DOI: https://doi.org/10.24113/ijoscience.v3i5.50

A Hybrid Approach for Data Encryption using Random Number and Padding Base

Suruchi Karnani
Department of Computer Science and Engineering
SR Group of Institutions
Jhansi, U.P., India
suruchi012@yahoo.com

Mr.C.P.Singh
Assistant Professor
Department of Computer Science and Engineering
SR Group of Institutions
Jhansi, U.P., India
cp.singh1984@gmail.com

***Abstract*-The utilization of mobile device and wireless networks tremendously alters our way of living. As with the brilliant security, access methods and effective ways, still people face various challenges to protect their data which carry in these apparatuses. The significant part comes under the trouble because it should be unsalable and not feasible for opponents to decrypt the information. The cryptography is effective for genuine users and reduces the battery drain. This paper recommends the data encryption. Data handling acts as a double stream of bit, the encryption that is known as self technique of individuals able to create a keystream by collecting the bits casually from the stream. Users can choose the bits length as per their needs by considering the security. Afterwards, the bit stream is encoded and saved in the portable devices as a cipher text form. This process makes the computation impossible to get the real data from cipher text form while maintaining the time and space.**

Keywords: Encryption, Random number, Padding, Complexity.

I. Introduction

The current industry requires such kind of network that is capable to exchnage the information along with the highest security and reduction package. these both tings are essential for data storage and time for the tranmission of information. This task is completed by two methods - encryption and compression and it is known as “Compression Crypto-System”. Now, move on the the technique of encryption which is a secure way of coding adn data compression too. It’s main aim is to decrease the space needs for storing the data and time for compression technique. In the proposed system - data security is frequently utilzied the encryption system that is private key and encoded strong. Then, it is produced by a model from the string symbols which comes from an input and constructed on an arithmetic coding [1] [2].

Encryption is a mechanism by which a message is transformed so that only the sender and recipient can see. For instance, imagine Alice needs to transmit a personal message to Bob, and then first of all she has to know the public key of Bob. Anybody can easily get his public key and he can send a message across the network without considering anything. When Alice achieves the Bob’s public key, then start encoding the data by using this key and send to the bob. Afterwards, Bob gets the message and decrypts it by utilizing his private key. [3]

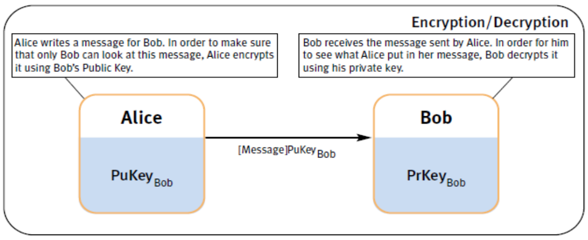

Encryption/Decryption
Alice writes a message for Bob. In order to make sure that only Bob can look at this message, Alice encrypts it using Bob's Public Key.
Bob receives the message sent by Alice. In order for him to see what Alice put in her message, Bob decrypts it using his private key.
Alice
$PuKey_{Bob}$
$[Message]PuKey_{Bob}$
Bob
$PrKey_{Bob}$

Figure 1: Simple Encryption Process

II. DATA SECURITY

Standard cryptography was capable to offer the security for information which is sent over the different channels where few things were imaginable like snooping and message capture. If sender wants to transmit the cipher and encryption key so it can give directly to the receiver, otherwise, transmit it in an indirect way (courier). This process is comparatively slow but channel is secure. Those messages sent in cipher text form so these are insecure over the channels.

Whereas modern cryptography designed to protect the sent data over the electronic lines which is at tremendous speed or it can stored in the computers. This mechanism works on two major principles – Secrecy and Authenticity. The term secrecy or privacy is necessary to protect the data from unauthorized individuals and authenticity is to avoid from the unlawful alterations of data. [4]

Everybody requires such kind of solution in data protection system which is efficient because it directly affects the upcoming generation's computing [10] and the usage of mobile device in original networks [5]. The enhancement of critical data and government policies needs enduring the retention of information to the storage security [15].

At the time of life cycle of data, users can notice several attack points that are genuine. Earlier, thre are various researchers put thier efforts to do better int his stream. As the entire repots and works, the author miss the finest and commendable achivements in network file system. Inspite of that, the author can easily describe the chart of current progression activity in the services of security for data storage protection in terms of distributed things. While in the entire life journey, the data should be secured.

