ON INFORMATION SECURITY USING A HYBRID CRYPTOGRAPHIC MODEL

M.O. Onyesolu*
Department of Computer Science
Nnamdi Azikiwe University, Awka
mo.onyesolu@unizik.edu

N.O. Ogwara
Department of Computer Science
Delta State University, Abraka
fegwara@yahoo.com

Manuscript History
Number: IRJCS/RS/Vol.04/Issue11/OCCS100080
DOI: 10.26562/IRJCS.2017.OCCS100080
Received: 21, September 2017
Final Correction: 09, October 2017
Final Accepted: 02, November 2017
Published: November 2017

Abstract— Developing a good database system and providing security control for the database has always been a big challenge. Encryption technique has previously been proposed to provide users with confidentiality in terms of outsource storage. However, a number of these encryption algorithms are weak, enabling adversaries to compromise data simply by compromising an algorithm. A response to this challenge was made by developing a new hybrid encryption model using features of Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). A comparison was made on our new hybrid encryption model with existing encryption models. The new model improved the security of information stored in a database. The results demonstrated that the new model offers a highly secured approach that provides users and organizations with data confidentiality and integrity. It also provided acceptable overhead performance and supports query processing.

Keywords— Algorithm, encryption, cryptography, advanced encryption, triple data encryption standard

I. INTRODUCTION

Information is a valuable asset in every organization. Almost all organizations have information systems that are database driven, some organization databases contain sensitive data, and therefore, database security becomes a major concern. Protecting the information stored in a repository is actually the database security. It deals with making database secure from any form of illegal access or threat at any level. Database security demands permitting or prohibiting user actions on the database and the objects inside it. Organizations that are running successfully demand the confidentiality of their database. They do not allow unauthorized access to their data/information and they also demand the assurance that their data is protected against any malicious or accidental modification [1]. Today, data security is one of the major concerns of every organization. Information stored in databases online, are open to possible attack by interested third party. Due to availability of hacking tools online, hackers can gain unauthorized access to such information, which reduces its integrity and confidentiality.
In order to avoid a situation where unauthorized users gain access to such information, it is good to make the information more secured by the use of cryptographic technique, so that unauthorized users will not temper with the integrity and confidentiality of such information. Most information communicated over the web or networks are not secured. If such information is not properly secured, computer hackers can access such information before it gets to the recipient and as such, the integrity of such information will be violated. In order to secure information the use of encryption technique becomes a subject necessary [2]. Information security is the collection of technologies, standards; policies and management practices that are applied to information to keep it secure [3]. Information security is the means used to protect information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction [4]. In recent days of the Internet, the encryption of data plays a major role in securing data in online transmission. Encryption of data focuses mainly on the security of data across the Internet. Different encryption techniques are used to protect the confidential data from unauthorized use. Data that can be read and understood without any special measures is called plaintext or clear-text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher-text. The main concepts that a security system has to respect are: confidentiality, integrity, availability and authentication. Most security systems use cryptography because it offers various algorithms and technique practically impossible to break because of their complexity. Cryptograph does not only protect data from unauthorized access or alteration, but it can also be used for user authentication. 97% of cybercrimes are undetected such that, the organizations databases which stored information in plaintext are at risk of losing their data to hackers that are targeting various databases online in order to obtain information for fraudulent purposes [5].

Presently, various types of cryptographic algorithms provide high security in information, computer and network related activities. These algorithms help to protect data integrity and authenticity from various attacks. These cryptographic algorithms are classified into two different types - symmetric and asymmetric. In symmetric encryption method both sender and receiver share a common key value for encryption and decryption. It requires that the sender finds some secure way to deliver the encryption/decryption key to the receiver [6]. In this paper, a hybrid symmetric technique for encryption is developed and used to secure data stored in the database.

