# Security Framework For Distributed Database System

**Shruthi T V[1], Ranjitha T K[2], Rohit B[3], Sameeksha B S[4], Shilpa S[5]**
[1]Assistant Professor,Dept of Information Science and Engineering
[2, 3, 4, 5]Dept of Information Science and Engineering
[1, 2, 3, 4, 5] East West Institute of Technology, Karnataka.

***Abstract***- *This research aims to study various Symmetrical Algorithms, and to determine a suitable algorithm for the encryption and decryption. There are various types of encryption algorithm, which can be used to encrypt the computerized information in different Organizations. Algorithms can encrypt and decrypt text file of variable length ,and also compute the packet delivery ratio, throughput but the time duration of each Algorithm for the encryption or decryption process of specific file size is not fixed. Text file of size "10 KB to 5 MB", are considered for the analysis; the time duration that each algorithm takes to encrypt or to decrypt the text file is computed. The proposed algorithm takes lesser time for encryption and decryption. Result obtained will be analyzed with the cipher text which will be UTF8 format ( Unicode Transformation Format, "8" Means "8" bits) to represent a character .*

***Keywords***- Cryptography, Encryption, Decryption, Time Duration, Packet delivery ratio, Packet losses, AES, DES, Rijndael, RC2, Blowfish, Cloud.

## I. INTRODUCTION

Nowadays the requirement to keep information secure is increasing. The concept of secure communication is not only for the government institution but also for the private sector such as organization, education and business projects. The transmission of information over the network are becoming widely used in many parts of the world which will make the world connected. To keep communication secure or to provide a security for the data in computer there are many cryptographic algorithms which can be used to provide a good security, some of them are similar while securing a small size of information and others are good for big size of data. With the increase in the progress of the technology in the world of communication, Cryptography has become very important for securing the information during transmission, so it protects information against active and passive attack.

The essential concept in all communications is that there must be three parts for the communication in order to be effective: First there must be two users or more, a sender and a receiver, they may have something to share between them. The second part of the communication is a medium which is the channel of the communication that is used for transmitting of the data between sender and receiver. The third part is a set of communication rules and protocols.

## II. PROBLEM OF THE STUDY

The following points are the problems of the study:

1) Hackers always attack and destroy the data in system through the security gaps.
2) Lack of finding suitable algorithm for the encryption or decryption of a specific range of the text file size.
3) The time durations that each symmetrical algorithm takes to encrypt or decrypt text different files are not similar.

## III. IMPORTANCE OF THE STUDY

The important of this study focus on the following points:

1) The main point of this study is to compare several symmetrical algorithms such as "AES, DES, RC2, Rijndael, blowfish" and to find out the best algorithm according to the time duration that each algorithm takes to encrypt or to decrypt a text file.
2) To adjust all the above mentioned algorithms according to the ability of the time duration that each algorithm takes to encrypt or decrypt a specific size of the text file.
3) To combine all the above mentioned algorithms in one program, so that the program could select a suitable algorithm while encrypting or decrypting the text file based on the size of the text file.

## IV. RELATED WORKS

For the more prospective about the performance of the cryptographic algorithms (encryption algorithms), this section explains and describes the previous works applied in the field of data encryption, the concept takes into consideration is a process of speed, throughput power consumption, a valance, data type, and data size. It also explains the findings obtained for several cryptography algorithms.

Shailja Kumari and Jyoti Chawla found that AES (Rijndael) is the most secure symmetric algorithm, it is also better and faster among all the algorithms which have been used in their study, and there is no serious weaknesses in AES (Rijndael) algorithm, there are many gaps of security in symmetric algorithms such as insecure transmission of secret key, weak keys, flexibility, speed, reliability and authentication in IDEA algorithm, it involves large class of weak keys facilitating the cryptanalysis for recovering the key, they also found that the Blowfish exposed to a differential attack against certain variants, it is also slow in speed but much more faster than (IDEA) International Data Encryption Algorithm. Consistent with my present results, they have used various cryptographic algorithms in order to compare between them and to find the much secure algorithm, with consideration of speed also. Inconsistent with present findings, Shailaj and Jyoti reported that their comparison was in the role of weak key, flexibility and reliability, they decided that AES (Rijndael) was the best in term of security performance, flexibility, and memory usage.