Verification and endorsement ate the most essential things in various systems of data security [13]. Usually, authentication can be developed via various methods like – digital signatures, passwords, MAC which stands for Message Authentication Code. Individuals can achieved the authorization by certificates, access control and much more. Availability is really significant to prevent from the risks like – system crash or can say that DOS (Denial of Service). The classic solution can create duplicate backups. Therefore, duplication moves towards the cost enhancement due to maintenance aspect.

The main aim of data security is to protect from those people who are not authorized to modify the data. Privacy is simply get via encryption during the data integrity which is done by the MAC or digital signatures. At the time of transmission, the information can be secured by SSL [9] and IPSec [12] protocols. For now, the security of data storage can be simply achieved by the schemes of user encryption. The variety of cipher schemes are introduced specifically for this aim which includes latest designs [7]. For being vigorous against the analysis of cryptography, key sharing [11] and management [24] are the most sever sections in the framework. Keep the process under the special attention during saving, eliminating and archiving the key things. Now, move towards next step, which is the key recovery system that helps users to decrypt the message which is in the form of cipher text under various conditions [6].

The main purpose of this project is to know about the scheme of robust stream cipher and explore the various flexible keystream creation techniques. In addition, high security management approach of keystream. People can read the detailed informtaion about this project in the upcoming section.

III. ENCRYPTION

The foremost component of encryption or decryption program development is the creation of key. Now, cryptography contains lots of applications that are commercial. If individuals want to secure their confidential data, cryptography offers a protective shield of a supreme level to various people and groups as well. The goal of this technique is not only offer security but, it can also able to give the perfect solutions to various other issues.

Cryptography is a brilliant mechanism that permits the information to be transmitted securely and only receiver can decrypt the data. The research on cryptography is continuously goes and algorithms are introduces. Hence, this is not an easy way to search the finest algorithm for it. The reason behind that, users are well-known about the important factors such as protection, algorithm features, and time and space complexities.

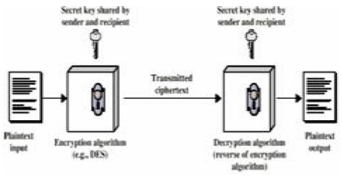

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2: representing conventional encryption

Encryption Approach Used

These days, individuals use the approach of symmetric encryption which is divided into two sections –

- Block Cipher Symmetric Cryptography
- Stream Cipher Symmetric Cryptography

But, mostly select first one which is block cipher due to its high efficiency and security reasons. It this technique, here is a common key among the transmitter and receiver which is termed as private key. The concept of this key is just altering the message into encoded text called cipher text by utilizing the private key where this text is decrypted by same private key into plane text. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transform in the dual keys. Basic concept of symmetric cryptography is shown in figure 2 [8].

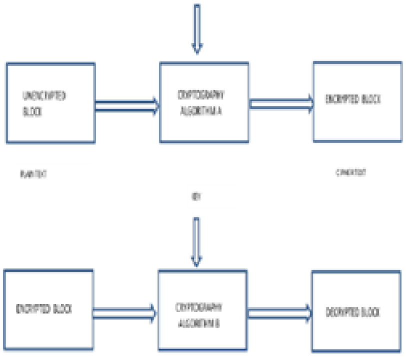


Figure 3: Symmetric Encryption

To decrypt the data and log files, transparent data encryption is used. This technique use a DEK which means Database Encryption Key and stored in the record of database boot for accessibility while retrieval. This termed as an Asymmetric key that is protected by a certificate and available in the master database. Transparent encryption is capable to secure the log and data files. This technology encrypts the data into hard disk and various backup media. It can also provide high level security to table, columns which is the files of database and generally saved in the CDs or floppy disks. This mechanism is utilized by Microsoft SQL server 2008 for decoding the information of database.

It encodes the data before it is inscribed on disk and decode before it is returned to the application. This process of cryptography is performed at the layer of SQL which is transparent to the applications and subsequent backups of database files to the disk. [16]

IV. VARIOUS KINDS OF ENCRYPTION

The information will be showed as several symbols, letters and numbers depend on the encryption type. Those individuals work in the field of cryptography can make their job in it or to encrypt the data/ break codes to get the encoded message.

