Data Transfer for Secure Information by Using Symmetric Key Algorithm

Khet Khet Khaing Oo[*], Yan Naung Soe [**]

[*]Faculty of Computer Systems and Technologies , University of Computer Studies, Monywa
[**] Faculty of Information Technology Support and Maintenance , University of Computer Studies, Myitkyina

DOI: 10.29322/IJSRP.9.07.2019.p91126
http://dx.doi.org/10.29322/IJSRP.9.07.2019.p91126

Abstract- Today, it is important that information is sent confidentially over the network without fear of hackers or unauthorized access to it. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data file in order to keep the message secret. Cryptanalysis on symmetric key cryptography is encouraging the use of larger key size and complex algorithm to achieve an unbreakable state. To implement this system AES (Advanced Encryption Standard) and CBC (Cipher Block Chaining) algorithms are used. Data transfer system can prevent from interruption, destruction reparation of eavesdroppers, hacker, and blockers and so on, and can make the data secure. The implementation is written in C# using Microsoft Visual Studio 2008 and Microsoft. Net Framework v3.5.

Index Terms- AES (Advanced Encryption Standard) and CBC (Cipher Block Chaining) algorithms

I. Introduction

Cryptography is the science of information and communication security. It is also the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against authorized parties by preventing unauthorized alteration of use. Generally, it uses a cryptographic system to transform a plaintext into a ciphertext, using most of the time a key. Cryptography provides the basic for the authentication of message as well as their secrecy and integrity.

Encryption/Decryption is the main process of cryptography. In this paper, we have studies AES and CBC, symmetric encryption, in order to transfer data securely. Since the security of symmetric encryption / decryption depends on a secret key. Since this system combines the AES with CBC mode, it provides more secure data transmission than simple conventional encryption.

II. BACKGROUND AND RELATED WORK

In cryptography, there are two types of encryption algorithms: symmetric and asymmetric. In this paper, we have studied AES-CBC, symmetric encryption. Symmetric key cryptosystems are an important type of modern cryptosystems where the same key is used for both encryption and decryption [1]. Five ingredients of symmetric encryption scheme are:

1.Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

2.Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

3.Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

4.Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

5.Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext [2].

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Block ciphers in general process the plaintext in relatively large blocks at a time.

III. PROPOSED INFORMATION SYSTEM

The main objective of this paper is to introduce a secure data transfer communication system that employs cryptography to encrypt and decrypt the secret message to be transmitted over a secure channel .In this system, in order to be secure of Data Transferring. Data encryption and decryption with AES-CBC algorithm are used . Any file type such as text file, image file and audio can be transferred by using Server/ Client application. The (Figure 1) shows the main form of the Administrator or Server Site and User or client Site. User (client) Accounts are assigned in Administrator Site and User Home and Password are identified by Administrator in order that the assigned users can login to User (client) Site and remove unwanted users. Moreover, user lists of User Site can be looked at from the view of Administrator Site. Administrator can encrypt and send assigned users data or any file by clicking the Add File button and remove by clicking Remove File button.

User can login to User (client) Site, can view encrypted any file type from the administrator site and download. But, since there files are sent by encryption, user can get existing original file by the use of decryption software. So, this decryption software has to be login to the User (client) Site and user downloads any file type in User Home Page encrypted. Key and IV Numbers from the User Site are needed to decrypt, sent together with encrypted file from Administrator Site, taken and utilized by the user for the decryption stage to get the existing file again.

Mainly security is used term surround the characteristics of integrity, authentication, privacy, and Availability. Now a days we depend on the send information over the network; risk of secure transmission over the networks has also increased. For the secure transmission that term are important for data transmission.

