International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-169
Volume: 6 Issue: 4 117 - 119

Enhancing the Security of AES Using Variable Key Cipher

[1]Siddhesh Bakshi,[2]Siddhesh Inamdar,[3]Unnati Khatu,[4]Pranav Sahu, [5]Dr. Sunil Wankhade.
Student,Dept of I.T, Rajiv Gandhi Institute of Technology, Mumbai, India.
Head and Professor, Dept of I.T, Rajiv Gandhi Institute of Technology, Mumbai, India.

***Abstract*—**Web hosting provides the ability to utilize resources through Internet. As a lot of service providers for hosting the web page are available in the competitive computer world. Security for a website is an important and critical aspect, and has numerous issues and problem related to it. In this we will discuss how to provide security for the data from the unauthorized users and provide integrity to the users. It requires a very high degree of privacy and authentication. To protect the data in the database server, cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as AES (Advanced Encryption Standard) hybridized with ECC (Elliptical Curve Cryptography) algorithm which gives enhanced security. It is based on several substitutions, permutation and transformation. .

Keywords*-AES, ECC Algorithm, Cryptopgraphy, Web Hosting, Admin, Users.*

*****

I. INTRODUCTION

Web hosting is a type of service using which individuals or companies can host their webpages on the internet by paying a nominal fee. For web hosting it is essential to have a domain name. Domain name helps finding the website easily on the internet.

The project follows a one to many schema. There is one admin and multiple users. The admin has the authority to add and remove data from the database. He also uploads files into the database. The files will be encrypted using a random key that will be generated automatically with the help of AES algorithm. When the user wants to access a particular file sent to him by the admin, he logs into the website and then proceeds to download the particular file. The user will be mailed his secret key so as to use it to download the particular file. If in case the key is entered incorrectly, the file cannot be downloaded.

II. LITERATURE SURVEY

The goal of web security is mainly to concentrate on the issues related to the data security and privacy features in cloud computing. In proposed system the multi cloud model is based on data storage on distinct cloud and then encrypts data using AES algorithm technique is used for efficient storage of data in cloud servers.

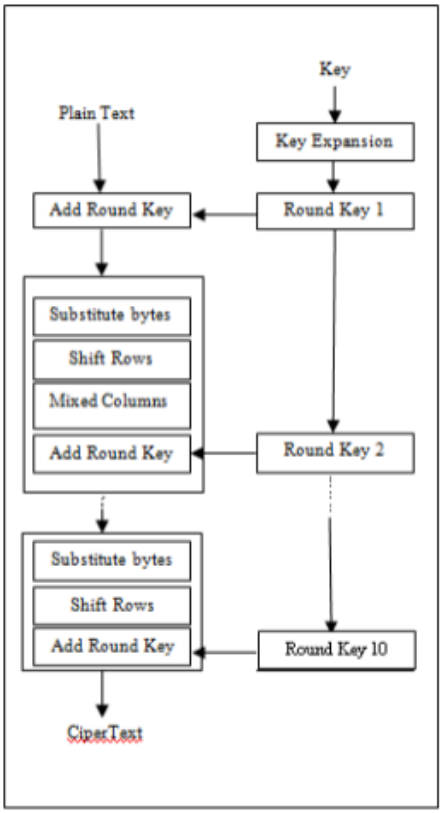
A. AES Algorithm

AES (Advanced Encryption Standard) is a symmetric encryption technique. The algorithm was proposed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be effective in both hardware and software; AES is block cipher which supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES algorithm operates on a 4×4 column-major order matrix of bytes, called as the state.

Algorithm:

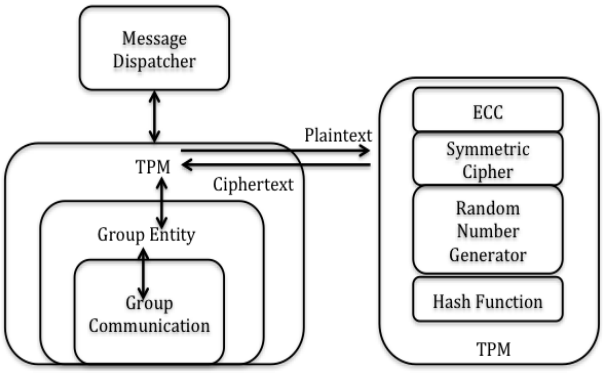
1. Key Expansion—round keys are obtained from the cipher key using Rijndael's key schedule. AES needs a separate 128-bit round key block for each round plus one more.
2. Initial Round and AddRoundKey—each byte of the state is merged with a block of the round key using bitwise xor.
3. Rounds Sub Bytes—the non-linear substitution step in which each byte is returned with another using a lookup table. Shift Rows—a transposition step in which the last three rows of the state are moved cyclically a definite number of steps. Mix Columns—a mixing operation which performs on the columns of the state, merging the four bytes in each column. AddRoundKey

4 .Final Round (no Mix Columns) Sub Bytes Then Shift Rows And AddRoundKey.



B. ECC Algorithm

Elliptical curve cryptography (ECC) is based on a public key cryptosystem based system that is on elliptic curve theory. Elliptic Curve Cryptography can be used to create smaller, faster, and more efficient cryptographic keys. ECC authentication scheme is more suited for wireless communications, like mobile phones and smart cards, personal information like financial transaction or some secret medical reports, confidential data where main consideration is to provide secure data.



III. Proposed System

In proposed system the model is based on data storage on distinct cloud and then encrypts data using AES technique is used for efficient storage of data.

