An Efficient Data Storage in Cloud Computing Using Advanced Encryption Standard Algorithm

[1]M. Kumaran, [2]A. Manimaran, [3]G. Sundararaju, [4].V.Seedha Devi,
[5]R. Loganathan

1, 2, 3. Assistant Professor, Department of Computer Science and Engineering, Jaya Engineering College
4. Associate Professor Department of Computer Science Engineering, Jaya Engineering College
5. Professor, Dept. of Textile Technology, Jaya Engineering College Chennai 602024,INDIA.
Email: kumaran.ma@gmail.com

Article Info
Page Number: 8574-8580
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 15 September 2022
Revised: 25 October 2022
Accepted: 14 November 2022
Publication: 21 December 2022

Abstract

The main objective of this paper is to transfer files using various protocols like Ftp, Sftp, Scp etc. It provides the feature of the master password that the password is protected by a strong AES cipher. It provides host as well as credential security. this paper optimizes the Advanced Encryption Standard (AES) in the Cloud environment. The analysis shows that Advanced Encryption Standard has better security and is therefore suitable for encrypting data in the Cloud environment. Now, security issues are another huge challenge facing the rapid development of the Cloud environment. Encryption technology can provide effective protection for data security of the Cloud environment.

Key words: Cloud Computing, encryption standard, Advanced Encryption Standard Algorithm, information security

1. INTRODUCTION

Usender is an open source free SFTP client, FTP client, WebDAV client, S3 client and SCP client for Windows. Its main function is file transfer between a local and a remote computer. Beyond this, usender offers scripting and basic file manager functionality. The system offers file sharing from local to remote computers using various multiple protocols. It offers various features like file encryption, compression, decompressing etc. It also provides scripting and task automation. various file related operations can be performed like file navigation, synchronization, delete. Usender provides the feature of the master password that the password is protected by a strong AES cipher. It provides host as well as credential security. Usender provides an easy graphical user interface for file transfer using multiple protocols like Ftp, Sftp, WebDAV, Scp etc. Usender is used for all common operations with files. You can start editing a file directly from Usender either using the Usender internal text editor or using integration with your favourite external text editor. Usender operations are not limited to individual files; usender offers several ways to synchronize your remote and local directories.

2. Objective

The main objective of this project is to transfer files using various protocols like Ftp, Sftp, Scp etc. It provides the feature of the master password that the password is protected by a strong AES cipher. It provides host as well as credential security

3. Existing System

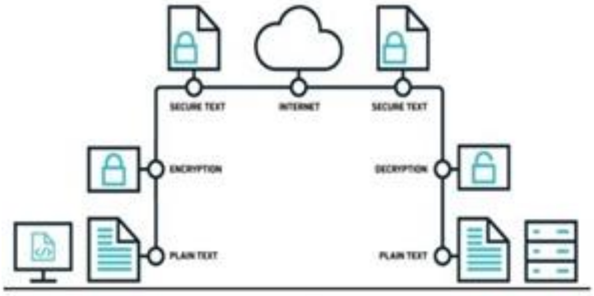
The existing system of this project provides file transferring. Using this user can upload or download the files. To transfer files some basic protocols are used. The existing system provides a graphical user interface to the user.

4. Proposed System

In proposed system, we have used various protocols for file transferring. This system also uses AES chipper for password protection which is used for system login. This application provides various system features like scripting and task automation. various file related operations can be performed like file navigation, synchronization, delete. It provides host as well as credential security. Usender provides an easy graphical user interface for file transfer using multiple protocols like Ftp, Sftp, WebDAV, Scp etc. Usender is used for all common operations with files. You can start editing a file directly from Usender either using the Usender internal text editor or using integration with your favorite external text editor. Usender operations are not limited to individual files; usender offers several ways to synchronize your remote and local directories. Usender provides the feature of the master password that the password is protected by a strong AES cipher. It provides host as well as credential security.

