. With the increase in speed of computer processing, Blowfish is able to create a much longer key so that it is much more difficult to try to hack the key value. Combination of both the algorithms has used which is known as Hybrid algorithm. These three algorithms have used for text encryption using Fuzzy logic. Training and testing of the uploaded data will be done using MATLAB simulation tool. Different parameters like Precision, Recall and F-measure will be calculated.

Keywords: *encryption, RSA, Blowfish, Fuzzy logic*

I. INTRODUCTION

One of the major challenges of sharing resources in a network data communication is its security. This premise is based on the following facts: once there is a connection established between computers they can share the resources, so security of data become critical[1]. Today's the use of exchanging digital images becoming very frequent due to the increasing growth in the network technology [2]. Protection of multimedia data, sensitive information (such as credit card, social security number and bank transactions) becomes very important. You can use a lot of encryption to protect confidential data from unauthorized access[3]. Therefore, in order to provide data security, a number of cryptographic techniques such as symmetric and asymmetric techniques are used [4]. A variety of non-symmetrical cryptographic techniques, are RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA (Digital Signature Algorithm)[5]. The process of encryption and decryption is provided below:

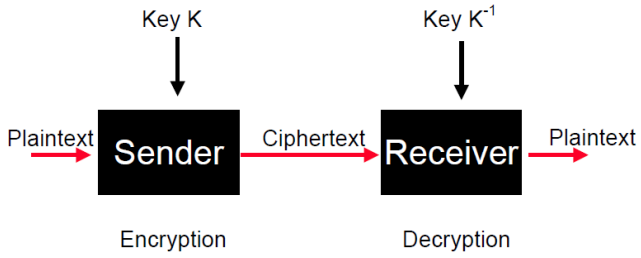

Figure 1: block diagram of encryption and decryption algorithm

In this research work, we propose a new method using fuzzy set theory to enhance the security. The data in the form of text to be transmitted is encrypted by using the RSA and blow fish algorithm [6]. The encryption algorithm is the mathematical procedure for performing encryption of data. A key is used to cipher a message and to decipher it back to the original message[7]. Then, the scrambled encrypted text is converted into the form of numeric by applying the fuzzy set theory [8]. The fuzzy logic will provide the text in the zero to one value. These numerical values before decryption are again converted into scrambled text. After this, if the key provided by the user is the same key that is used for the encryption then original data will be retrieved[9]. This paper, integrates the encryption of text and conversion of the unscrambled text from numerical to original by using fuzzy logic[10].

II. METHODOLOGY

Step 1**:** Firstly, Upload data that we want to encrypt.

