Generate Secure Image based Password to Access the Cloud Data

Anuja Patole
Department of Computer Engineering BSIOTR, JSPM's, Wagholi.

A. C. Lomte, PhD
Department of Computer Engineering BSIOTR, JSPM's, Wagholi.

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 using 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 also provide the strong security to registered users during data uploads and downloads user data. In this paper covered the idea of generating an algorithm for generates secure image based password authentication system.

Keywords

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

1. 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 ,finds the problem 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.

1.1 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 proposed system is based on the data protection using the encryption and steganography technique. In this system the secure image based password is generated to access the all files from the server.

The desired paper is organized as follows. The proposed System and algorithm in Section 2; System analysis is presented in Section 3; System requirement specification in Section 4; Mathematical model in Section 5; Result discussion in Section 6 and concludes the paper.

2. 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 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 then 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.

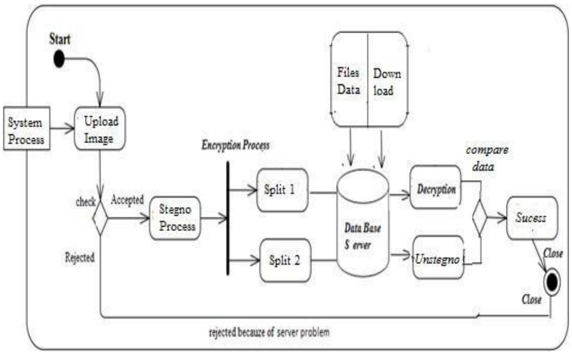


Fig 1. System architecture

B. **Algorithm:**

```
START
Step 1: Enter valid data for stegno
Step 2- U=Upload (image), he input is consider as image Step
3- W= Write (data),
Step 4- K=Key generation (image) e.g=
key=123456;
Step 5- E= Encrypt(image, key, data), encode the upcoming
image
Step 6- C=Convert (image),
If(encrypt), then image convert plain to cipher
Text
Split (image1, image2); Stored (image) Download image
Else, image not encrypted/embedded
Step 7- D=Decrypt (image), decode the image
if (decode), then image convert cipher text to plain
Combine (image1, image2); Else, image not decoded
Step 8- Decrypted image Step 9: Valid User
END
```

3. SYSTEM OVERVIEW

In existing survey there are many authentication techniques like textual, graphical, thumb authentication, smart card etc. The graphical authentication methods based on images selection are not sufficient because in these techniques images are predefined by the system. In existing system, a different problem facing in the information security for user authentication. Today’s password authentication is alphanumeric password but is difficult to set in the mind and usually all user forget as times passes when user remain unattached from the system, but in case of proposed image based password there are less chances to forget password because people remember images more easily than text based password. If you generated the image based password then network also creates the strong

i.e. no one get the password from the unethical activity. There is also no chance for unauthorised user, hackers to steal the graphical based password because hackers will be unable to access the images uploaded by the user as password. This system proposes a new technique based on password of user for Authentication that is image based password Authentication. In this proposed system, a new technique is introduced for data security. In this method, user will upload images from web browser connected to the local server and password will hide using the steganography in the images uploaded by one user will not be visible to other user.

4. 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 widelyaccessibly 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.For system performance calculation, in this paper evaluated time required for steganography and encryption process generation is shown.

5. RESULT AND DISCUSION

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

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 2: The security analysis of Recall based graphical password schemes.

Scheme	Existing System	Proposed System
Password Create Time	64sec	50sec
Login Time	9sec	7sec
File Download Time	10sec	8sec
Success Rate	38-94%	83-96%

