IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Triple Level User Authentication With Confidentiality

Mrs.Shaik Rahimunnisa

Assistant professor

Computer Science and Engineering

Vignan's Institute of Engineering for Women, Visakhapatnam

Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India

M.Sai Mounica, N. Sai Sandhya, K.Lavanya, A.HemaLatha

B. Tech Students

Computer Science and Engineering

Vignan's Institute of Engineering for Women, Visakhapatnam

Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh, India

Abstract: In the modern world as there is a drastic hike in the usage of the use internet for our daily work there is a need to keep our information safe and secure that an intruder can't misuse it. Cryptography was established to solve this problem. Cryptography converts this sensitive information to an un-interpretable form such that it cannot be interpreted by anyone except the transmitter and intended recipient. The main aim of cryptography is to protect the data from unauthorized user access or hackers.

Through this project, we develop a three-level authentication for the user to protect his data and additionally transmitting his data with confidentially. Authentication is used by servers when the server needs to know exactly who is accessing their information on site. Authentication is used by a client when the client needs to know that the server is the system it claims to be. Usually, authentication by a server entails the use of a user name and password.

The project contains the triple-level password system which contains login password, color combination, and picture password. Using these levels we provide better security and sees that's the user gets authenticated and confidentiality is met. For confidentiality, we chose to use AES i.e Advanced Encryption Standard used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys for each user. This is also called public-key cryptography. Hence we acquire confidentiality.

Keywords: Authentication, graphical passwords, multi-factor, textual passwords, 3-level passwords, image ordering, AES.

1.INTRODUCTION

Cryptography using three-level password security secure the important folders in the system. The main aim of the project is to provide the users a secure way that helps the users to secure the sensitive and important data folder in their systems. The sensitive data is in the form of text, images, videos, etc. There is an authentication system that validates users for accessing the system only when they have input the correct password. The project involves three levels of user authentication. In this sender will have to first go through all the three stages of authentication. After going through all the stages the sender's text will be encrypted using the cryptography algorithm.

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized user's information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. Three-level password authentication helps for securing the data from any attacker. The sender and receiver have to go to all three stages of authentication for encrypting or decrypting the data. A large number of cryptography algorithms exists in the present scenario. Those algorithms work efficiently but the same type of plain text is converted into ciphertext. The cryptanalysis for this type of ciphertexts is becoming an easy process. But we want to store and send our folders in a secure way. With this project, it will be difficult for the intruders to identify the ciphertext because in this project we use multi-level authentication for the user and receiver for the data transmission, and hence there will be high confidentiality.

2.LITERATURE SURVEY

Most early authentication mechanisms are solely based on passwords. While such protocols are relatively easy to implement, passwords (and human-generated passwords in particular) have many vulnerabilities. As an example, human-generated and memorable passwords are usually short strings of characters and (sometimes) poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time [1]. Due to these concerns, hardware authentication tokens are introduced to strengthen the security in user authentication, and smart-card-based password authentication has become one of the most common authentication mechanisms. Smart-card-based password authentication provides two-factor authentication, namely, a successful login requires the client to have a valid smart card and a correct password.

While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (e.g., an attacker has successfully obtained the password and the data in the smart card). In this case, a third authentication factor can alleviate the problem and further improve the system's assurance. Another authentication mechanism is biometric authentication [2], [3], [4], where users are identified by their measurable human characteristics, such as fingerprint, voiceprint, and iris scan. Biometric characteristics are believed to be a reliable authentication factor since they provide a potential source of high-entropy information and cannot be easily lost or forgotten. Lee et al. [5] designed an authentication system that does not need a password table to authenticate registered users. Instead, a smart card and fingerprint are required in the authentication. However, due to the analysis given in [6], Lee et al.'s scheme are insecure under conspiring attack. Lin and Lai [7] showed that Lee et al.'s scheme is vulnerable to masquerade attack. First, Lin-Lai's scheme only provides client authentication rather than mutual authentication, which makes it susceptible to server spoofing attacks [8]. Second, the password changing phase in in-Lai's scheme is not secure as the smart card cannot check the correctness of old passwords [9]. Third, Lin-Lai's scheme is insecure under impersonation attacks due to the analysis given by Yoon and Yoo [10], who also proposed a new scheme. However, the new scheme is broken and improved by Lee and Kwon [11]. In [12], Kim et al. proposed two ID-based password authentication schemes where users are authenticated by smart cards, passwords, and fingerprints. However, Scott [13] showed that a passive eavesdropper (without access to any smart card, password, or fingerprint) can successfully login to the server on behalf of any claiming identity after passively eavesdropping on only one legitimate login. Bhargav-Spantzel et al. proposed a privacy-preserving multi factor authentication protocol with biometrics [14].

