ISSN 2395-1621

A Survey on Private Data Security System Using Half Image based Password on Cloud Computing

Sarang Rajurkar, Amar Memane, Rakhi Kale, Murlidhar Pathak

Department Of Computer Engineering

Jspm's Imperial College Of Engineering And Research
Wagholi, Pune 412207 Savitribai Phule Pune University.

ABSTRACT

Secure data process it can significantly reduce the data protection watch from admin and server security provider. Existing data security password protection is very low security and easy to guess to attacker like combination of special symbols, number and character, captcha based password, pattern based password and biometric based password. So all these problems overcome based on the combination of different technique to generate the high security based image based half encrypted password. In this system, use the steganography, encryption, encoded and splitting technique to generate the secure password to authenticate the private organization to access the important files and data from the server.

Keywords: AES, Stegno, Data Privacy, Data Encryption, OTP Analysis.

ARTICLE INFO

Article History

Received: 3rd June 2021

Received in revised form :

3rd June 2021

Accepted: 5th June 2021

Published online :

5th June 2021

I. INTRODUCTION

Information security is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in the world any data center across the network geographically distributed. The cloud computing analysis serious problems and issues based on the user authentication process, information integrity mean any user can modify data or not and data confidentiality mean data losses. So design the proposed system to implement an enhanced new technique to secure private important data and apply algorithm in order to optimize the data and minimize the Confidentiality, Integrity and Authentication problems.

In these system users storing and accessing the data from server and to data centers. In cloud computing and other environment area provide the security using the different technique like, Cryptography Process, Steganography Technique and many more.

A. Cryptography Mechanism

Encryption:
Encryption Process is the mostly used to every environment to provide the security to data, image, video and many more application. Encryption process is conversion of the plain text to cipher text. Here in this paper system use encryption process on the image to generate the encrypted image as an image based encrypted password. All these process is carried out on server side.

Decryption:
The decryption process is the reverse process on encryption, it mean cipher text to plain text. When decrypt the image then server know the its valid image or not.

Fig 1. Image Encryption and Decryption Process

B. Steganography Mechanism:

Image Steganography:
The process of concealing the secret message in an image file is known as image steganography. It has certain limitations like you cannot embed a large amount of data in an image because it may distort which may arise suspicion that the image might contain any information.

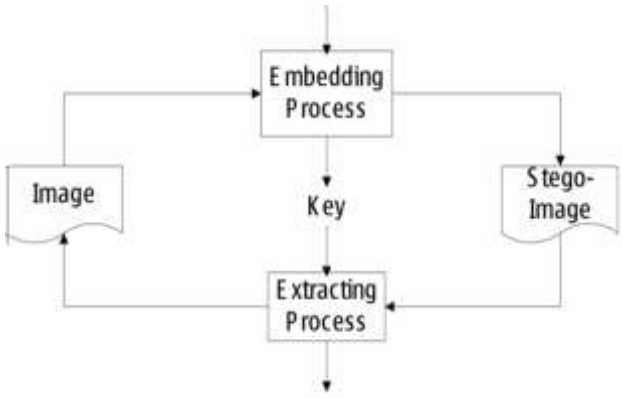

Fig 2. Image Steganography Process

II. PROBLEM STATEMENT

The existing system for password creation is very simple and easy to create by any human. The human set the short or easily-guessing passwords, based on character, number and special symbol. So our proposed system is authentication by Secure Encrypted Image based password.

III. LITERATURE SURVEY

[1] Farhana Zaman Glory, A tif U Aftab, "Strong Password Generation Based On User Inputs"
Description: Passwords can defend against two password cracking attacks named the "Dictionary attack" and the "Brute Force attack". The reliability of our generated passwords is entirely satisfactory.
Limitation: Here only word on the limited attack possibilities and input is based on user.

[2] Mohammad Mohammadin odoushan, "Implementation of Password Management System Using Ternary Addressable PUF Generator"
Description: The architecture takes advantage of known technology modules such as SRAM PUFs, hash functions, and microcontrollers.
Limitation: One of the problems with the presented password management is the potential loss of the password by the user. The password management cannot erase the message digest because the address in the look-up table is also lost.