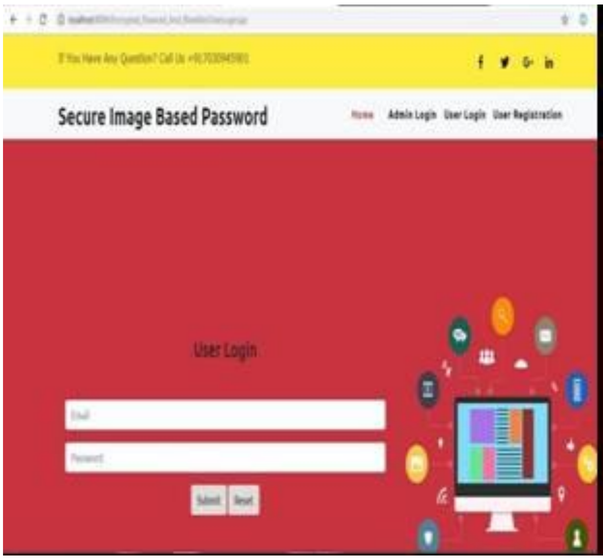


Fig 2. User login

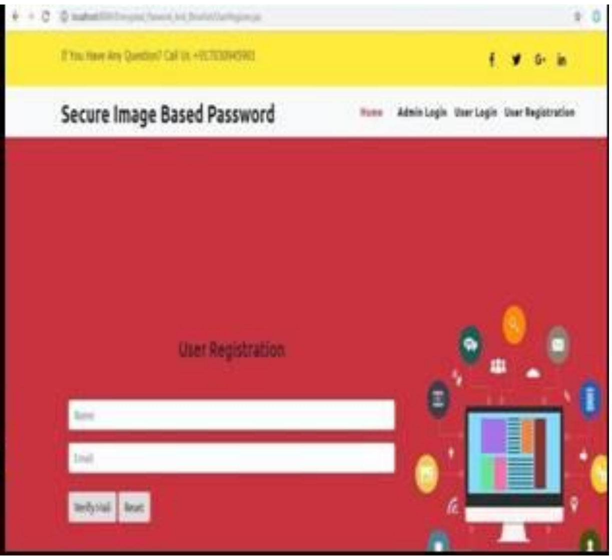


Fig 3. User registration

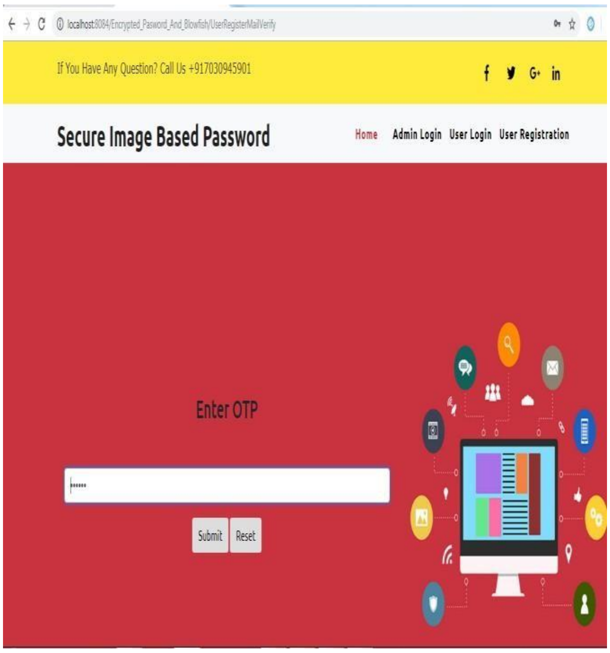
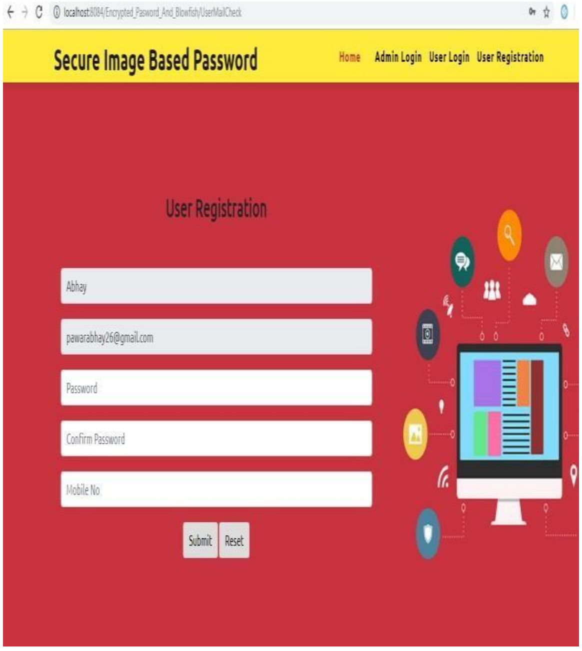
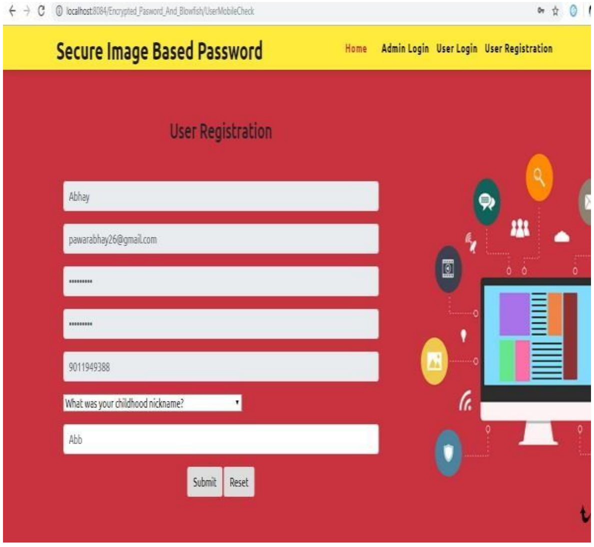