3.EXISTING SYSTEM AND DRAWBACK

The different existing verification to web login is traditional alphanumeric password or graphical password or Biometric Authentication. An alphanumeric password is a mystery word, an expression, or a mix of incidental characters and numbers that validate the personality of the client. Alphanumeric passwords are customary and conventional methods for verification. The human propensity in making secret words makes them helpless and they are liable to different digital attacks. Passwords created with minimum effort and ease of guests are vulnerable to get a cracked password. Biometric verification has its own particular quality and confinements. Significant issues in biometric verification are false dismissing rate, false acknowledgment rate, inability to catch, and select rate. In this digital world, passwords play a crucial role in enhancing data security.

The only disadvantage is if users forget the password, they cannot retrieve it.

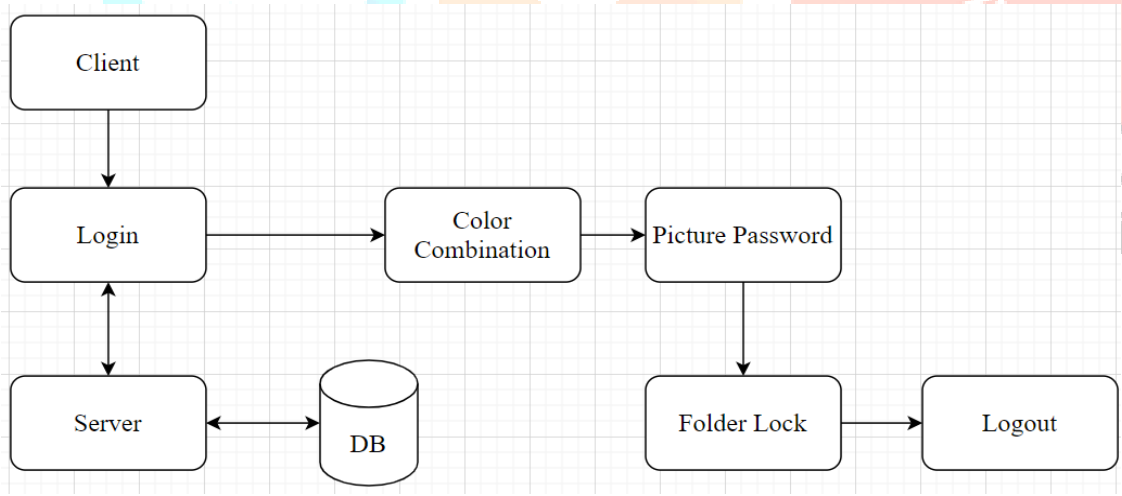
4.PROPOSED SYSTEM

The knowledge factors: Something the user k `````` nows (login, one time password, security question).

The ownership factors: Something the user has(security tokens, hardware token, cell phone holding the software token) .

Most of the organizations use biometrics as a authentication method. Considering alphanumeric password which is static in nature and they are simple but not much secured. Since many of the users choose the easily guessable password such as their favorites, date of birth.

5. CONTENT DIAGRAM



6. FLOWCHART

A flowchart is a diagram that represents a process or algorithm. Flowcharting allows you to breakdown any process into byte sized sections and displays them in shorthand form. That's way, audience can easily see the logical flow and relationships between steps. A flowchart might be helpful when drawing a step by step picture of the process for understanding.