[3] Yu-Chi Chen, Tsung-Hsuan Hung, Sung-Hsien Hsieh, and Chih-Wei Shiu, "A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms"
Description: New technique by using multi-secret sharing as the underlying encryption, which indeed induces a blow-up issue of the key size. For preserving the efficiency of the key size, apply a compression by using lightweight cryptographic algorithms.

Limitation: Its take time for generation of password and verification. The accuracy of password verification is fail sometimes.

[4] Jannatul Bake Billa, Anika Nawar, "PassMan: A New Approach of Password Generation and Management without Storing"
Description:
The system should provide the users with a safer feeling to use password manager systems as it becomes more secured and non-volatile.
Limitation:
This system is not user friendly. As our application does not save any information in the Cloud for further verification.

IV. PROPOSED SYSTEM

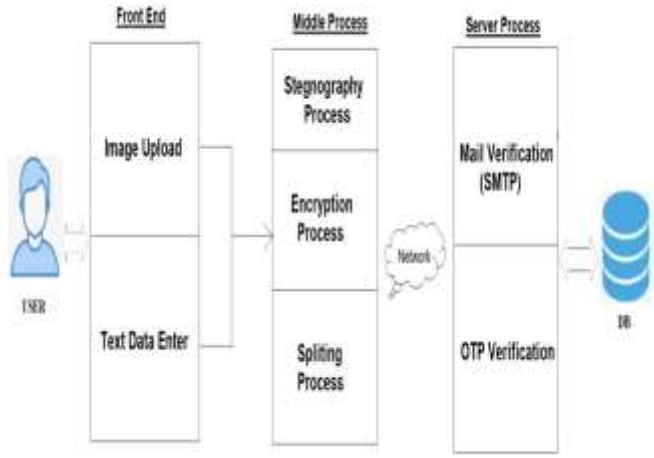

Fig 3. System Block Diagram

A. Description:

User Module:
On the user side, a user provide the his/her username and password to the server. Then, the get method to catch the username and plain password are transmitted to the server through a secure channel.

Steganography Module:
If the received password is provide the steganography process for hiding the data in to the image.

Encryption Module:
Once data hide in the above (2) stage is then provide the secure encryption process and image splitting technique is applied.

Splitting Process Module:
Finally every user will get the secure half image and another half image to the data server.

B. Algorithm:

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it

divides a message up into fixed length blocks during encryption and decryption.

C. Mathematical Model

Our system can be represented as a set
System S = {I, O, C, E, S}
Where,
I=set of inputs
O=set of outputs
C = set of constraints
E = Encryption using blowfish and
S= Steganography for data hide
I=Input:
Input I = {image upload, user details, username, password}
O=Output:
Output O = {Encryption done, successfully access data, notification}
C=Constraint
C = {C1, C2}
Where,
C1 = "User should enter a valid data for generate the secure image".
C2 = "Client machine and server should always be connected to the local server for requesting any data and response to from the server."

V. CONCLUSION

Image based password to secure private company files and data access from secure server. It secures the database server from unauthorized user. These systems also check valid mail ids and Mobile number for reducing unknown mail ids and number. This method is mainly concerned with preventing identity theft and prevents phishing. It also was providing customer data security.

VI. REFERENCES

[1] Farhana Zaman Glory, A tif U Aftab, Strong Password Generation Based On User Inputs,IEEE 2019.

[2] Mohammad Mohammadin odoushan, Implementation of Password Management System Using Ternary Addressable PUF Generator, IEEE 2019.

[3] Yu-Chi Chen, Tsung-Hsuan Hung, Sung-Hsien Hsieh, and Chih-Wei Shiu A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms, IEEE 2019.

[4] Yu-Chi Chen, Tsung-Hsuan Hung, Sung-Hsien Hsieh, and Chih-Wei Shiu, PassMan: A New Approach of Password Generation and Management without Storing, IEEE 2019.