ADMIN LOGIN:- IN THIS MODULE, THE ADMIN LOGS INTO THE SYSTEM USING USERNAME AND PASSWORD. IF USERNAME AND PASSWORD MATCHES THEN THE ADMIN GETS ACCESS TO THE ADMIN APPLICATION WEBPAGE.

1. **User Login**:- In this module, the user login into the system using username and password. If username and password matches then receiver gets access to the user side application webpage.

2. **Encryption Module**:- In the module sender enter the message which is send to the receiver. He/ She encrypts the message using AES used in combination with ECC **.**

3. **Decryption Module**:-Receiver decrypt the message using the private key mailed to him by the admin.

The proposed system consists of a webpage which can be accessed by an administrator as well as users. The administrator has the authority to add or remove users from the database. Also the authority to manage files like uploading files and sharing files with users lies with the administrator. When the administrator adds a new user's details into the database, immediately a mail is sent to the user which contains details of the user's login details. When the administrator uploads any file for storing, the file undergoes encryption. A secret key generated using AES ALGORITHM in combination with ECC ALGORITHM encrypts the file. When a user requests for a particular file, the administrator selects that file and uploads it for the user to download. When the user logs into the website using his login credentials, he sees the file name as well as a download button. When he clicks the download button, he is prompted to enter the secret key used for encrypting the file in order to decrypt and download it. The secret key is mailed to him by the administrator. The file is downloaded when the key is entered correctly.

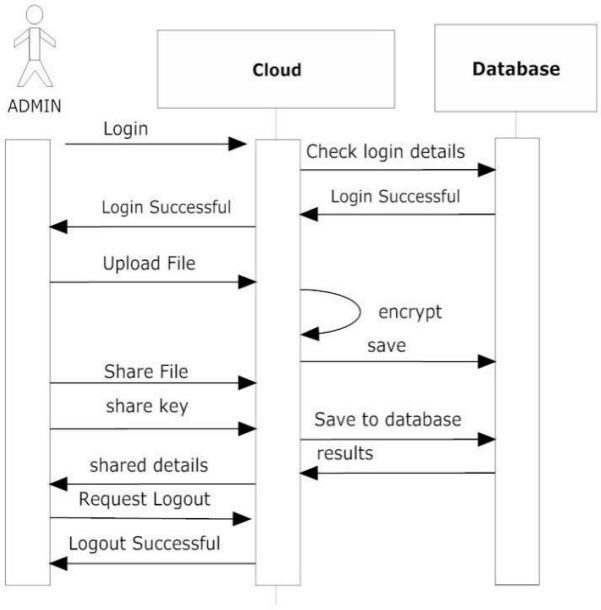


Fig: Admin side activity

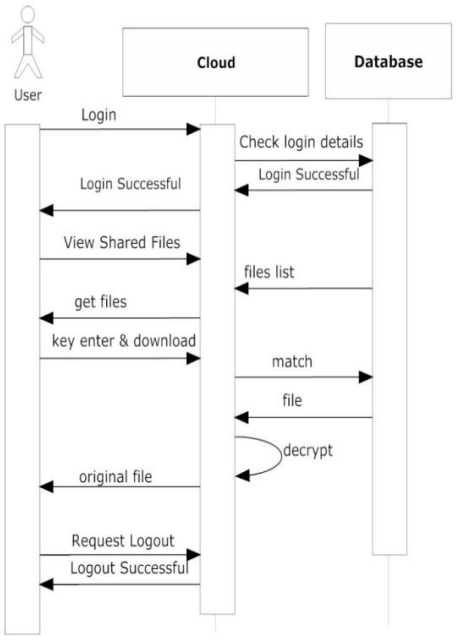


Fig: User side activity

IV. RESULTS

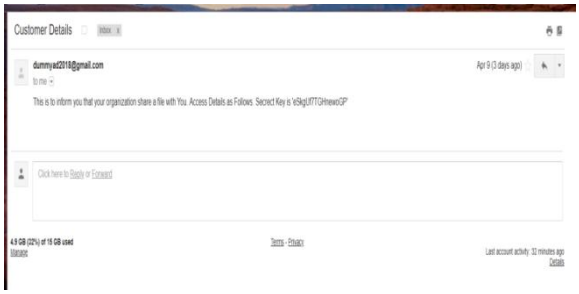
1. The admin logs in with his id and password on the admin login page

2. The admin has the authority to add new users as well as to share files with existing users.

3. By selecting the add new user button , the admin can easily add a new user.

4. When the user tries to download the file as sent to him by the admin, he is first asked for the security key. If he enters the key correctly, he can download the file. Incorrect submission of the key will prevent him from downloading the file.

5. The secret key is automatically mailed by the admin to the user as the admin uploads the file for the user.



5. User login interface.

REFERENCES

[1] Chakradhara Rao and A.V.Ramana DATA SECURITY IN CLOUD COMPUTING International Journal of Current Trends in Engineering & Research (IJCTER).

[2] Vishal R. Pancholi Dr. Bhadresh P. Patel Matrushri L.J Gandhi (Bakorvala)and Enhancement of Cloud Computing Security with Secure Data Storage using AES.

[3] Sreedhar Acharya B. and Dr. M. Siddappa A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Cloud Computing International Journal of Applied Engineering Research

[4] Andrew S.Tanenbaum Computer Network

[5] Monjur Ahmed and Mohammad Ashraf Hossain, “Cloud Computing and Security Issues in the Cloud”, in computing and Information Sciences, ISSN 2079- 8407, VOL.3, No.3, MARCH 2012