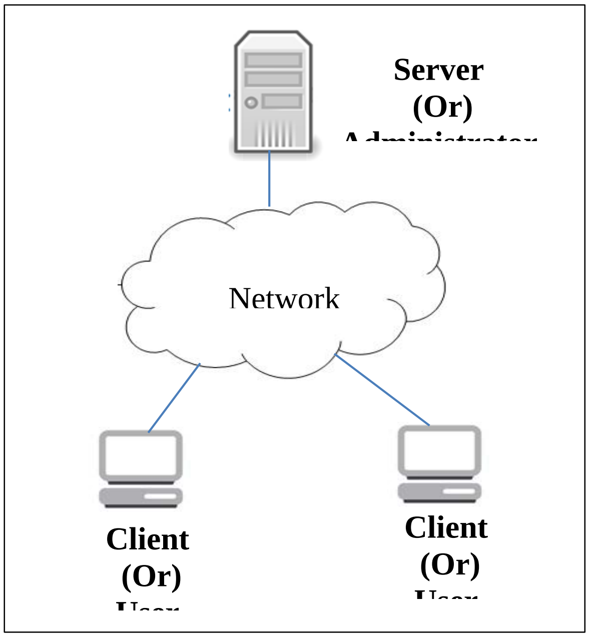


Figure 1. proposed system

IV. TECHNOLOGY USED

With the development of Science and technology, the information system is essential in our daily life. Cryptocurrencies emulate the concept of real world signatures by using cryptography techniques and the encryption keys. Cryptography methods use advanced mathematical codes to store and transmit data values in a secure format. Cryptography is a technique to send secure messages between two or more participants – the sender encrypts/hides a message using a type of key and algorithm, sends this encrypted form of message to the receiver, and the receiver decrypts it to generate the original message [3]. The System presented in this paper used the symmetric (AES) and CBC algorithms to implement the system for secure data transfer.

Advanced Encryption Standard (AES)

The development of data techniques the The development of data techniques the problem of data security becomes more and more important. In cryptography, AES is one of the most popular algorithms used in symmetric key encryption. AES is one of the most popular algorithms used in symmetric key cryptography . It is available by choice in many different encryption packages. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits can produce a corresponding output of the same size . AES is fast in both software and hardware, is relatively easy to implement, and requires little memory [1]. AES is used by the vast majority of network-based symmetric cryptographic application. AES is a substitution permutation process, which is a series of mathematical operations that use substitutions (also called S-Box) and permutations (P-Boxes) .

AES Encryption algorithm

```
1) Key Expansion
2) Initial round
        a. AddRoundKey
3) Nr -1 Round
        a. SubBytes
        b. ShiftRows
        c. MixColumns
        d. AddRoundKey
4) Final Round
        a. SubBytes
        b. ShiftRows
        c. AddRoundKey
```

AES uses variable number of rounds (Nr) which are fixed: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [5]. During each round, above operations are applied on the state.

- SubBytes: The substitute bytes operation is a nonlinear byte substitution that operates on each of the state bytes independently using S-box and changes the byte values.
- ShiftRow: every row in the 4x4 ray is shifted a certain amount to left depending on the row index.
- MixColumn: The mixcolumns transforma-tion uses a mathematical function to transform the values of a given column within a state, acting on the four values at one time as if they represented a four-term polynomial.
- AddRoundKey: each byte of the state is combined with a round key, which is a different key for each round and derived from the AES (Rijndael) key [1].

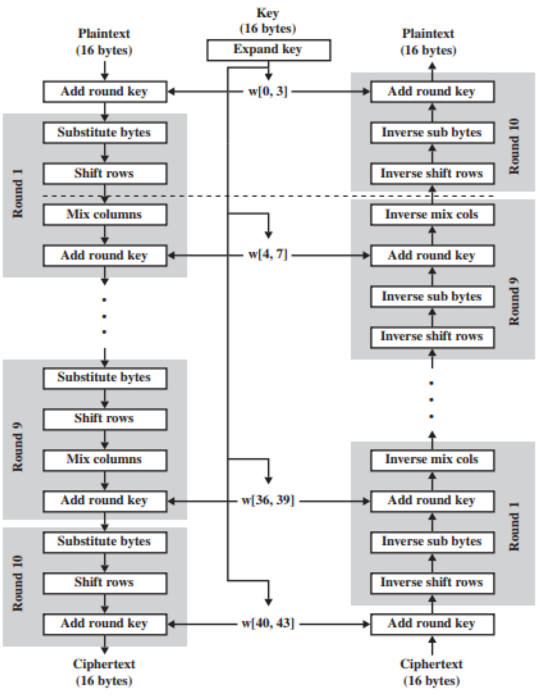
(Means and variances of the variables) necessary for classification.

AES Decryption algorithm

```
1) Key Expansion
2) Initial round
        a. AddRoundKey
3) Nr -1 Round
        a. Inverse Shift Row
        b. Inverse Sub Bytes
        c. AddRoundKey
        d. Inverse MixColumns
4) Final Round
        a. Inverse Shift Row
        b. Inverse Sub Bytes
        c. AddRoundKey
```

AES decryption uses essentially the same algorithm, with the following changes: the inverse of the four main operations are used.