II. SOME EXISTING CRYPTOGRAPHIC MODELS

A. Shannon Symmetric Cryptosystem Model

Figure 1 is the schematic diagram of Shannon symmetric cryptosystem model. X represents a message source such that:

\[ X = (X_1, X_2, X_3, \ldots, X_M) \quad (1) \]

The \( M \) elements are letters in some finite alphabet. Traditionally, the alphabet usually consists of the 26 capital letters. Nowadays, the binary alphabet (0, 1) is typically used. For encryption, a key of the form \( K = (K_1, K_2, K_3, \ldots, K_M) \) is generated.

If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination. With the message \( X \) and the encryption key \( K \) as input, the encryption algorithm forms the cipher text \( Y = (Y_1, Y_2, Y_3, \ldots, Y_N) \). This can be written as

\[ Y = E(K, X) \quad (2) \]

This notation indicates that \( Y \) is produced by using encryption algorithm \( E \) as a function of the plaintext \( X \), with the specific function determined by the value of the key \( K \). The intended receiver, in possession of the key, is able to invert the transformation:

\[ X = D(K, Y) \quad (3) \]

An opponent, observing but not having access to \( K \) or \( X \), may attempt to recover \( X \) or \( K \) or both \( X \) and \( K \). It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover \( X \) by generating a plaintext estimate \( XX \). Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover \( K \) by generating an estimate \( KK \).

B. Hill Cipher Symmetric Encryption Model

Hill cipher, invented by Lester S. Hill in 1929 uses matrix multiplication for mixing the plaintext [7]. Hill cipher works on groups of letters in different ways. It works by displaying a group of letters as a vector. Encryption is done by matrix multiplication [8]. Hill cipher satisfies two properties that good cryptosystems would have. These properties are diffusion and confusion.
i. **Diffusion:** One change in plaintext character should affect as many characters as possible in ciphertext. It is known that Hill cipher converts any plaintext character to number, and then inserts it in a matrix of column vector. If we take – be – as plaintext characters then it will be – 1, 4 -, the matrix of column vector will be 11

then any change in plaintext must affect cipher text characters.

ii. **Confusion:** The key should not relate to the ciphertext. Hill cipher uses key matrix to encrypt the message and key inverse to decrypt it. Hill cipher example with Key Matrix 2 × 2 uses math equation with condition that the key matrix has to be invertible relative to mod 26.

Give Plaintext:

\[ p_1, p_2, p_3, p_4, ..., p_{n-1}, p_n \]  \hspace{2cm} (4)

Given a Key with Matrix k =

\[
\begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix}
\]  \hspace{2cm} (5)

**Encryption:**

1. Form vectors as follows:

\[
\begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix}
\]  \hspace{2cm} (6)

2. Multiply each vector by k (Equation 5) to obtain a pair of cipher text letters. These give Equations 7, 8 and 9.

\[
k \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} = \begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix} \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} \equiv \begin{pmatrix}
c_1 \\
c_2 \\
c_3 \\
\vdots \\
c_{n-1} \\
c_n
\end{pmatrix} \pmod{26}
\]  \hspace{2cm} (7)

\[
k \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} = \begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix} \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} \equiv \begin{pmatrix}
c_1 \\
c_2 \\
c_3 \\
\vdots \\
c_{n-1} \\
c_n
\end{pmatrix} \pmod{26}
\]  \hspace{2cm} (8)

\[
k \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} = \begin{pmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{pmatrix} \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} \equiv \begin{pmatrix}
c_1 \\
c_2 \\
c_3 \\
\vdots \\
c_{n-1} \\
c_n
\end{pmatrix} \pmod{26}
\]  \hspace{2cm} (9)

3. The cipher text message is 

\[ C_1, C_2, C_3, ..., C_n \]  \hspace{2cm} (10)

**Decryption:**

1. Calculate \( k^{-1} \)

2. For each pair of cipher text find a plaintext by:

\[
k^{-1} \begin{pmatrix}
c_1 \\
c_2 \\
c_3 \\
\vdots \\
c_{n-1} \\
c_n
\end{pmatrix} \equiv \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} \pmod{26}
\]  \hspace{2cm} (11)

\[
k^{-1} \begin{pmatrix}
c_1 \\
c_2 \\
c_3 \\
\vdots \\
c_{n-1} \\
c_n
\end{pmatrix} \equiv \begin{pmatrix}
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{n-1} \\
p_n
\end{pmatrix} \pmod{26}
\]  \hspace{2cm} (12)
III. THE HYBRID MODEL

The hybrid model is a new encryption algorithm for data security application. The schematic model is shown (Fig. 4). This new model uses two different symmetric encryption algorithms, the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) to develop a hybrid cryptographic system to enhance data security in two ways.

