Study on secure encrypted data

J Component Final Report

CSE4003 Cyber Security

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology
In
Vellore Institute of Technology
By

1. Tanala Surya Tataji – 19BCE0635
2. Nadimpalli L Narasimha Raju – 19BCE2247
3. R.Jaswanth – 19BCE0011

Under the Guidance of

Dr. Deebak BD

School of Computer Science and Engineering
VIT, Vellore

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Declaration:

We hereby declare that the project entitled “Study on secure encrypted data” submitted by our team, for the award of the degree of Bachelor of Technology in Cyber Security to VIT is a record of bonafide work carried out by our team under the supervision of Dr. Deebak BD.

I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Vellore

Table of Contents

Objective

We propose to theoretically study various schemes proposed by authors which are secure and efficient and use the concept of Analysis of encrypted data techniques. We can conduct this study through this project, **the objective** is to secure data with user conveniences. The proposed Secure File System (SFS), we have designed, provides file data security using cryptographic techniques in a transparent and convenient way. SFS requires that the user creates a directory and name it with the prefix 'encrypt' to store the encrypted file data. here we will be studying some algorithms which a few a part of this concept. We will be seeing brief explanation of those algorithms.

1. Problem addressed:

1.1 Type of Research

Updating the data is the basic operation for databases,but it is quite troublesome when we deal with data encryption.we need to avoid the process of breaching privacy and this inefficient process “decrypting all – updating specific – encrypting all”, For security, data-level privacy protection and user-level access control are both important. For efficiency, the accessibility of most users should be carefully considered. In a cloud environment, data interaction and a large number of users will exacerbate these challenges.

Type of Research: Qualitative Research

2. Prior research

In the paper SeUpdate: Secure Encrypted Data Update for Multi-User Environments.

The authors have proposed a sse system in which we can embed flexible access control policies depending on the obligations and capabilities of departments, and achieve a flexible controlled data update and keyword search without leaking sensitive data to both external attackers and clouds. we can grant different users different permissions to read / write data and allow cross-terminal data updates (or different users) and search for keywords in aggregated data. While ensuring data privacy and query, data integration efficiency is improved.

This way the actual encrypted data resides in the encrypted directory and the mapping provides a window to access these encrypted file in clear text form to the authenticated user. CFS uses Data Encryption Standard (DES) to encrypt file data.

EFS stores the encryption keys on disk in a lockbox that is encrypted using the user's login password.We achieved high security by including support for AES, designing a strong access control mechanism using public cryptography and session entry for accessing confidential data.Most of the solutions provided works in user space. The simple and naive approach used by many people to secure their file data is to use common utilities like 'crypt' or 'aescrypt'. These utilities take the filename and the password as inputs and produce the encrypted file

3. Significance

This article make a significant role in the field of data encryption and they briefly explained about the different kinds of available encryption techniques and compare them and getting the positives and negatives of these different encryption techniques and different methodologies proposed to overcome the existing difficulties.

In this article, the author consenus with the article we are analysing.

https://ieeexplore.ieee.org/document/9511199/

4. Introduction, Literature Review and Methodology:

A. Introduction

This way the actual encrypted data resides in the encrypted directory and the mapping provides a window to access these encrypted files in clear text form to the authenticated user. CFS uses Data Encryption Standard (DES) to encrypt file data.

EFS stores the encryption keys on disk in a lockbox that is encrypted using the user's login password. We achieved high security by including support for AES, designing a strong access control mechanism using public cryptography and session entry for accessing confidential data. Most of the solutions provided works in user space. The simple and naive approach used by many people to secure their file data is to use common utilities like 'crypt'

or 'aescrypt'. These utilities take the filename and the password as inputs and produce the encrypted file.

B. Literature Review

starting point for this research is SeUpdate: Secure Encrypted Data Update for Multi-User Environments.The author proposed trusted authority(TA) which is responsible to setup the whole system and generation of the key. Set of users may play two roles like update user who is approved to update the database.the cloud server which is responsible for information storage and keyword search for search User's search request.The supervisor gateway is also proposed to check update user's authority.

searchable symmetric encryption (SSE) that performs efficient keyword search over encrypted data.

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to perform keyword queries and update operations on the encrypted file collections. DSSE has several important applications such as privacy-preserving data outsourcing for computing clouds.

Searching in a multiuser environment have Two issues basically that to be considered for DSSE where multiple data users and data owners, the keys should be considered. The first issue is complete (read and write) access control, Another problem is user efficiency.

forward and backward security (FS/BS) is to have the security at the front end of the webpage and security to the backend servers also.