localhost:8084/Encrypted_Pasword_And_Blowfish/UserRegisterMailVerify
If You Have Any Question? Call Us +917030945901
Secure Image Based Password
Home
Admin Login
User Login
User Registration
Enter OTP
Submit
Reset

Fig 4. For Email verification OTP



Abhay
pawarabhay26@gmail.com

Fig 5. For Password and Mobile



localhost:8084/Encrypted_Pasword_And_Blowfish/UserMobileCheck

Abhay

pawarabhay26@gmail.com

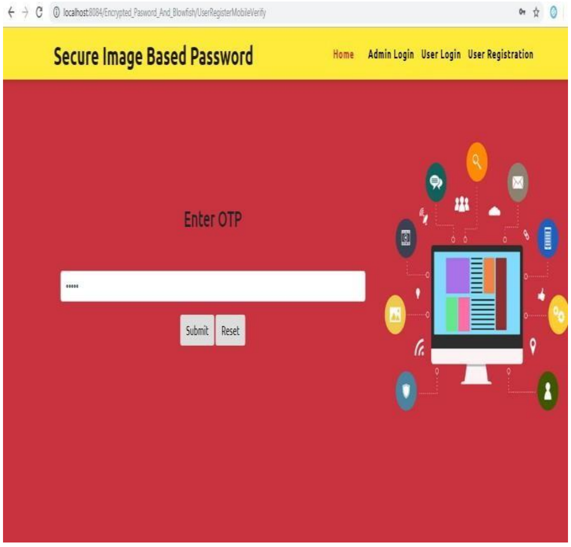
****

****

9011949388

What was your childhood nickname?