1. The new system has the encryption part where data to be stored in a database is encrypted. The system uses an encryption process by employing the two encryption standards AES with a secret key 1 for encrypting the data and re-encrypting the first cipher text using another encryption algorithm, 3DES, with a secret key 2 (Fig. 2).

2. Data stored in the database can be decrypted using decryption process for 3DES with a secret key 2 to decrypt the data for authorized users only before decrypting the output of the 3DES decryption using decryption algorithm for AES with secret key 1 (Fig. 3).

The hybrid encryption system is n-tuple where n = 5 with tuple attributes given as:

\[ FHES = (P, C, K, E, D) \]

Where:
- \( P \) is a finite set of plaintexts
- \( C \) is a finite set of ciphertexts
- \( K \) is a finite set of keys
- \( E \) is a finite set of encryption algorithms
- \( D \) is a finite set of decryption algorithms.

For each \( k \in K \) there are encryption algorithms in \( E \). The encryption algorithms are functions:

\[ e_{k,n} : P \rightarrow C_n \text{ where } n = 1 \]  

Assuming that \( P = x \), where \( P \) is a polynomial of higher degree. The encryption of the plaintext to ciphertext is obtained using the integration of \( P(x) \) with respect to \( x \).

In the first encryption process, when \( n = 1 \)

\[ e_{k1} = \int Pdx = \int xdx \]  

\[ k \begin{pmatrix} c_{e-1} \\ c_e \end{pmatrix} = \begin{pmatrix} p_{x-1} \\ p_x \end{pmatrix} \mod 26 \]  

\[ (13) \]
In the second encryption process when \( n = 2 \)

\[
e_{k_2} = \int C_1 dx = \int \left[ \frac{x^2}{2} + a_0 \right] dx
\]

\[
= \frac{x^3}{6} + a_0 x + a_1 = C_2 \tag{16}
\]

Such that

\[
ed_{k_n} : C_{n-1} \rightarrow C_n \quad \text{for } n > 1
\]

Also for each \( k \in K \) there are decryption algorithms in \( D \). The decryption algorithms are the derivatives of the functions. Such that

\[
d_{k_n} : C_n \rightarrow C_{n-1} \quad \text{for } n > 1
\]

In the first decryption process when \( n = 2 \)

\[
d_{k_2} = \frac{d}{dx} C_2
\]

\[
d_{k_2} = \frac{d}{dx} \left( \frac{x^3}{6} + a_0 x + a_1 \right)
\]

\[
d_{k_2} = \frac{x^2}{2} + a_0 = C_1 \tag{19}
\]

In the second decryption process when \( n = 1 \)

\[
d_{k_1} = \frac{d}{dx} C_1
\]

\[
d_{k_1} = \frac{d}{dx} \left( \frac{x^2}{2} + a_0 \right)
\]

\[
d_{k_1} = \frac{2x}{2} = x \tag{20}
\]

Such that \( d_{k_2}(e_{k_2}(d_{k_1}(e_{k_1}(p)))) = p \) for every plaintext \( p \in P \).

In other words, for every key \( k_1 \) and \( k_2 \) the function \( d_{k_2} \) and \( d_{k_1} \) is the inverse function of the function \( e_{k_2} \) and \( e_{k_1} \) respectively. In particular, this means that

\[
p = d_{k_2}(e_{k_2}(d_{k_1}(e_{k_1}(p)))) = d_{k_2}(e_{k_2}(d_{k_2}(e_{k_2}(p')))) = p'.
\]

The hybrid encryption algorithm is safest even though the encryption methods employed are known by a cryptanalyst or a hacker. Mathematically, this means that the cryptanalyst knows the functions \( e_1, e_2, d_1 \) and \( d_2 \).