C. Methodology

Four entities are involved in SeUpdate system:

They are as follows

Trusted Authority (TA): The off-line trusted authority will maintain and it is responsible to setup a whole system, generation of the key and distribution of the key, and read access control policy embedding. It will be only active in this stage.

set of Users with their corresponding data:

The arrangement of clients can be split into various disjoint classes, called security classes. A security class can address a single client, a division or a user group in an organization. A User in a May plays two roles, they are the Update User who is approved to update the cyphered database and the Search User who has advantage to search the shared encrypted or encoded information. The write authorization is finished by Users and the update demand contains the corresponding or particular authorization data.

Cloud Server:

The semi-legitimate cloud server is responsible for information storage, encrypted database update for Update User's update requests and keyword search for Search User's search requests.

Supervisor Gateway (SG):

The semi-legitimate supervisor gateway is all set to check Update User's update authority, channel its update requests, and deliver the checked update solicitations to CS by a secure channel.

Data encryption standard (DES)

It is mostly used and accepted. its commonly available cryptographic system now a days. It was developed by IBM in 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS). It uses 56 bits key to encrypt the 64-bit block size data. It processes 64 input bits into 64-bit cipher text and algorithm perform 16 iterations. So, the main objective of the project is to parallelly implement the DES Algorithm and hence reduce the execution time for encryption and decryption process.

Proposed Algorithm:

1) Start
2) Read the plain text file and store the text as a string.
3) Split the string into parts of 8 characters each and store it in vector.
4) Read the 16bits hexadecimal key and convert it to 64 bits binary.
5) Convert key from 64 to 56 bits by dropping parity bits.
6) Divide 56 bits key to left and right of 28 bits each and left shift them according to the round number and combine them again to obtain 56 bits key.
7) Compress key from 56 to 48 bits by using key compression matrix.
8) Repeat step 6 for the 16 times and store the thus obtained round keys in a vector.
9) In pragma declaration, explicitly mention schedule as guided and mention no of threads.

10) Call encryption function from pragma block.

Encryption Function:

a. Convert the characters to binary representation by taking ASCII value into consideration.
b. Do Initial Permutation to the 64 bits plain text and split it to Left and Right Plain Texts of 32 bits each.
c. Expand the RPT from 32 bits to 48 bits and do XOR Operation with the round key.
d. Do S Box Permutation and the 32 bits result from s box permutation is sent to P- box permutation.
e. Do XOR Operation between thus obtained 32 bits result and LPT and swap left and right.
f. Repeat a-e for 16 rounds except that step e is not done in final round.
g. Combine left and right to obtain 64 bits text and do final permutation to obtain cipher text.

Asymmetric algorithm

Most public key ciphers rely on high computational cost operations. Therefore, keeping performance considerations in mind, for data encryption/decryption computational effort to encryption/decryption using Asymmetric key is very powerful compare to symmetric key algorithm. It's providing more security compare to symmetric key as in the symmetric key algorithm encryption and decryption is done with the same key whereas in asymmetric key algorithm public key is used for encryption and private key is used for decryption and also performance of encrypting file very good. It is general purpose software.