- Inverse Shift Row: The inverse shift row transformation, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a 1-byte circular right shift for the second row, and so on [4].
- Inverse Sub Bytes: Inverse Sub Bytes is the inverse of the byte substitution transformation, in which the inverse S-box is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (2^8) [1].
- Inverse MixColumns: Inverse Mix Columns is the inverse of the Mix Columns transformation. Inverse Mix Columns operates on the State column-by-column, treating each column as a four-term polynomial as described [5].
- AddRoundKey: The round keys are used in the reverse order.



(a) Encryption (b) Decryption

Figure 2.AES-128 is a 10 round block cipher encryption and decryption algorithm

Cipher block chaining (CBC)

In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block; the same key is used for each block. In effect, we have chained together the processing of the sequence of plaintext blocks. The input to the encryption function for each plaintext block bears no fixed relationship to the plaintext block. Therefore, repeating patterns of bits are not exposed. As with the ECB mode, the CBC mode requires that the last block be padded to a full bits if it is a partial block.

For decryption, each cipher block is passed through the decryption algorithm. The result is XORed with the preceding ciphertext block to produce the plaintext block [4].The AES-CBC encrypted as shown in (Figure 3).

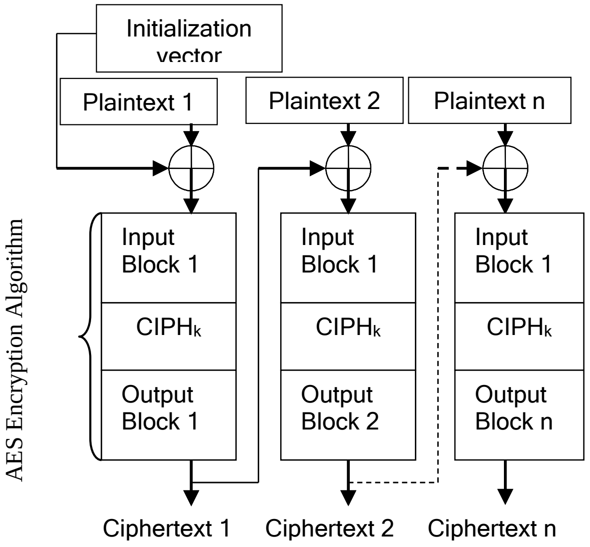


Figure 3. AES-CBC encryption

In AES-CBC encryption, the first input block is formed by XOR the first block of the plaintext with IV. The AES cipher function is applied to each input block to produce the ciphertext block (output block). With CBC mode, an XOR is performed on the input plaintext and the previously ciphertext block (output block). Since previously encrypted data is not available for the first operation an initialization vector (IV) must be provided. CBC works on complete 128-bits blocks of plaintext. In AES-CBC decryption, the AES inverse cipher function is applied to the first ciphertext block, and the resulting output block is XOR with the IV to recover the first plaintext block. In general, to recover any plaintext block (except the first), the AES inverse cipher function is applied to the corresponding ciphertext block, and the resulting block is XOR with the previous ciphertext block as shown in (Figure 4).

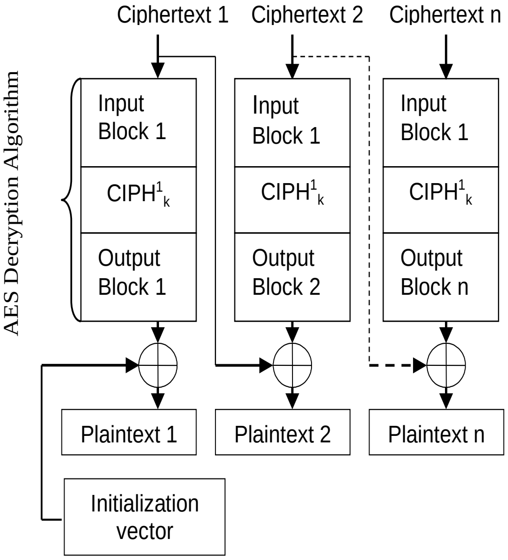


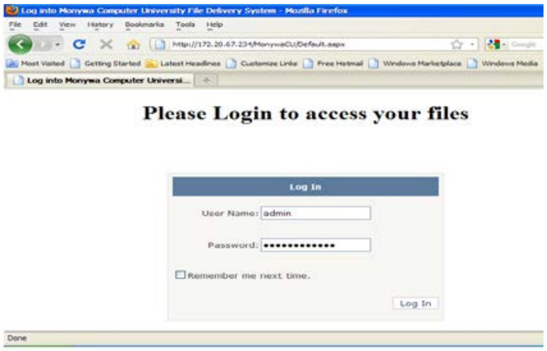
Figure 4. AES-CBC decryption

A common way to achieve the necessary increase is to append some extra bits, called padding, to the trailing end of the data string as the last step in the formatting of the plaintext. Other methods may be used; in general, the formatting of the plaintext is outside the scope of this recommendation. The padding bits can be removed unambiguously provided the receiver can determine that the message is indeed padded. One way to ensure that the receiver does not mistakenly remove bits from an unpadded message is to require the sender to pad every message, including messages in which the final block (segment) is already complete.