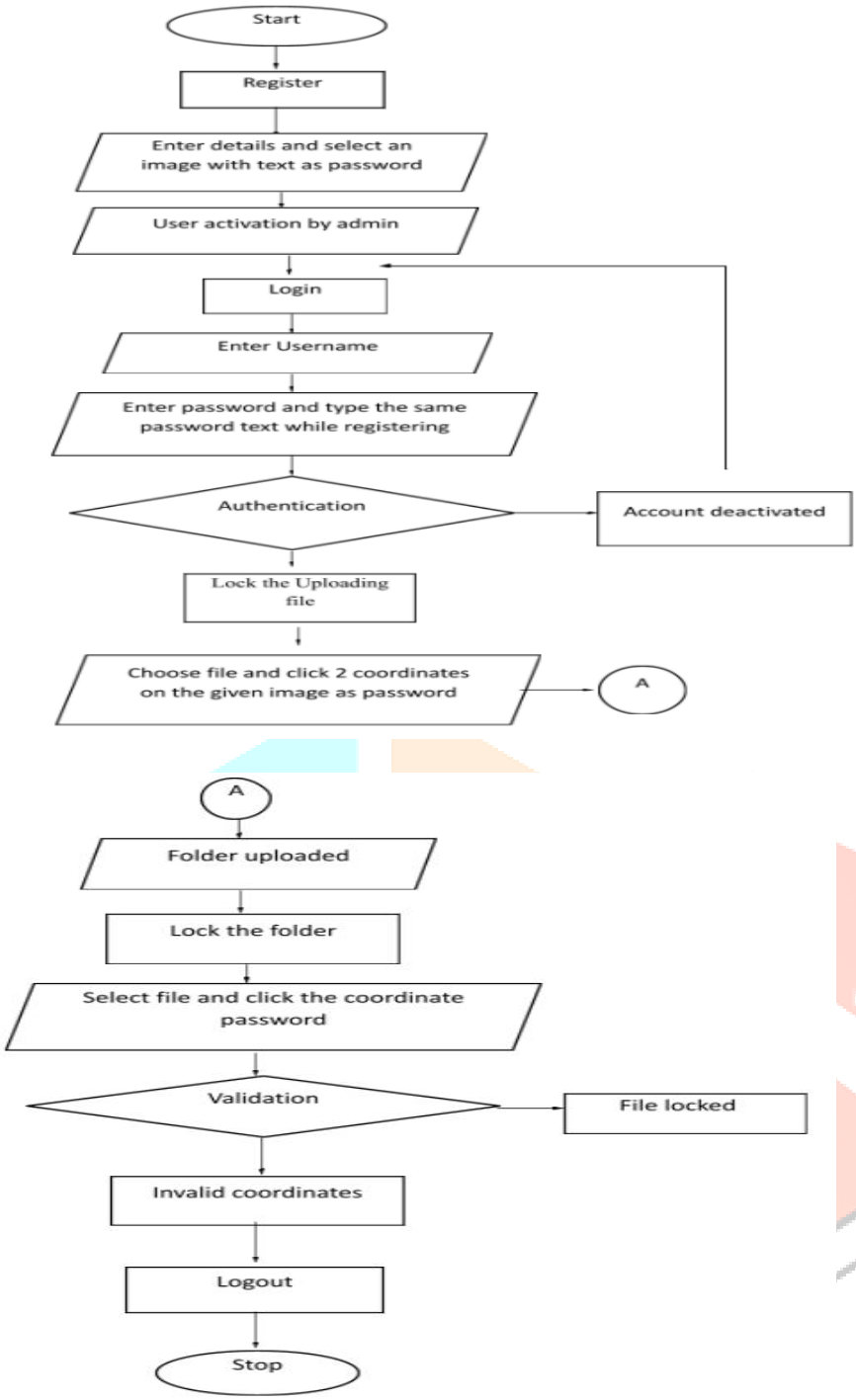
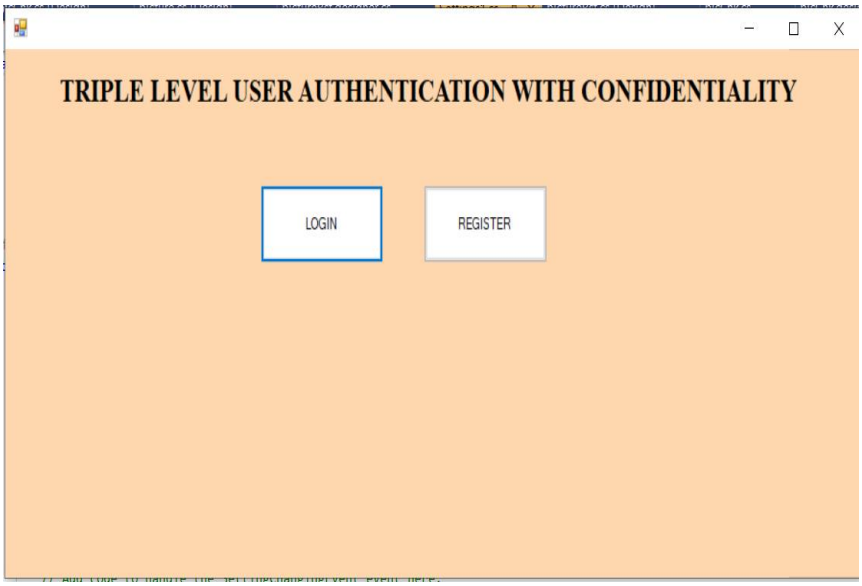
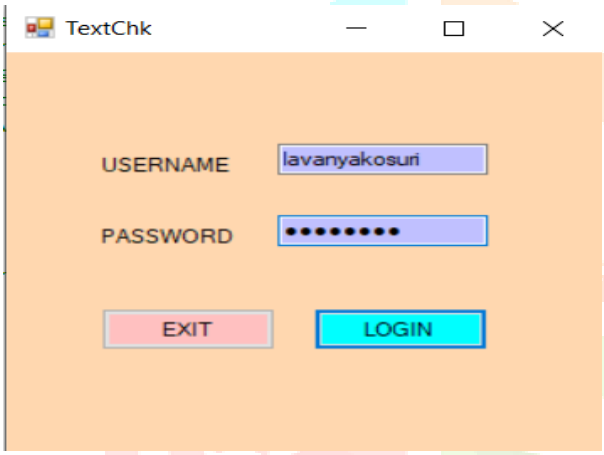