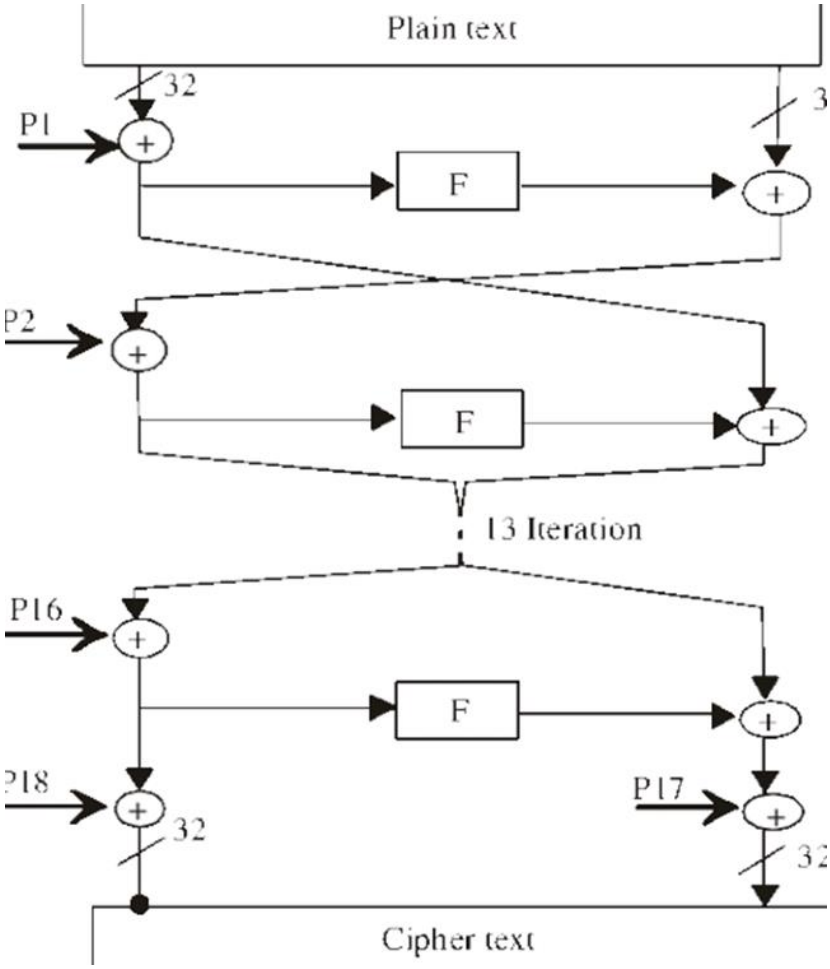
The main advantage of this algorithm is it doesn't use the same substitution cipher which is like, an alphabet won't be replaced by other alphabet. Instead for example, take an alphabet **a** and add 5 so that we get **f,** the key will be 5 for all the letters in the plain text. The key changes for every iteration in this algorithm. It succesfuly came out of Brute Force Attack. We are extracting each digit of the key and it is stored in an array. In Encryption, addition of ASCII character of plain text and number in the array position creates new cipher text and dor Decryption subtraction of the same is done.

Most public key ciphers rely on high computational cost operations. Therefore, keeping performance considerations in mind, for data encryption/decryption computational effort to encryption/decryption using **Asymmetric key** is very powerful compare to symmetric key algorithm. It's providing more security compare to symmetric key and also performance of encrypting file is very good. It is general purpose software.

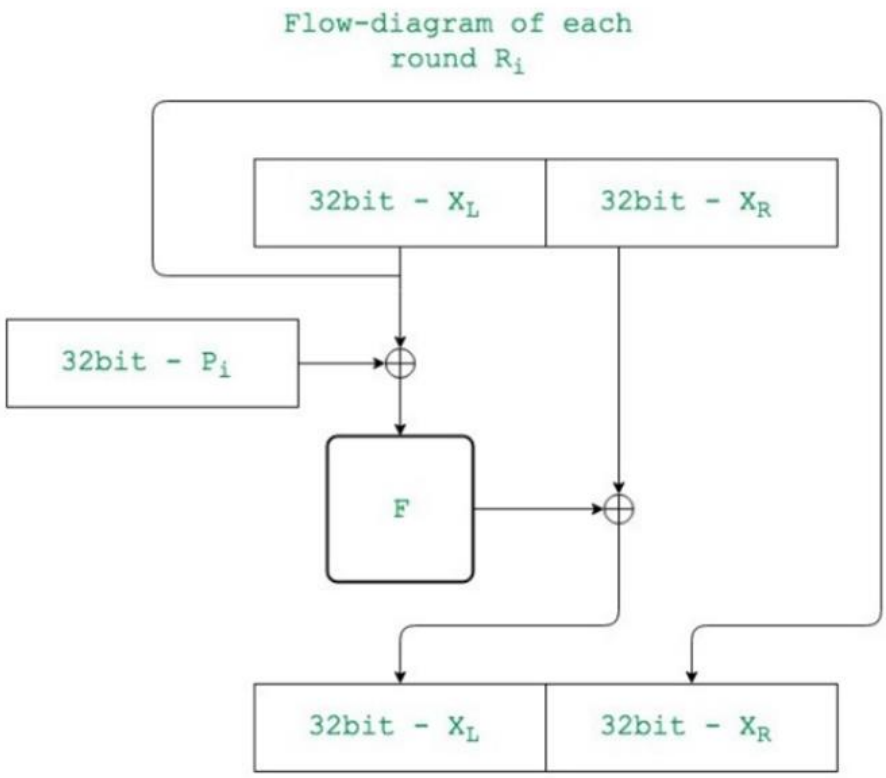
Blowfish

Blowfish is a key, cryptographic block cipher with key designed by Bruce Schneier in 1993 and placed in a public domain which uses the Fiesta network.