Manual Encryption

It is a kind of encryption that usually involves the utilization of encryption software. These are the programs which are computerized to encrypt the data in bit forms digitally. Users can completely participate in manual encryption. First of all, choose a file which user wants to encrypt and then select the kind of technique as per the security system abilities.

Transparent Encryption

This is another kind of software in encryption method. Individuals can download it in their computer systems to start the encryption technique and accomplish the work via automatic procedure. It is termed as one of the secured software I this stream due to its memory. Manual encryption forgot the things sometimes but it doesn’t take any chance to leave anything.

Symmetric Encryption

Entire encryption technique is accomplished by a well-structured software program. The easiest way to do this work is “Symmetric encryption”. In this way, a letter/ number/ symbol overlap with another symbol/ letter in the code. Users can pick any written text and then put another letters and numbers for the coded part.

Asymmetric Encryption

This type of encryption is really safe and simple which is utilized to encrypt the information at the time of receiving. Asymmetric encryption is done in an electronic way. The public key is provided by those ones who want to send something in any place which is visible to all. By encrypting the data using the key is after transit the users. Frequently this thing is done by emails. [17]

V. LITERATURE REVIEW

The major issues of todays way of communicating is depend on few things – security, speed, and size of content. This paper introduced the basic concepts of data compression and encryption. Let’s, starts with the first section which concentrates on the creation of cryptography and data compression. After that, the author focuses on the compression cryptosystem. At last, this technique is discussed on the initials of encryption and compression of data. First of all, the data is compressed to reduce its size and then enhance the transfer rate of data. Afterwards, the compressed data is encoded to offer the security. Therefore, the proposed technique of author is really good and efficient to decrease the data size, increase the transfer rate and provide the protection at the time of communication. [2]

The breaks of data is a most common and huge problem because of laptops stolen issues. The resolutions are able to protect the important files on laptops but not as much easy to deploy due to the users which are not convenient. This is a finest way to determine the techniques to offer a modest system to be safe by encrypting the files on laptops. Users watch that only a few numbers of individuals have sensitive information. Rather than protecting all of the user’s files, it secure user designated sensitive files that are rarely accessed outside of specified trusted locations. Our approach is to use information and services available only in a trusted location to assist in key derivation without user involvement and without authenticating the laptop to any outside service. They study two settings: home use where zero management overhead is needed (i.e., a “plug-and-play” solution) and a corporate setting where staff management of a whitelist of acceptable devices allows a higher level of security. They have implemented both systems and found automatic key derivation introduces a five second delay during the initial access to sensitive files. [18]

VI. PROPOSED WORK

This section is handling two things. First Algorithm and second Flow chart.

Step 1. Calculate Random Number by adding ascii value of all the characters of a Key and than perform mod operations on the result by key length

```
int RN = 0;
for (int i = 0; i < Key.Length; i++)
{
        RN += (int)Key[i];
    }
    RN = RN % Key.Length*7;
```

Step 2. Now, Convert the key into 7 bit binary format

```
    Key = con_binary_7(Key);
```

Step 3. Next generate Different keys equal to Key_Length/2 by xoring all the bits by bit (random number + key number position) ahead.

```
    for (int q = 0; q < 1 + kl / 2; q++)
    {
        Key1[q] = R_Ran_xorbits(Key, RN + q);
    }
```

Step 4. Now, divide the plaintext equal to key length chunks and than xor each chunk by all keys by first converting plaintext into 7 bit binary format. If the last chunk is not equal to key length than make key equal to last chunk length and do the same.

```
    for (int i = 0; i < PlainText.Length; i += kl)
    {
        if (PlainText.Substring(i).Length < kl)
        {
            PT = con_binary_7(PlainText.Substring(i));
            Key = Key.Substring(0, PT.Length);
            for (int q = 0; q < 1 + kl / 2; q++)
            {
                Key1[q] = Key1[q].Substring(0,
PT.Length);
            }
        }
        else
        {
            PT = con_binary_7(PlainText.Substring(i,
kl));
        }
        PT = xor(PT, Key);
        for (int q = 0; q < 1 + kl / 2; q++)
        {
            PT = xor(PT, Key1[q]);
        }
        CipherText += (PT);
    }
```

Step 5. Convert the resultant cipher text in to 8 bit character format.