Fig : 3.5 Flow chart for Triple level User authenticaton

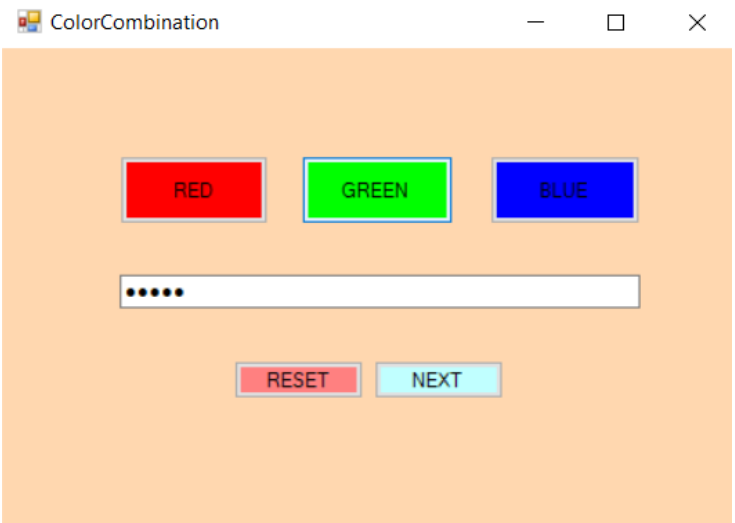
7. RESULTS



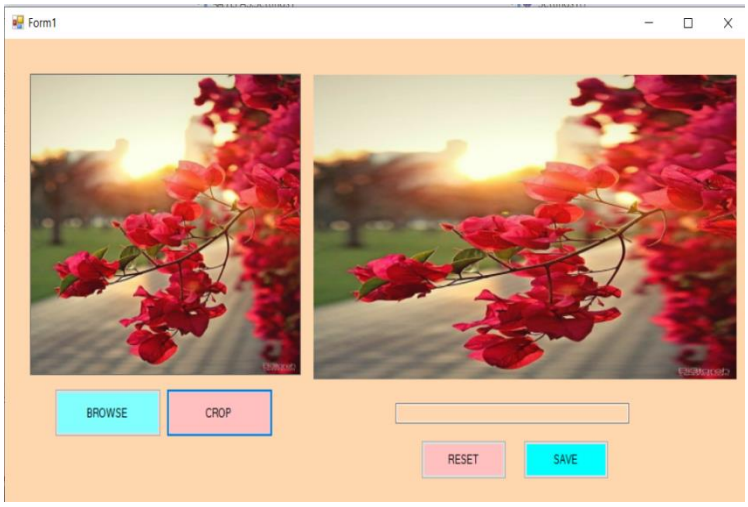
Fig(a):Home page



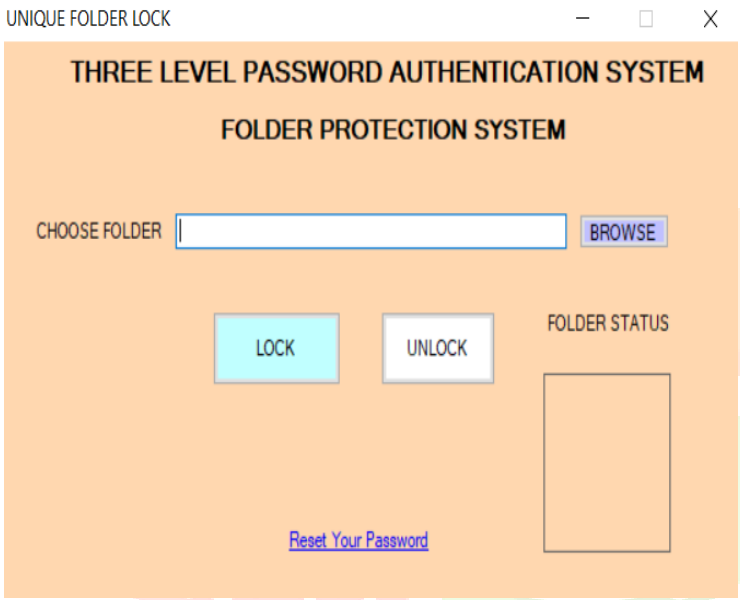
Fig(b):Login Page



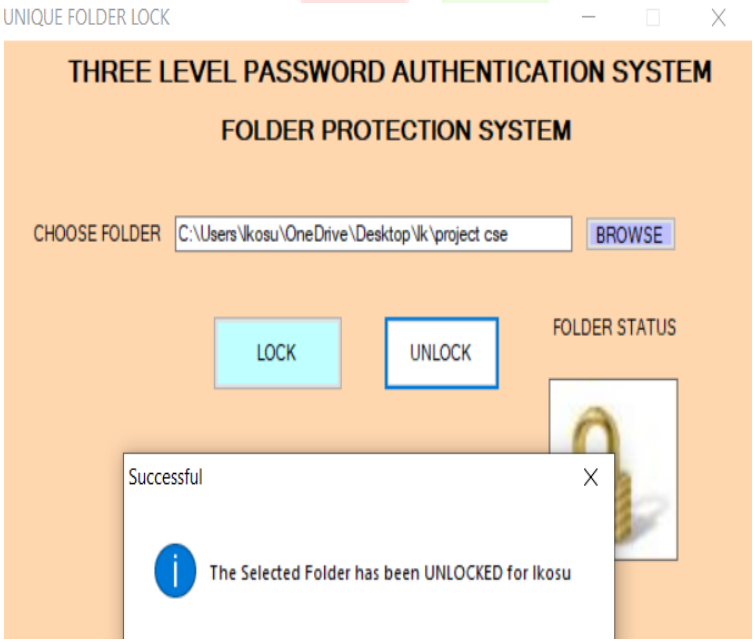
Fig(c):Color Combination



Fig(d):Picture Password



Fig(e):Folder Locking System



Fig(f):Folder Locking System

8. CONCLUSION

The project involves three levels of user authentication. There are varieties of password systems available, many of which have failed due to bot attacks while few have sustained it but to a limit. In short, almost all the passwords available today can be broken to a limit. Hence this project is aimed to achieve the highest security in authenticating users. It contains three logins having three different kinds of password systems. The password difficulty increases with each level. Users have to input the correct password for successful login. Users would be given the privilege to set passwords according to their wishes. The project comprises text passwords i.e. login password, color combination, and picture password for the three levels respectively. This way there would be negligible chances of bot or anyone to crack passwords even if they have cracked the first level or second level, it would be impossible to crack the third one. Hence while creating the technology