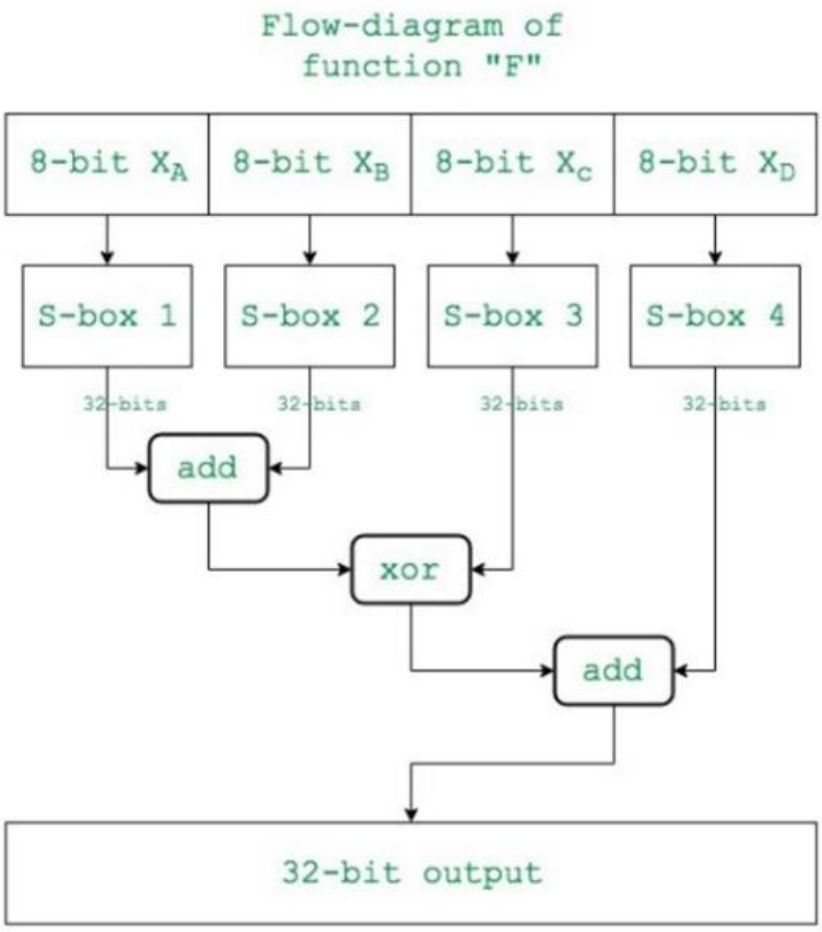
There are 16 rounds for encryption and decryption in functional design.
The size of The block is 64bits and the key size can be upto 448 bits.
The cipher use the 18 subarrays each of the 32 bits commonly known as P-boxes and 4 substitution box each having 32 bits.
Blowfish is in use as one of the fastest block ciphers and which is publicly freely available