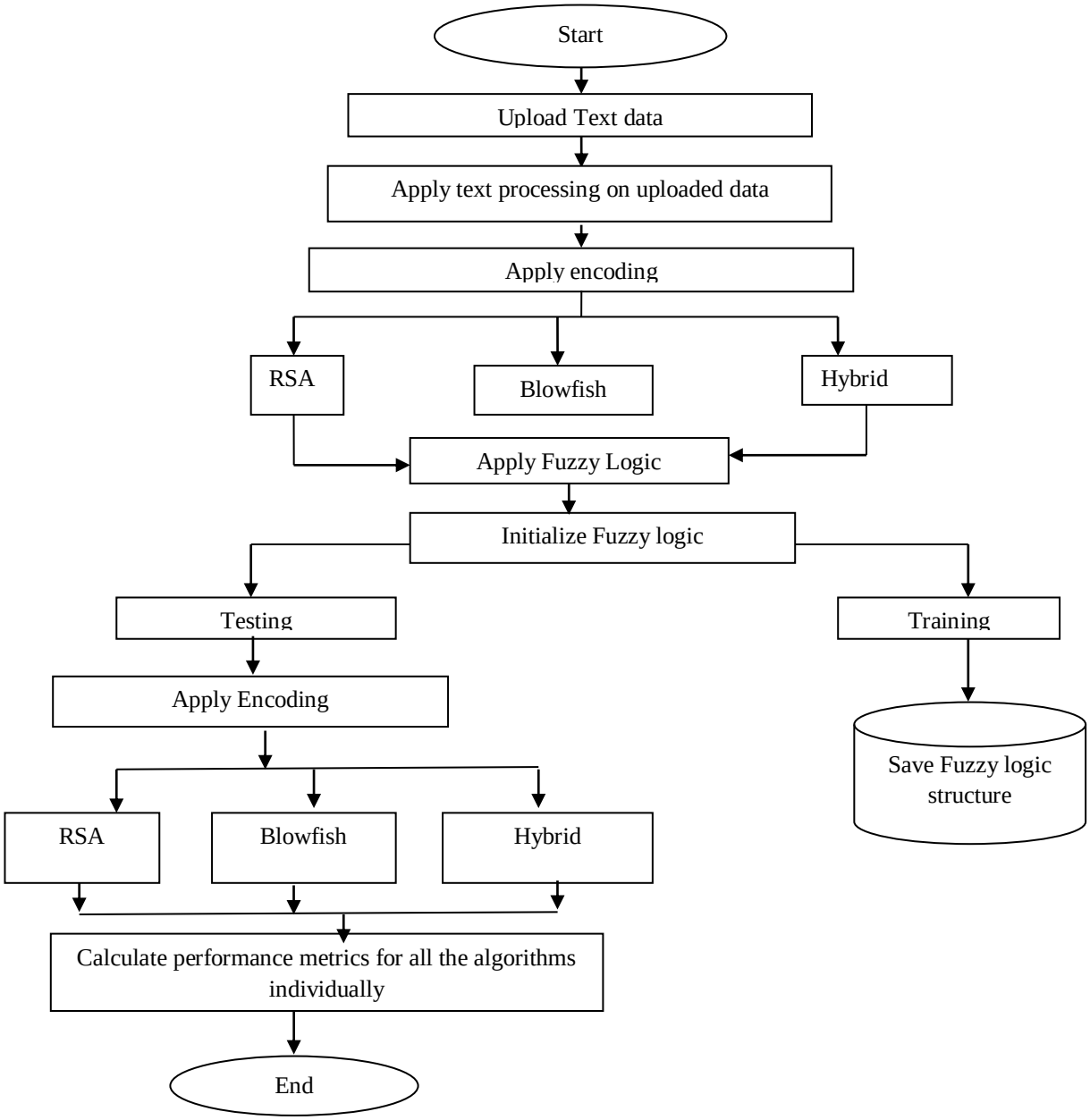

Figure 2: Flowchart of proposed work

Step 2: Processing has been applied on uploaded data.
Step 3: Uploaded data has been encrypted using Encryption algorithms like RSA, Blowfish and Hybrid.
Step 4: Fuzzy logic has been applied for training and testing.
Step5: Initialization of fuzzy logic algorithm is done.
Step6: On this text cases, training is applied and the fuzzy logic structure has saved.

Step7: On parallel to training on fuzzy data, testing has done after initialization of fuzzy logic.

Step8: Data has been encrypted using RSA, Blowfish and Hybrid.

Step9: For each algorithm performance matrix has calculated.

III. SIMULATION RESULTS

In this section, the results obtained after simulating the code in MATLAB are discussed in detail.

Table 1 Simulation results

Parameters	RSA algorithm	Blowfish Algorithm	Hybrid Algorithm
Precision	.47933	.62185	.93169
Recall	.3107	.50093	.78832
F-measure	.26702	.55487	.85402

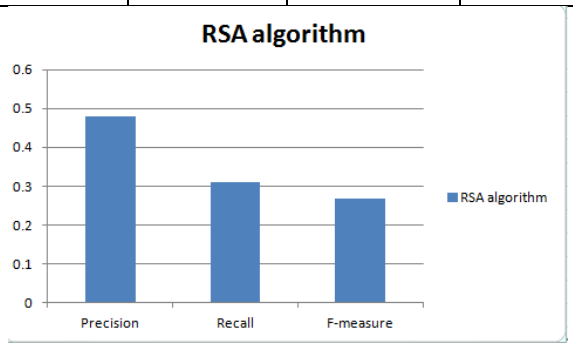

Figure 3: measure parameters for RSA algorithm

In figure 3 measured parameters like Precision, Recall and F-measure have displayed. The values obtained for precision, recall and F-measure are .47933, .3107 and .26702 respectively. It is clear from the figure that precision values obtained for RSA is more than the recall and f-measured value.