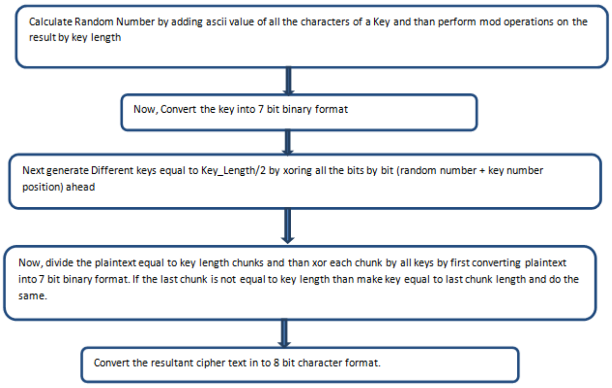

Calculate Random Number by adding ascii value of all the characters of a Key and than perform mod operations on the result by key length
Now, Convert the key into 7 bit binary format
Next generate Different keys equal to Key_Length/2 by xoring all the bits by bit (random number + key number position) ahead
Now, divide the plaintext equal to key length chunks and than xor each chunk by all keys by first converting plaintext into 7 bit binary format. If the last chunk is not equal to key length than make key equal to last chunk length and do the same.
Convert the resultant cipher text in to 8 bit character format.

Figure 4: Flow chart of proposed system

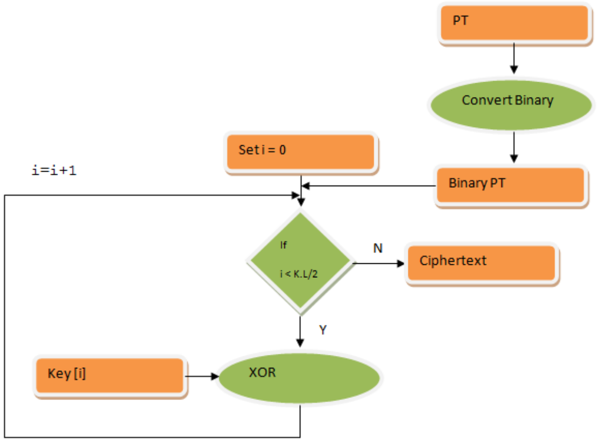


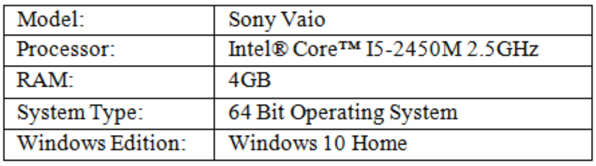
Figure 5: Proposed Flow Chart

VII. Result Analysis

System Configuration

Researchers have performed the encryption of the various data of different length. The system on which these iterations have be performed is having following configuration as shown in table 1.

Table 1: System



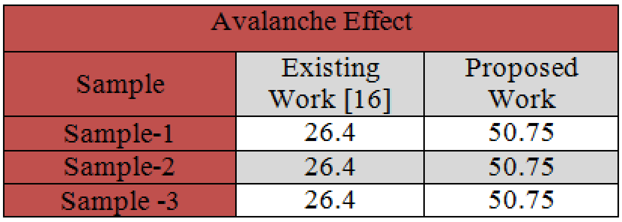
Model:	Sony Vaio
Processor:	Intel® Core™ I5-2450M 2.5GHz
RAM:	4GB
System Type:	64 Bit Operating System
Windows Edition:	Windows 10 Home

Result Parameter

In cryptography, the avalanche effect refers to an attractive property of block ciphers and cryptographic hash functions algorithms.

$$\text{Avalanche Effect} = \frac{\text{Number of change bit in cipher text}}{\text{Number of bit in cipher text}}$$

Table 2: Avalanche Effect of Base & Proposed Algorithm

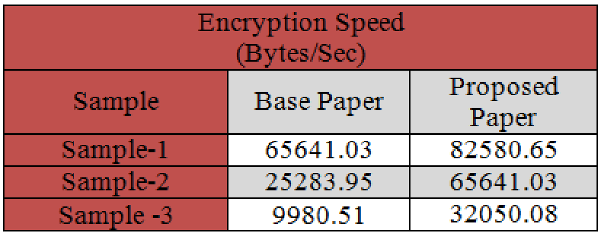


Avalanche Effect		
Sample	Existing Work [16]	Proposed Work
Sample-1	26.4	50.75
Sample-2	26.4	50.75
Sample -3	26.4	50.75

Execution Speed

It is quantity which shows the effectiveness of the work in terms of time required to execute. It's unit is Bytes/Second. Which means it will calculate the encryption of the bytes in one second time duration.