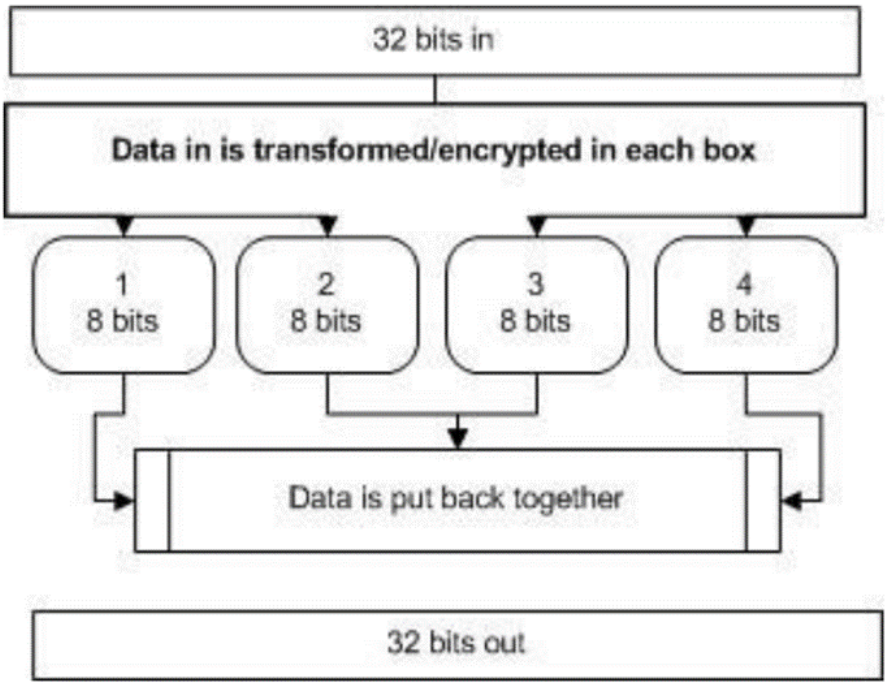
Flow For each round=



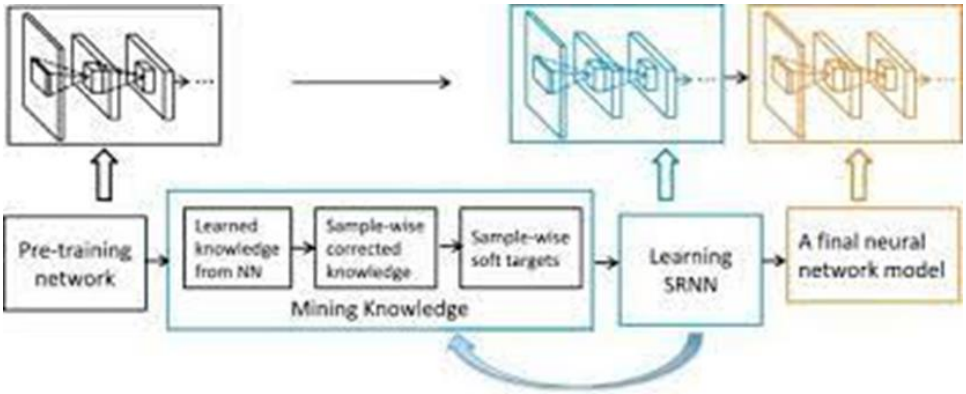
Flow diagram of each (function) F



SRNN algorithm it has two phases
Encryption phase=
Generates N number of subkeys for your key



Decryption phase=
Submitting the n number of sub encrypted keys to get our desired key



5. Contributions:

A. Contribution of the Author

The author of this paper proposed a new tool called SEcure encrypted data UPDATE. From Searchable Encryption which is a safe DSSE scheme with complete access control in the multi-user setting.authors introduced some good features Secure and efficient

encrypted data update,- Complete access control and efficient user search in the multiuser setting they used the possibility of a productive key task plan to support flexible and hierarchical read access control. There is no need to share a secret key between users and just one search token needs to be generated and transmitted and sent by a client for looking of all his authorized information.. As an effort to fix the existing systems, the authors have used some of the techniques and algorithms to fix the problem and make the software complex and secured way by using algorithms like DES, ASYMENTRIC, BLOWFISH, ETC.

B. Our Contribution

All our group members have contributed equally for making the documents and for doing the above research.

In this study we analyze the present encryption techniques and difficulties of encryption that are being used already and we try to study on different encryption schemes for a to make a good study and compare among the different encryption schemes.

All our group members have contributed equally for making the documents and for doing the above research.

Below are those algorithms where each person focused on .

Nadimpalli L Narasimha Raju [19BCE2247]: blowfish and snrr algorithm.

R.Jaswanth [19BCE0011]:IDEA and AES algorithm.

Tanala surya tataji[19BCE0635]: DES and symmetric algorithm

6. Further research:

Searching in a multiuser environment have Two issues basically that to be considered for DSSE where multiple data users and data owners, the keys should be considered. The first issue is complete (read and write) access control, Another problem is In a multi-user system where different people may try to perform dictionary attacks to get the desired encryption key.

Need for a good encryption scheme is still on demand,so by trying mixing the positives from each other and making the super hybrid version of an encryption algorithm will tends to increase

the security in the digital platform.so generating a encryption key which can't be breaked is a never ending process,it's just evolves with the time

Reference:

Abdulhameed, M. (2018). *A Survey on Symmetric and Asymmetric Crytography Algorithm in Information Security.* International Journal of Scientific and Research Publication.

S Manku, K. (2015). *Blowfish Encryption Algorithym for Information Securing.* india: Research works by Research Gate.

V. Yamuna, A. A. (7-july-2015). *Efficient and Secure Data Storage in Cloud using DSE.* Copyright to IJIRCCE .