Mohiuddin Ahmed et al. They have talked basically in their paper about "cryptographic technique", under title "Cryptography and State-of-the-art Techniques", they explained that there are constant improvements of data security and information storage systems but still cryptography techniques need to be more agile and strong. They recommended that in the future the cryptography should be implemented in image processing and storage systems.

Tannu Bala and Jogesh they have found that security is very important and powerful for the computerized information in the terms of networking and internet, and various communication systems. The paper was under the title "Asymmetric Algorithms and Symmetric Algorithms". The role of their studies was the comparison of different symmetric algorithms (DES and AES), Asymmetric algorithms (RSA and Elgamal), and they recommended that AES algorithm is better while using symmetric algorithms, however Elgamal is powerful while securing the information in asymmetric algorithms. In the future plan they recommended that algorithms will improve to provide more powerful security system.

## V. COMPONENTS REQUIRED

**Software Used:**

1. JAVA
2. Java Script
3. HTML
4. Java Database Connectivity (JDBC)
5. TOMCAT 6.0 Web Server

## VI. EXISTING SYSTEM

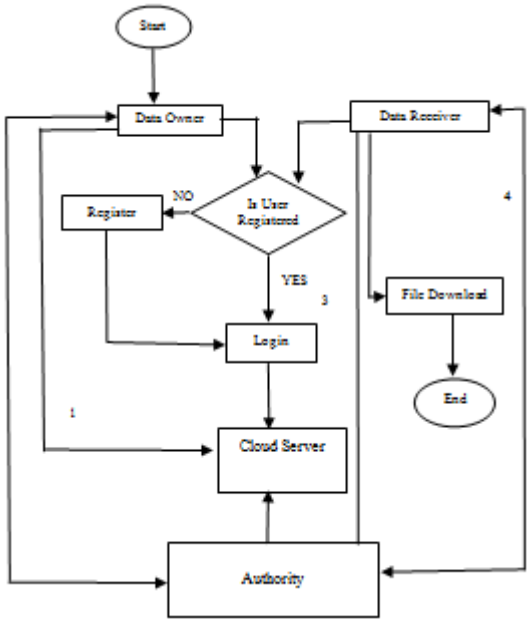
The Data Encryption Standard is a block cipher, meaning a cryptographic key and is applied to algorithm to block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups into 64-bit blocks. Each block enciphered using the secret key into a 64-bit ciphertext by means of permutation and substitution. The process involves 16 rounds and is run using four different modes,making each cipher block dependent on all the previous blocks or encrypting blocks individually. decryption is simply the inverse of encryption,the steps are same but reversing the order in which the keys are applied.

The Advanced Encryption Standard (AES), can also be the Rijndael algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys of 128, 192 or 256 bits. AES was found to replace the Triple DES (3DES) algorithm used for a good amount of time universally. Though, security was the only consideration, the 3DES would be an appropriate choice for a standardized encryption algorithm for decades . The main drawback was slow software implementation.

The Rijndael Algorithm (pronounced "Reign Dahl," "Rain Doll" or "Rhine Dahl") is the Advanced Encryption Standard (AES) recommended by the US National Institute of Standards and Technology for sensitive protection of data, unclassified government information. NIST has been used other encryption algorithms, such as DES (Data Encryption Standard), Triple DES and Skip jack for encrypting government information.

The Lotus sponsored the development of RC2 , who were seeking a custom cipher , after evaluation by the NSA, could be exported as part of their Lotus Notes software. when Rivest incorporated, the NSA suggested a couple of changes. In 1987 the block encryption algorithm was developed . It is a secret key block encryption algorithm which uses a variable size key from 1 byte to 128 bytes. It consists of input and output block size of 64-bit each. This algorithm was designed to be easily implemented on 16-bit microprocessors.