Abb

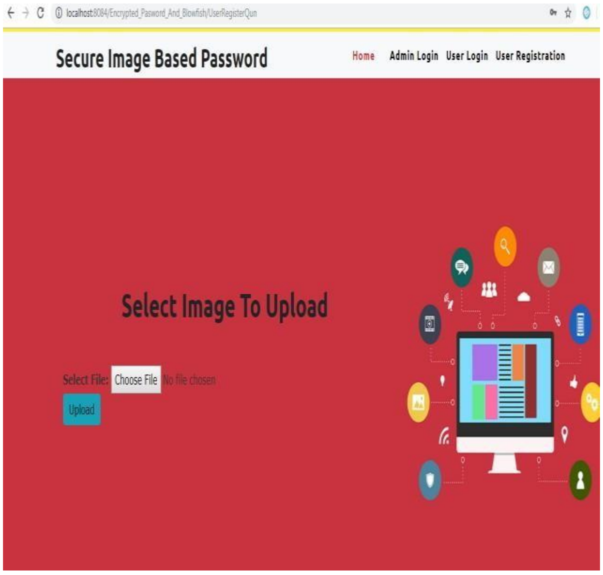


localhost:8084/Encrypted_Pasword_And_Blowfish/UserRegisterMobileVerify

*****

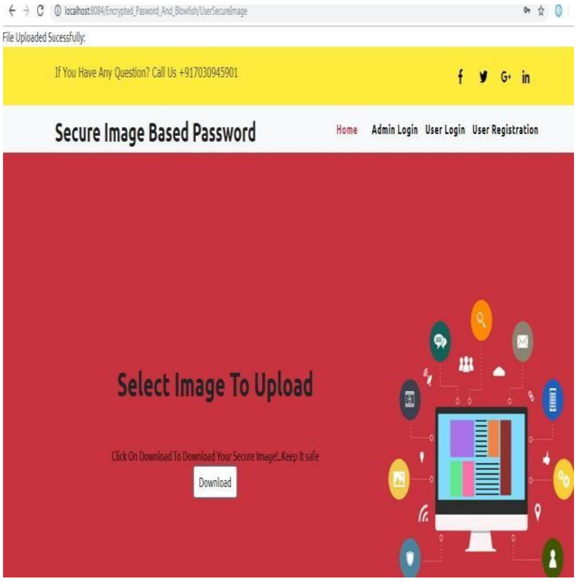
Fig 6. For Mobile verification OTP

Fig 7. Security question generation



localhost:8084/Encrypted_Pasword_And_Blowfish/UserRegisterQun

Select File: No file chosen



localhost:8084/Encrypted_Pasword_And_Blowfish/UserSecureImage

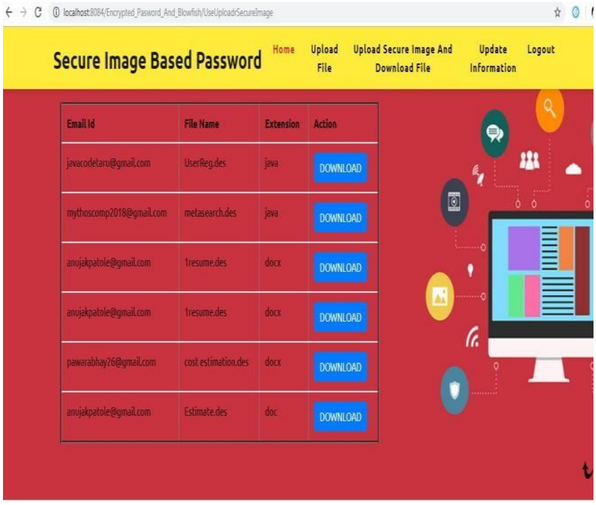
File Uploaded Sucessfully.

If You Have Any Question? Call Us +917030945901

Click On Download To Download Your Secure Image!..Keep It safe

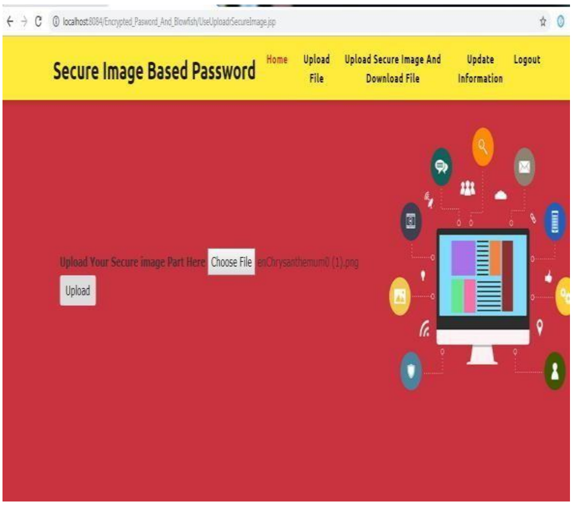
Fig 8. Secure Image upload

Fig 9. Download secure image password


Secure Image Based Password
Home
Upload File
Upload Secure Image And Download File
Update Information
Logout

localhost:8084/Encrypted_Pasword_And_Blowfish/UseUploadrSecureImage

Email Id	File Name	Extension	Action
javacodetaru@gmail.com	UserReg.des	java	DOWNLOAD
mythoscomp2018@gmail.com	metasearch.des	java	DOWNLOAD
anujakpatole@gmail.com	1resume.des	docx	DOWNLOAD
anujakpatole@gmail.com	1resume.des	docx	DOWNLOAD
pawarabhay26@gmail.com	cost estimation.des	docx	DOWNLOAD
anujakpatole@gmail.com	Estimate.des	doc	DOWNLOAD


Secure Image Based Password
Home
Upload File
Upload Secure Image And Download File
Update Information
Logout
Choose File
Upload

localhost:8084/Encrypted_Pasword_And_Blowfish/UseUploadrSecureImage.jsp

Upload Your Secure image Part Here enChrysanthemum0 (1).png

Fig 10. Upload secure image for data access

Fig 11. File download after secure image provided

6. CONCLUSION

In this system designed new technology, combination of encryption and steganography based password. In proposed design framework create the secure password to access the database file server. In the end of the system, avoid the attack from outsider, phishing sites and design the complexity of encrypted password. The results show that the proposed system is better than the other system and stronger than the other password protection system.

7. ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all friends and well- wishers who supported us in completing this paper successfully I am especially grateful to guide Dr. A. C. Lomte for her time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

8. 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 16thInternational 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