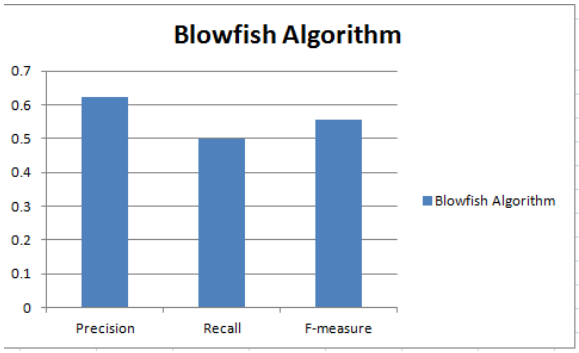

Figure 4 : measure parameters for Blowfish algorithm

In figure 4 measured parameters like Precision, Recall and F-measure have displayed. The values obtained for precision, recall and F-measure are .62185,.50093 and .55487 respectively. It is clear from the figure that precision values obtained for Blowfish algorithm is more than the recall and f-measured value.

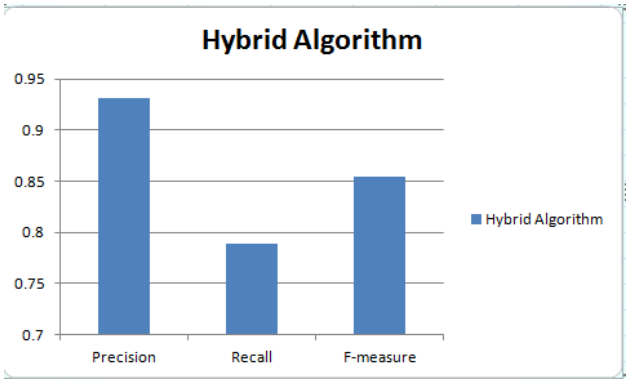

Figure 5 measure parameters for Hybrid algorithm

In figure 5 measured parameters like Precision, Recall and F-measure have displayed. The values obtained for precision, recall and F-measure are .93169, .78832 and .85402 respectively. It is clear from the figure that precision values obtained for hybrid algorithm is more than the recall and f-measured value.

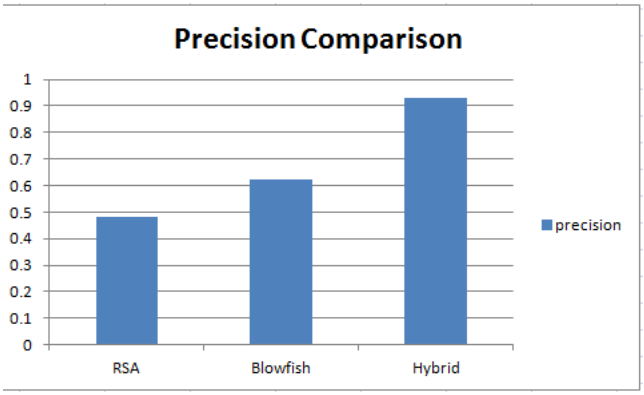

Figure 6 Precision comparison graphs for RSA, Blowfish and Hybrid algorithm

Precision values obtained for RSA, Blowfish and Hybrid algorithms in the form of graph have displayed in figure 6. Form the graph, it is concluded that the value of precision obtained for Hybrid algorithm is maximum, and for RSA it is minimum. So, it is concluded that more is the value of precision more accurate are the text retrieved at the receiver end. As , Hybrid algorithm is the combination of RSA and

Blowfish algorithm therefore the results obtained for precision are more accurate than other two algorithms.

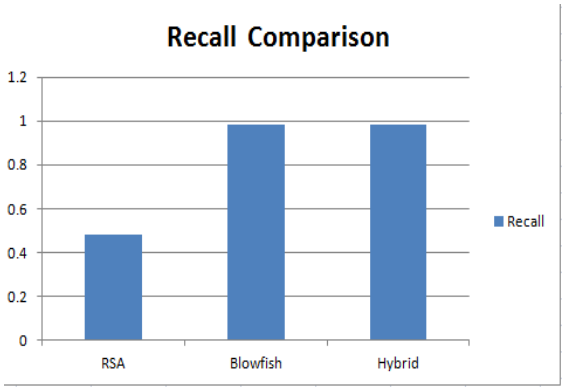

Figure 7: Comparison graph of Recall for RSA, Blowfish and Hybrid algorithm

Recall values obtained for RSA, Blowfish and Hybrid algorithms in the form of graph have displayed in figure 7. Form the above graph it is concluded that the value of Recall obtained for RSA algorithm is minimum, whereas, for Blowfish and hybrid algorithm it is maximum. Recall is high forBlowfish and Hybrid algortithms because it is the ratio of required data and total test data.So,In the proposed work required information is higher than the unwanted feature so recall rate is high.

