ISSN 2395-1621

# Secure Data Access using Steganography and Image based Password

[#1]Shantanu Khade, [#2]Pratiksha chauragade, [#3]Siddhi Chavan

[1]shantanu.khede007@gmail.com
[2]siddhirchavan1234@gmail.com

[#123]Department of Computer Engineering,
Dhole Patil College of Engineering, Pune.

**ABSTRACT**

**In modern day technology, the Information Society is at risk. Passwords are a multi-user computer systems usual first line of defense against intrusion. A password may be textual with any combination of alphanumeric characters. But no authentication protocol is fully secured against todays hackers as all of them are Static in type. Dynamic authentication protocol is still a theoretical concept. In this paper, proposed system doing introduce a secure data scheme with cryptographic primitives for data access from the database server. In a proposed methodology we use the data encryption and steganography technique to secure the image password generation to secure access on the data server's files, for more security splitting technique used to the stegno image for verification server side and client side user data. This system provides strong data security to storage on local cloud server and we also provide the strong network communication security to registered users during data uploads and downloads user data. In this paper covered the idea of generating an efficient algorithm for generates secure image based password Authentication system.**

**Keywords: Images based password, Recognition based technique, data verification, password protection, blowfish algorithm.**

ARTICLE INFO

**Article History**

Received: 10th December 2019

Received in revised form :

10th December 2019

Accepted: 13th December 2019

**Published online :**

**13th December 2019**

## I. INTRODUCTION

Today data security and user data authentication is a basic level for information security. Now day's internet is providing all free accessibility to get the desired information and resources across the world. Every environment, organization, social network, or any other platform all are continuously tries to provide strong security to their users which are accurate and more secure for users. Basic concept of user is authentication, information system because it provides the ability to the user to access the system. Previous old security techniques which are using from a long time provide worst-less security for authentication than the advance security techniques. In the perspective of information security there may be following main objectives of authentication or security.

- How to maintain the track an unauthorized user from gaining access to system?
- How to analysis the user accessed to the required resources of system?
- How to validate user and with other resources communication?

As per analysis and described by the researchers paper and psychological studies we found the problems and advantages of the existing system that it is nature of humans that they remember images better than text, therefore the password which is graphical based, can be used alternatively to text based password. In this system the password verifies of hide data which is used to access to required resources of system. Password image is kept secret from other users so that an unauthorized user can't access the valid data, resources of system. Now day's authentication can be done through several techniques like Textual/ Alphanumeric, Smart Card, Bio-metric, Graphical etc. Each technique provides high cost development; data dependency; network problems so no provide the better accuracy.

**Problem Statement:**

Exploitation of password (user account) is one of largest issues in cyber security as it is an easy way to gain the unauthorized access from the attacker. Today's process is the single widespread form of attack that penetrates a network, system, or resource with or without the use of tools

 

to unlock a resource that has been secured with a password is known as password cracking. There are many reasons that make passwords cracking possible. These reasons include human factors such as short or easily-guessing passwords, usage of weak algorithms. So our proposed system is based on the data protection using the encryption and steganography technique. In this system we generated the secure image based password to access the all files from the server.

The desired paper is organized as follows. Section 2 presents related works about secure data in cloud environment; The proposed System and algorithm in Section 3; System analysis is presented in Section 4; System requirement specification in Section 5; Mathematical model in Section 6; Result discussion in Section 7 and concludes the paper.

## II. REVIEW OF LITERATURE

John K. Alhassan, Idris Ismaila, Victor O. Waziri, and Adamu Abdulkadir, in this paper author explain the XORed encryption technique, steganography and cryptography. They are combined to provide a security system capable of encrypting a secret message using RSA algorithm. To hide the data, they are used advanced LSB method is used. The original message is encrypted at the initial stage and then separated into two portions P1 and P2. An XOR operation is applied to the first portion (P1) using the odd location and to the second portion (P2) using the even position of the LSB+1.The Position of the LSB is then used to hide the XORed encrypted message[1].

R. Nivedhitha, Dr. T.Meyyappan, in this paper, author proposed steganography and encryption technique to hiding the data in the images. Many different file formats can be used for data security, but digital images are the most popular because of their frequency on the internet. This paper introduces two new methods where in cryptography and steganography are combined to encrypt the data as well as to hide the data in another medium through image processing. In this paper using the secure image by encryption is done using DES algorithm with the key image[2].

Ako Muhammad Abdullah, Roza Hikmat Hama Aziz, A Hash Least Significant Bit with Affine cipher algorithm has been proposed in this paper for providing high security to data in a network security. First author encrypt the given data with the new proposed cryptography algorithm and then embed in the image. In this algorithm, Eight bits of the secret message are divided into [3, 3, 2] and embedding into the Red, Green, Blue pixels values of the cover image respectively. Here a hash function is used to select the particular position of insertion in LSB bits. This new introduce system allows a message sender to select keys to encrypt the secret message before embedding into the image and a receiver is used the keys to decrypt the message. Receiver can be decrypted the encrypt message with incorrect the keys but to a different form from the original message. This system has the ability to provide better security while transferring the secret message from one end to the other end in network environment[3].