V. IMPLEMENTATION OF SECURE DATA TRANSFER SYSTEM

A. Login Page

In the Login page, the user needs to fill the security information (such as Administrator user Name and Password) to access the system. If the User Name and Password is correct, the user can enter to the Users Option.


Log into Monywa Computer University File Delivery System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.20.67.234/MonywaCU/Default.aspx
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media
Log into Monywa Computer Universi...
Done

Please Login to access your files

Log In

User Name: admin

Password: ●●●●●●●●●●●●●

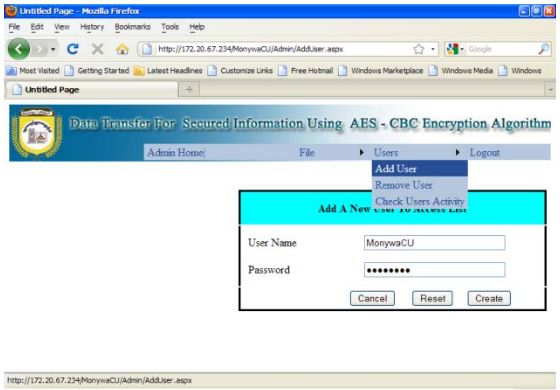
□ Remember me next time.

Log In

Figure 5. Administrator form

B. Create Add User

From the Users Option Tab, the user can choose to go to Add User, Remove User and Check User Activity Page. In the Add User page, the user needs to fill new User name and password to create the system.


Untitled Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.20.67.234/MonywaCU/Admin/AddUser.aspx
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows
Untitled Page
Admin Home
File
Users
Logout
Add User
Remove User
Check Users Activity
http://172.20.67.234/MonywaCU/Admin/AddUser.aspx

Data Transfer For Secured Information Using AES - CBC Encryption Algorithm

Add A New User To Access List

User Name: MonywaCU

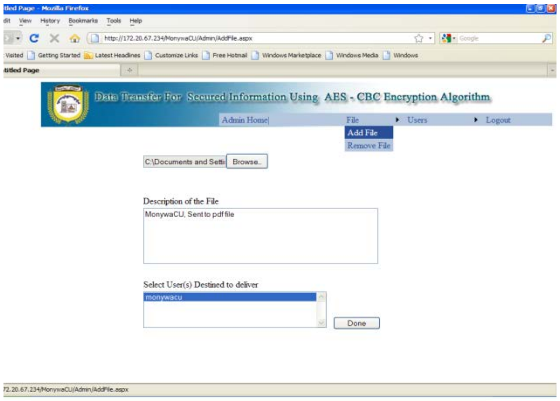
Password: ●●●●●●●●

Cancel Reset Create

Figure 6. Add user

C. Encryption and Sending Any Files

In Figure 7, shows: the administrator can choose the files that files that is transmitted from the file menu. When File menu is click, Add File sub menu is appeared. It can be added files to deliver operation and can be selected user(s). Who can download the files when Add File sub menu is clicked.


Untitled Page - Mozilla Firefox
Edit View History Bookmarks Tools Help
http://172.20.67.234/MonywaCU/Admin/AddFile.aspx
Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows
Untitled Page
Admin Home
File
Users
Logout
Add File
Remove File
72.20.67.234/MonywaCU/Admin/AddFile.aspx

Data Transfer For Secured Information Using AES - CBC Encryption Algorithm

C:\Documents and Setti Browse..