5. Related Works

5. 1 System Architecture

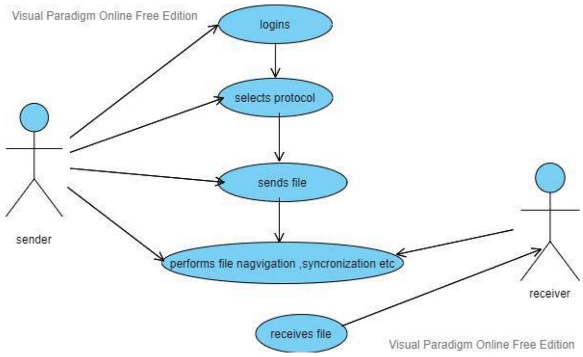


The above diagram clearly describes the process undergone during file transfer. The file which is in plain text format is encrypted and converted into secure text through the internet using protocol, the file is transferred to the receiver’s computer which does not compromise in the quality. This system helps the user to download the file from the remote server. For sending or receiving the file the user just needs to drag and drop the file from the remote server or local directory. The user can also undergo various transfer session with different users. It doesn’t even take minutes for transferring files

5.2 Uml Diagrams

5.2.1 Use Case Diagram

Use case diagrams are employed in UML (Unified Modelling Language), A standard notation for modeling of real-word objects and systems. Describes both the static structure and the dynamic behavior of the system.In many ways, a communication diagram is a simplified version of a collaboration diagram introduced in UML State Diagram. These static parts are represented by classes, interface, objects, components and nodes. Class diagram basically represent the object-oriented view of the system which is static in nature.


Visual Paradigm Online Free Edition
logins
selects protocol
sends file
sender
performs file nagvigation ,syncronization etc
receiver
receives file
Visual Paradigm Online Free Edition

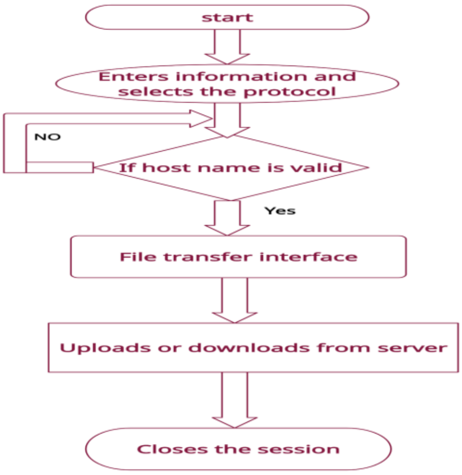
Use Case Diagram

The boundary, which defines the system of interest in relation to the world around it. The actors, usually individuals involved with the system defined according to their roles. The use cases, which specific roles are played by the actors within and around the system. The relationship between and among the actors and the use case. UML diagrams that drawn by visual paradigm, such as the use case, class, state machine, sequence, collaboration, activity and component use case diagram help of the actors, user, and the system.

5.1.2Data Flow Diagram

Data flowcharts are a way of displaying how data flows in a system and how decisions are made to control events. To illustrate this, symbols are used. They are connected together to show what happens to data and where it goes.

The following data flowdiagram depicts the process involved in the scenario and sequence of data flows when a file is transferred.


start
Enters information and selects the protocol
NO
If host name is valid
Yes
File transfer interface
Uploads or downloads from server
Closes the session

Data flow Diagram

5.3 Human Interface Design

The user interface, in the industrial design field of human interaction diagram, is the space where interactions between humans and machines occur. The goal of this interaction is to allow effective operationand control of the machine from human's end, whilst the machine simultaneously feeds back information that aids the operator's decision-making process. The goal of user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesirable outputs to human.

6. Algorithm

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys

6.1 Encryption

Encryption is a popular techniques that plays a major role to protect data from intruders. AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-process. Each round consists of the following four steps to encrypt 128 bit

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes

This step implements the substitution.

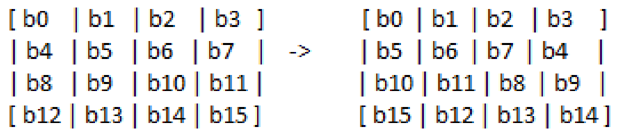
In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :

This step is just as it sounds. Each row is shifted a particular number of times.

