Implementation of Encrypted Image Based Password to Authenticate Company Data from the Cloud

Vidya Kale, Rupali Pawar, Priyanka Pawar, Prajakta Alai, Prof. Amol shenkar
Department of Computer Engineering,
Anantrao Pawar College of Engineering and Research, Parvati, Pune -09.

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 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 system 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, blow-fish algorithm.

I. INTRODUCTION

Now day's internet is providing all free accessibility to get all the desired information and resources across the world. Today data security and user data authentication is a basic level for information security. Basic concept of information security is authentication, because it provides the ability to the user to access the system. Previous old security techniques which are using from a long time provide less security for authentication than the advance security techniques. Every environment, organization, social network, or any other platform, all is continuously trying to provide strong security to their users which are accurate and more secure to users.
As per analysis and described by the research paper and psychological studies, we found 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 and credentials are stored in image file, 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, Biometric, Graphical etc. Each technique provides high cost development; data dependency; network problems so no-one provides the better accuracy, but our system is able to provide better accuracy.

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 the 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 introduced 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 able decrypt 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 authenticated 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 pre-processing 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.

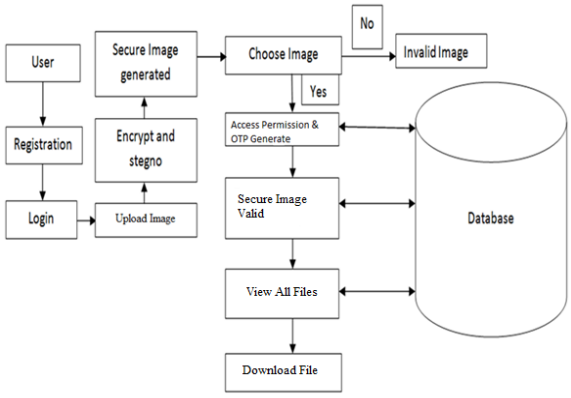

Fig 1. Architecture diagram

User Module:
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.

Steganography Module:
The received credentials is provided with steganography process for hiding the data in to the image.

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

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

B. 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."

IV. RESULT AND DISCUSION

Fig 2. Home page

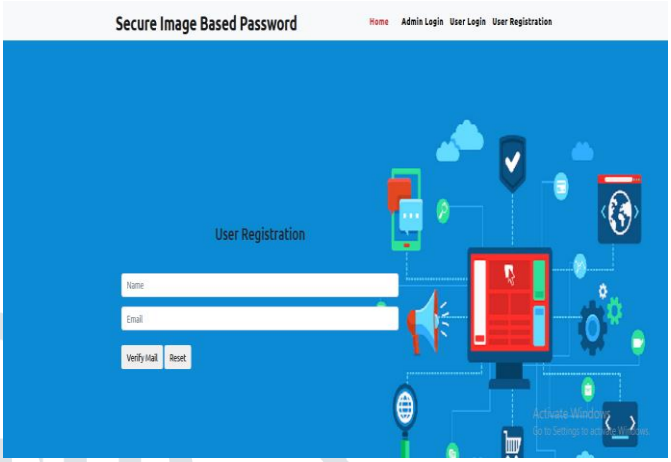

Fig 3. Verification page

Factor / Technique	Security	Installation Cost	Memorable	Data Redundancy	User Acceptance
Proposed System	High	Very High	High	Low	Very High
Textual Password Authentication	Medium	Very Low	Medium	High	High
Smart Card Authentication	High	High	Low	Low	Low
Biometric Authentication	Very High	Very High	Very High	Low	Very Low

Table 1: Comparison result of proposed system with other authentication techniques

V. CONCLUSION

This is image based password system, to implement secure data access. It secures the database server from unauthorized user. This method is mainly concerned with preventing identity theft and prevents phishing, brute force attacks. It also provides customer data security.

VI. 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