## VII. PROPOSED SYSTEM




*1.User Autentication 2.Encryption key req/res 3.Req/Res Secret Key for download 4.Decryption Key Req/Res*

*Flow chart*

The Blowfish algorithm can achieve an efficiency of data encryption up to 4 bits per clock. We avoid I/O limited constraint by changing the I/O from 64 bits to 16 bits in this algorithm. The proposed architecture ought to fulfil the need of high data encryption and can be separately connected to different devices. Blowfish algorithm is a variable-length key block cipher. Applications where there is a strong communication link and where the key will not be changed too often there, we will be using the Blowfish algorithm It is quicker than DES. Blowfish is a 16-pass block encryption algorithm which cannot be broken. Blowfish is frequently used because it encrypts data on large 32-bit microprocessors at fastest rate of 26 clock cycles per byte. It is compact as it can run in less than 5K of memory. It simply uses addition, XOR, lookup table for 32-bit operands. It is secure and has variable key length; it can be in the range of 32 448 bits: default 128 bits key length.

Firstly, Data owner and Data receiver has to be registered. Authority plays a vital role of providing permission for both encryption and decryption of the file with the generation of secret key. Cloud server stores all the file, permission provided by authority, secret keys and the user details. Once the data owner has the permission to upload the file and secret key, data owner can select the algorithm to be encryption. The parameter such as Encryption time, Throughput, Packet Losses, Packet Delivery Ratio are captured and are put into excel file. These parameters are analysed for different file sizes and the final conclusion of the best algorithm. Similarly, Once the data receiver has the permission to download the file and secret key, data receiver can view the data of the file or download the file.

## VIII. OBJECTIVES

The objectives of this study are as follows:

- To study different symmetrical algorithms techniques.
- To find out the time duration that each algorithm takes to encrypt or decrypt different size of text file so that Programmers need not to reinvent the wheel each time to develop a new application.
- To compute the packet delivery ratio, throughput and packet losses
- Create a positive cryptography culture for text file.

## IX. RESULTS

### 1. Encryption Time

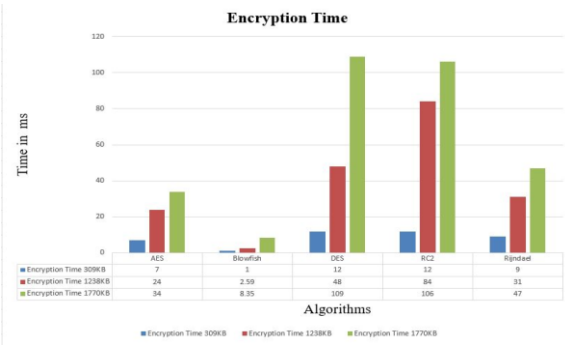



Figure 9.1

Figure 9.1 shows encryption of 309KB,1238KB,1770KB of text in various algorithms, which are shown, it also explains the time duration that each algorithm takes to encrypt of text files, in the role of bar plot,

### 2. Decryption Time

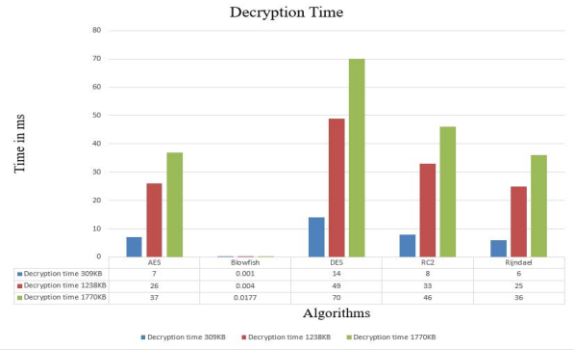



Figure 9.2

Figure 9.2 shows the time duration for each algorithm and the time duration that each algorithm takes to decrypt 309KB,1238KB,1770KB of text file in the sequence of bar plot