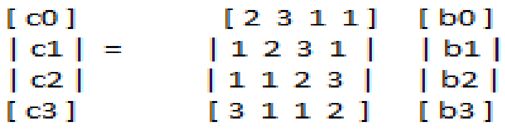
- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.



```
[ b0  | b1  | b2  | b3  ]        [ b0 | b1 | b2  | b3   ]
| b4  | b5  | b6  | b7  |   ->   | b5 | b6 | b7 | b4    |
| b8  | b9  | b10 | b11 |        | b10 | b11 | b8 | b9  |
[ b12 | b13 | b14 | b15 ]        [ b15 | b12 | b13 | b14 ]
```

Mix Columns

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.



```
[ c0 ]         [ 2 3 1 1 ]   [ b0 ]
| c1 |  =     | 1 2 3 1 |   | b1 |
| c2 |        | 1 1 2 3 |   | b2 |
[ c3 ]        [ 3 1 1 2 ]   [ b3 ]
```

Add Round Keys

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

6.2 Decryption

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

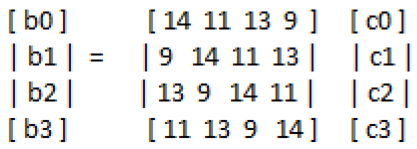
The stages of each round in decryption are as follows:

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.



```
[ b0 ]       [ 14 11 13 9 ]   [ c0 ]
| b1 | =    | 9  14 11 13 |   | c1 |
| b2 |      | 13 9  14 11 |   | c2 |
[ b3 ]       [ 11 13 9  14 ]  [ c3 ]
```

Inverse SubBytes:

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

7. Results

The user enters the login details and selects the protocol. The password, file name and file content are encrypted using AES algorithm. After login user is directed to the transfer interface. Here the user can drag and drop from to the remote directory and perform upload and download files. This provides many features to users. Using this user can transfer and receive files within seconds. This system also does not compromise the quality of the file.

8. Conclusion and Future Enhancement

8.1 Conclusion

This system proposes the ideology of transferring files using protocols. The user enters the login details and selects the protocol. The password, file name and file content are encrypted using AES algorithm. After login user is directed to the transfer interface. Here the user can drag and drop from to the remote directory and perform upload and download files. This provides many features to users. Using this user can transfer and receive files within seconds. This system also does not compromise the quality of the file.

8.2Future Enhancement

Future work will extend the proposed system. This system can be used only in windows this can be enhanced in future. To use the system the user requires basic knowledge about protocols and system, in future the user friendliness of the system can be improved.

1. Ying Liu, Wei Zhang, XinxiaPeng,Yan Liu, Sida Zheng andTongjia Wei(2019)**“*Design of password encryption model based on AES algorithm*”** IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) .
2. NaSu,Yi **Zhang and Mingyue** Li(2019) **“*Data Encryption Standard Based on AES Algorithm*”** IEEE 1st International Conference on Civil Aviation Safety and Information Technology (ICCASIT).
3. **Elbaz, C., Rilling, L., and Morin, C.,**“Reactive and Adaptive Security Monitoring in Cloud Computing”,Proc. - 2018 IEEE 3rd Int. Work. Found. Appl. Self* Syst. FAS*W 2018, Vol. 4, No. 3, pp. 5–7, 2019, doi: 10.1109/FAS-W.2018.00014.
4. **Kankhare, D. D., and Manjrekar, A. A.,**“A cloud Based System to sense Security Vulnerabilities of Web Application in Open-Source Private Cloud IAAS”,2016 Int. Conf. Electr. Electron. Commun. Comput. Optim. Tech. ICEECCOT 2016, Vol. 5, No. 3, pp.252–255,2017.
5. **Xiong, L. and Xu, Z.**“Re-encryption Security Model over Outsourced Cloud Data”,IET Conf. Publ., Vol. 2013, No. 643 CP, pp. 1–5, 2013, doi: 10.1049/cp.2013.2473.
6. **Qian, H., and Wen, Q.,**“A Cloud Based System For Enhancing Security of Android Devices”,Proc. IEEE CCIS2012 A, Vol. 6, No. 4, pp. 245–249, 1857.
7. **Elsayed, M. and Zulkernine, M.** “Towards Security Monitoring for Cloud Analytic Applications”, Proc. - 4th IEEE Int. Conf. Big Data Secur. Cloud, BigDataSecurity 2018, 4th IEEE Int. Conf. High Perform. Smart Comput. HPSC 2018 3rd IEEE Int. Conf. Intell. Data Secur., Vol. 7, No. 5, pp. 69–78, 2018.