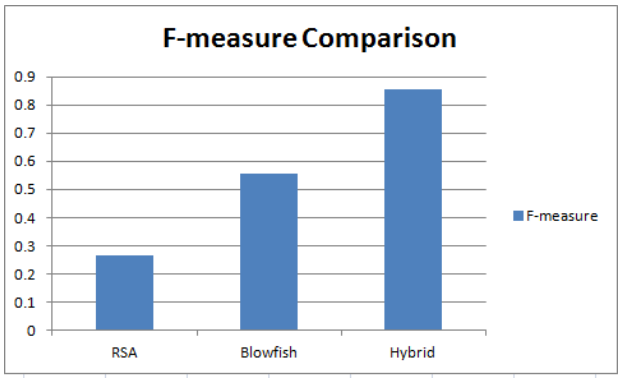

Figure 8 Comparison graph of F-measure for RSA, Blowfish and Hybrid algorithm

F-measure values obtained for RSA, Blowfish and Hybrid algorithms in the form of graph have displayed in figure 8. Form the above graph it is concluded that the value of F-measure obtained for Hybrid algorithm is maximum, and for Blowfish algorithm it is minimum.

IV. CONCLUSION

Experiment results show that the average encryption precision value for RSA, Blowfish and Hybrid algorithm are .47933, .62185 and .93169 respectively. The Recall values obtained for RSA, Blowfish and Hybrid algorithm are .3107, .50093 and .78832. In addition to these parameters another parameter which is calculated is F-measure. The values obtained for this parameter using RSA, Blowfish and Hybrid algorithm are .26702, .55487 and .85402 respectively. Blowfish is secured than the other algorithms. Blowfish gives higher precision as compared to RSA algorithm. The hybrid of RSA and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities. This hybrid structure of enhanced RSA and Blowfish provides more security. In future, The processing time can be reduced by running both the algorithms simultaneously instead of one after another. Blowfish can be replaced by Twofish symmetric algorithm. It is also recommended to use image and video as input data and check the behavior of the algorithm.

V. REFERENCES

[1]. Barker, E. (2017). SP 800-67 Rev. 2, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher. *NIST special publication*, *800*, 67.

[2]. Zhou, N., Zhang, A., Zheng, F., & Gong, L. (2014). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology*, *62*, 152-160.

[3]. Aljawarneh, S., & Yassein, M. B. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, *76*(21), 22703-22724.

[4]. Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynamics*, *92*(4), 1745-1759.

[5]. Wang, W., Si, M., Pang, Y., Ran, P., Wang, H., Jiang, X., ... & Jeon, G. (2018). An encryption algorithm based on combined chaos in body area networks. *Computers & Electrical Engineering*, *65*, 282-291.

[6]. Rivest, R. L. (1994, December). The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86-96). Springer, Berlin, Heidelberg.

[7]. Madanayake, P. R. D., Peiris, M. D. N. S., Ranaweera, G. H., Jayathilake, K. U. K. K., Senarathne, A., & Abeygunawardhana, P. K. W. (2013). Advanced encryption algorithm using fuzzy logic.

[8]. De Silva, C. W. (2018). *Intelligent control: fuzzy logic applications*. CRC press.

[9]. Domínguez-Navarro, J. A., Artal-Sevil, J. S., Pascual, H. A., & Bernal-Agustín, J. L. (2018, April). Fuzzy-logic strategy control for switched reluctance machine. In *Ecological Vehicles and Renewable Energies (EVER), 2018 Thirteenth International Conference on* (pp. 1-5). IEEE.

[10]. De Silva, C. W. (2018). *Intelligent control: fuzzy logic applications*. CRC press.