### 3. Packet Delivery Ratio

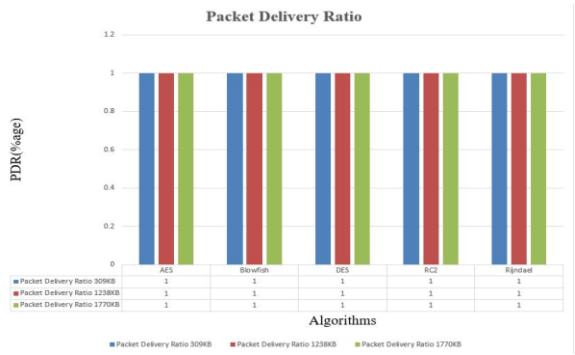



Figure 9.3

The Packet Delivery Ratio(PDR) is the ratio of packets successfully received to the total sent. In figure 9.3 the PDR value is one for all text files because local system is acting as both client and server.

### 4. Throughput

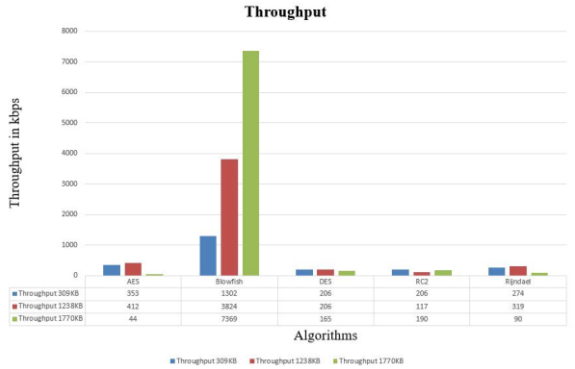



Figure 9.4

Throughput is the rate at which information is sent through the network.In above figure 9.4 throughput is measured for various text file in terms of data packet per second

## X. CONCLUSION

Five symmetrical cryptographic algorithms i.e. AES,DES, RC2,Rijndael,and Blowfish are considered in this study, each of these algorithms have been used for encryption and decryption of different text files which vary in size, the text files of sizes 309KB, 1238KB, 1770KB are considered . The time duration for each algorithm to encrypt and decrypt text file, packet delivery ratio and throughput is computed. This code written in java, after analysis of time durations for each process, the finding was some algorithms are appropriate for the small size of the text file and others are appropriate for big size of the text file and according to this result of the analysis, the concept of the suitable crypt (suitable cryptography) has constructed, the concept is in the term of checking the size of the text file before encryption and decryption process, and the program chose suitable crypt automatically according to size of the text file, the result is analysed by web server.

## REFERENCES

[1] Kumari, S. and Chawle, J. (2015) Comparative Analysis on Different Parameters of secured information for Encryption Algorithms . International Journal of Innov ation & Advancement in Computer Science , 2, 123-129.

[2] Mohiuddin Ahmed, T.M., Sazzad, S. and Elias Mollah, Md. (2012) Cryptography and State-of-the-Art Techniques. Issued by IJCSI International Journal of Computer Science 9, 583-586.

[3] Bala, T. and Kumar, Y. (2015) Asymmetric Algorithms and Symmetric Algorithms: A Review. International Journal of Computer Application, International Conference of Advancement in Engineering and Technology (ICAET 2015), 1-4.

[4] Stallings, W. and Brown, L. (2012) Computer Security Principles and Practices. Microsoft Corporation United States of America, Boston, 2nd Edition, Upper Saddle River, New Jersey, 10.

[5] Kaur, A. and Kumari, S. (2014) Secure Database Encryption in Web Application. International Journal of Adv anced Research in Computer and Communication E engineering , 3, 7606-7608.

[6] https://www.villanovau.com/resources/iss/history-of-information-security/#.wjxaw _iy3vi

[7] Jan, C. and Van Der Lubbe, A. (1998) Basic Method of Cryptography. Cambridge University Press, Cambridge.

[8] MIDN and Lee, K. (2015) Advanced Encryption (AES) Selection Process—How Rijndael Won. Capston SM463A