the emphasis was put on the use of innovative and non traditional methods. Many users find the most widespread text-based password systems unfriendly, so in the case of three-level passwords we tried creating a simple user interface and providing users with the best possible comfort in solving passwords.

9. REFERENCES

[1] Ed. Dawson, J. Lopez, J.A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure," Proc. IEEE Int'l Conf. Information Technology: Research and Education (ITRE '03), pp. 274-278, 2004.

[2] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme

e Using Smart Cards," Electronics Letters, vol. 38, no. 12, pp. 554-555, June 2002.

[3] C.C. Chang and I.C. Lin, "Remarks on Fingerprint-Based Remote User Authentication Scheme Using Smart Cards," ACM SIGOPS Operating Systems Rev., vol. 38, no. 4, pp. 91-96,

[4] C.H. Lin and Y.Y. Lai, "A Flexible Biometrics Remote User Authentication Scheme," Computer Standards Interfaces, vol. 27, no. 1, pp. 19-23, Nov. 2004.

[5] M.K. Khan and J. Zhang, "Improving the Security of 'A Flexible Biometrics Remote User Authentication Scheme'," Computer Standards Interfaces, vol. 29, no. 1, pp. 82-85, Jan. 2007.

[6] C.J. Mitchell and Q. Tang, "Security of the Lin-Lai Smart Card Based User Authentication Scheme," Technical Report RHULMA20051, http://www.ma.rhul.ac.uk/static/techrep/2005/ RHUL-MA-2005-1.pdf, Jan. 2005.