Description of the File: MonywaCU, Sent to pdf file

Select User(s) Destined to deliver: monywacu

Done

Figure 7. Encryption and sending any file

D. Encrypted file

User receive encryption file

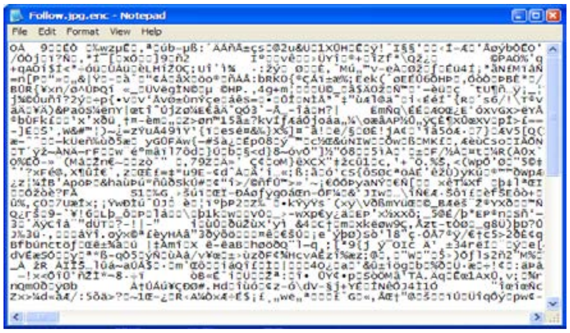
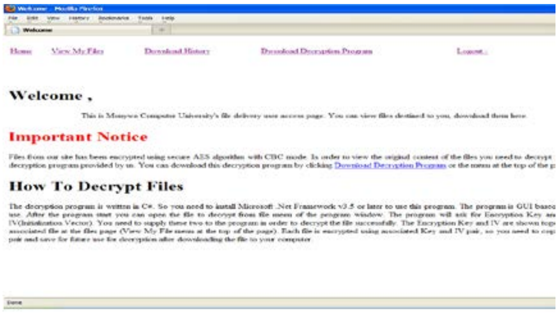


Figure 8. Encrypted file

E. User home page

The User Home page , It can be managed the process that Encrypted file and IV (Initialization Vector) and key are downloaded.


Welcome - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Welcome
Home
View My Files
Download History
Download Decryption Program
Logout
Done

Welcome ,

This is Monywa Computer University's file delivery user access page. You can view files destined to you, download them here.

Important Notice

Files from our site has been encrypted using secure AES algorithm with CBC mode. In order to view the original content of the files you need to decrypt decryption program provided by us. You can download this decryption program by clicking Download Decryption Program or the menu at the top of the p

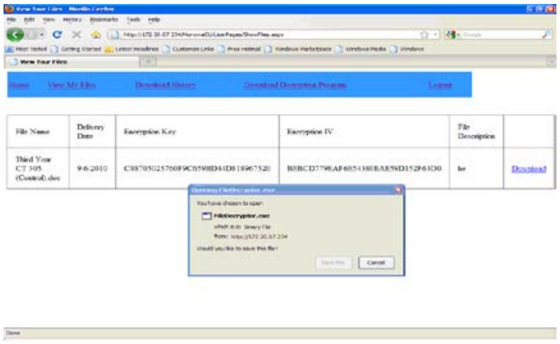
How To Decrypt Files

The decryption program is written in C#. So you need to install Microsoft .Net Framework v3.5 or later to use this program. The program is GUI based use. After the program start you can open the file to decrypt from file menu of the program window. The program will ask for Encryption Key and IV(Initialization Vector). You need to supply these two to the program in order to decrypt the file successfully. The Encryption Key and IV are shown toge associated file at the files page (View My File menu at the top of the page). Each file is encrypted using associated Key and IV pair, so you need to cop pair and save for future use for decryption after downloading the file to your computer.

Figure 9. User home page

F. Download to decrypt program

The download files lists and its IV and Key can be seen from View My Files menu.


View Your Files - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.20.67.234/PersonalCU/UserPages/ShowFiles.aspx
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Windows Marketplace Windows Media Windows
View Your Files
Home View My Files Download History Download Decryption Program Logout
Done

File Name	Delivery Date	Encryption Key	Encryption IV	File Description	
Third Year CT 305 (Control).doc	9-6-2010	C88705025760F9C6598D44D818967520	B8BCD779EAF6854380BAB59D152F63D0	he	Download

Opening FileDecryptor.exe

You have chosen to open:

FileDecryptor.exe

which is: Binary File

from: http://172.20.67.234

Would you like to save this file?

Save File | Cancel

Figure 10. Download to decrypt program

G. Decrypted File

Show the condition is called decrypt the original file. When the encrypted file has been decrypted, asked for the please to save the decrypted file. It can be seen the original file when the saved file is opened.

Figure 11. Decrypted file

VI. CONCLUSION

This system implements secure data transfer system using AES algorithm and CBC mode their advantages can be taken to support an encryption/ decryption technique for the client /server system. While the performance of symmetric key cryptography that is implemented using only block cipher algorithms. Therefore, this system provides not only authentication but also confidentiality by using symmetric encryption.

REFERENCES

[1] https://github.com/gittejas/aes128

[2] https://flylib.com/books/en/3.190.1.29/1/

[3] https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

[4] https://wanguolin.github.io/assets/cryptography_and_network_security.pdf

[5] https://www.slideshare.net/nikhilgupta131/aes128-bit-projectreport

AUTHORS

First Author – Khet Khet Khaing Oo, Faculty of Computer Systems and Technologies , University of Computer Studies, Monywa

Second Author – Yan Naung Soe, Faculty of Information Technology Support and Maintenance , University of Computer Studies, Myitkyina