This illustrates the basic premise of modern cryptography called the Kerckhoff’s Principle which says that the security of a cryptosystem depends on the secrecy of the keys and not the secrecy of the encryption algorithm itself.

If \((P, C, K, E, D)\) is to be a successful cipher, it must have the following constraint properties:

1. For any key \( k \in K \) and a plaintext \( p \in P \), it must be easy to compute the ciphertext \( e_k(p) \).
2. For any key \( k \in K \) and a ciphertext \( c \in C \), it must be easy to compute the plaintext \( d_k(c) \).
3. Given one or more ciphertexts \( c_1, c_2, c_3, \ldots, c_n \in C \) encrypted using the key \( k \in K \), it must be very difficult to compute any of the corresponding plaintexts

\[
d_k(c_1), d_k(c_2), \ldots, d_k(c_n)
\]

without the knowledge of \( k \).
4. Given one or more pairs of plaintexts and their corresponding ciphertexts \((p_1, c_1), (p_2, c_2), \ldots, (p_n, c_n)\), it must be difficult to decrypt any ciphertext \( c \) that is not in the given list without knowing \( k \). This is known as security against a chosen plaintext attack.
IV. RESULTS AND DISCUSSION

The results are presented in Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, Fig. 7 and Table 1. Five text files of different sizes were used to conduct experiments. In the experiments, comparison and evaluation were made on the performance of encryption algorithms considering their encryption time, decryption time and size of encrypted file. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme. This is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme and the new hybrid encryption model are performed. Table 1 shows the result of the comparison of Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES) and the new Hybrid Encryption Standard (HES) with respect to encryption time, decryption time and size of encrypted file.
### Table 1

**Comparison of AES, 3DES and FHES**

<table>
<thead>
<tr>
<th>S/N</th>
<th>Algorithm</th>
<th>Packet Size (KB)</th>
<th>Encryption Time (millisecond)</th>
<th>Decryption Time (millisecond)</th>
<th>Data Size of Encrypted File (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AES</td>
<td>150</td>
<td>15</td>
<td>18</td>
<td>199</td>
</tr>
<tr>
<td></td>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HYBRID (FHES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>AES</td>
<td>299</td>
<td>28</td>
<td>35</td>
<td>397</td>
</tr>
<tr>
<td></td>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HYBRID (FHES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>AES</td>
<td>443</td>
<td>35</td>
<td>49</td>
<td>529</td>
</tr>
<tr>
<td></td>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HYBRID (FHES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>AES</td>
<td>597</td>
<td>54</td>
<td>70</td>
<td>793</td>
</tr>
<tr>
<td></td>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HYBRID (FHES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>AES</td>
<td>747</td>
<td>71</td>
<td>86</td>
<td>992</td>
</tr>
<tr>
<td></td>
<td>3DES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HYBRID (FHES)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From Table 1, the time taken by new hybrid encryption algorithm for both encryption and decryption processes is much higher compared to the time taken by AES and 3DES algorithm. This makes the new hybrid encryption algorithm more secure since it will take a longer time to decrypt data. It also requires the use of two secret keys which cannot be guess easily by an unauthorized user.

---

![Fig. 5 Comparison of encryption time in AES, DES and FHES](image)

![Fig. 6 Comparison of decryption time in AES, DES and FHES](image)

Fig. 5, Fig. 6, and Fig.7 show the time taken for encryption, decryption, and the size of the encrypted file on various size of file by three algorithms.

© 2014-17, IRJCS - All Rights Reserved
V. CONCLUSIONS

A new cryptographic model to enhance the security of data both in transit and at rest was presented. The new hybrid encryption model takes much longer time compared to the time taken by the existing models. Since the hybrid algorithm takes longer time for both encryption and decryption, it makes it more secure, since the higher the encryption process the longer it will take for a hacker to break the encryption algorithm, since computing power is on the increase, speed will not be a problem in the nearest future and as such, in certain classified database, we cannot trade security with speed.

REFERENCES