Table 3:Encryption Speed Analysis



Encryption Speed (Bytes/Sec)		
Sample	Base Paper	Proposed Paper
Sample-1	65641.03	82580.65
Sample-2	25283.95	65641.03
Sample -3	9980.51	32050.08

VIII. Conclusion

The Transparent Data encryption works like a chief guest in the protection of transmitted data. Two things are able to secure the sensitive data on disk drives and can take back up of media files. This security is especially for those users who are not authorized and helps to decrease the data loss issues. It is designed under the recent task which is brilliantly tested and implemented from every corner.

Execution Time

From the outcome study it has been established that the performance of proposed concept in execution time is better than existing concept. By double layer, we achieve higher security level. The lower execution time gives better utility of the method in case of online service, as it is very obvious that for any online application required time plays very important and critical role. As shown in table 3.

Avalanche Effect

From Table 2 , it is observed that avalanche effect are calculating between key values on different size of plain text, in all four case proposed technique producing higher avalanche effect.

References

[1] Yu Chen and Wei-Shinn Ku, "Self-Encryption Scheme for Data Security in Mobile Devices".

[2] Ajit Singh and Rimple Gilhotra, "Data Security Using Private Key Encryption System Based On Arithmetic Coding", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[3] Curry, Ian, Entrust Technologies, "Getting Acquainted With Entrust/Solo and Public-key Cryptography", version 1.0, July 1997, "Public Key Encryption and Digital Signature: How do they work?".

[4] Cornelius Lowell Robling 1910-1965, "Denning, Dorothy E., (Dorothy Elizabeth), 1945- Cryptography and data security."

[5] W. Daniel, T. Pintaric, F. Ledermann, S. Dieter, "Towards Massively Multi-User Augmented Reality on Handheld Devices", International Conference on Pervasive Computing, Munich, Germany, 2005.

[6] D. E. Denning and D. K. Branstad, "A Taxonomy for Key Escrow Systems," Communications of the ACM, Vol. 39, Issue 3, 1996.

[7] eSTREAM, ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream.

[8] Vishwa gupta, Gajendra Singh , Ravindra Gupta, "Advance cryptography algorithm for improving data security", Volume 2, Issue 1, January 2012

[9] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL Protocol, Version 3.0," Internet draft, Networking Group, March 1996.

[10] C. Galdi, A. Del Sorbo, and G. Persiano, "Distributed Certified Information Access for Mobile Devices," Workshop in Information Security Theory and Practices (WISTP'07), Crete, Greece, May 8-11, 2007.

[11] Y. Jiang, C. Lin, M. Shi, and X. Shen, "Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications," IEEE Journal on Selected Areas in Communications, Vol. 24, No. 9, Sep. 2006.

[12] A. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Networking Group, Nov. 1998.

[13] A. J. Nicholson, M. D. Corner, and B. D. Noble, "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, vol. 5, no. 11, pp. 1489- 1502, Nov., 2006.

[14] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, Vol. 35, Issue 3, Sept. 2003.

[15] P. E. Sevinc, M. Strasser, and D. Basin, “Securing the Distribution and Storage of Secrets with Trusted Platform Modules,” Workshop in Information Security Theory and Practices (WISTP’07), Crete, Greece, May 8-11, 2007.

[16] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011, “Transparent Data Encryption- Solution for Security of Database Contents”.

[17] Karthik .S1, Muruganandam, “Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System”, Volume 2 Issue 11, November 2014.

[18] Ahren Studer, Carnegie Mellon University, astuder@cmu.edu& Adrian Perrig, Carnegie Mellon University, “Mobile User Location-specific Encryption (MULE): Using Your Office as Your Password∗”