Dipankar Dasgupta, Rukhsana Azeem, this paper explains most authentication systems based on self-id use as a password data, which is referred to as Positive Identification of a user authentication. These systems use a password profile containing in the list of all the user passwords that are authorized to access the system or the server. The negative password counterpart represents all strings that are not in the password database, which can possibly be explored by hackers using the different tools. The author developed system demonstrated that by examining Anti-Password Clusters, it is possible to deduce what is in the password database it complemented. Here different steps introduces for performing the this system, firstly Data Collection of user password, secondly Data preprocessing using the MD5 algorithm, thirdly Anti-P generation this algorithm uses only one class for generating Anti-Passwords for the complement class (Anti-Ps)[4].

Zubayr Khalid, Pritam Paul, Khabbab Zakaria, Himadri Nath Saha, in this paper, author covered the idea of generating an efficient algorithm that can work as the final in the Dynamic Password Authentication system. Author used the standard deviation for secure data within statistics to generalize the possible password which is further secured by Feistel Block Cipher Algorithm and Advanced Encryption Standard Algorithm, leading and following the said mathematics respectively. In this proposed system order to allow creating variable password in the least time interval possible, author also maintain not more complexity of the given process[5].

## III. PROPOSED METHODOLOGY

### *A. Architecture*

The proposed architectures provide the, authentication in that phase is divided into steps.

1. On the user side, a user provide the his/her username and password to the server. Then, the get method we catch the username and plain password are transmitted to the server through a secure channel;
2. If the received password is provide the steganography process for hiding the data in to the image.
3. Once data hide in the above (2) stage is then we provide the secure encryption process and image splitting technique is applied.
4. Finally every user will get the secure half image and another half image to the data server.

 

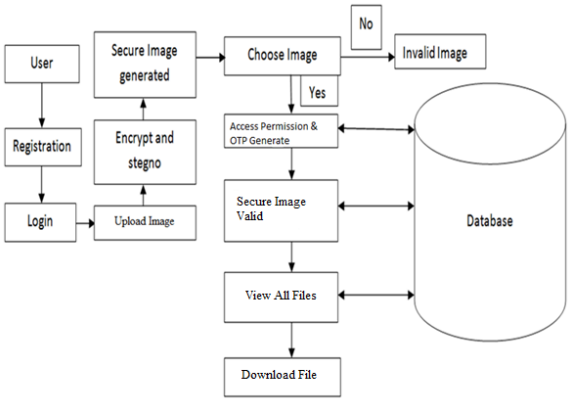


Fig 1. Architecture diagram

## IV. SOFTWARE REQUIREMENT SPECIFICATION

The proposed system created based on the java programing language. Net bean tool used for programing the proposed system. User data is stored in mysql database. This system is used widely accessibly a web technology application using JSP with local server. Web application that facility to access the any data, communicates to each other using the with local server and Trustee Server using REST API. In this system mostly used the image for generate the secure password on local cloud server. We have evaluated time required for steganography and encryption process generation.

## V. CONCLUSION

In We us image based password to secure college data access. It secures the database server from unauthorized user. This method is mainly concerned with preventing identity theft and prevents phishing. It also was providing customer data security.

## REFERENCES

[1] John K. Alhassan, Idris Ismaila, Victor O. Waziri, and Adamu Abdulkadir, "A Secure Method to Hide Confidential Data Using Cryptography and Steganography", Federal University of Technology, Minna, Nigeria November 28 – 30, 2016.

[2] R. Nivedhitha, Dr. T.Meyyappan, "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.

[3] Ako Muhammad Abdullah, Roza Hikmat Hama Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm" International Journal of Computer Applications, Volume 143 – No.4, June 2016.

[4] Dipankar Dasgupta, Rukhsana Azeem," A Negative Authentication System" 2007 (revised on April 15, 2007), The University of Memphis.

[5] Zubayr Khalid, Pritam Paul, Khabbab Zakaria, Himadri Nath Saha, "An Encryption Key for Secure Authentication: The Dynamic Solution", Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 3, 540-544 (2017).

[6] D. Wang, D. He, H. Cheng, and P. Wang, "fuzzyPSM: A new password strength meter using fuzzy probabilistic context-free grammars," in Proceedings of 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Jun. 2016, pp. 595–606.

[7] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.

[8] Y. Li, H. Wang, and K. Sun, "Personal information in passwords and its security implications," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2320–2333, Oct. 2017.

[9] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th International Conference on World Wide Web. ACM, 2007, pp. 657–666.

[10] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Designing password policies for strength and usability," ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 13:1–13:34, May 2016

 