International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Multi-Level Authentication System

Gaurav N. Wadke[1], Nikhil Sable[2], Jisha Samuel[3], Sudesh Kajava[4], Prof. Dhiraj Amin[5]

[1,2,3,4]Student, Computer Engineering, Pillai College of Engineering, Maharashtra, India
[5]Faculty, Computer Engineering, Pillai College of Engineering, Maharashtra, India

---

Abstract - *The System is an authentication application that validates users for accessing the system only when they have input correct passwords. The System involves multiple 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.*

This system is aimed to achieve the highest security in authenticating users. At present authentication is done in several ways: such as, textual, graphical based, Image based and third- party authentication. The project comprises a Login and Registration form with AES Encryption and Decryption where the user id and password will be encrypted. The initial levels include Text password and Graphical password. Both the password type is a Knowledge based authentication technique which is further classified into recall-based technique and recognition-based technique respectively. Different levels can be added further into the application like OTP using hash functions such as SHA-1, MD5 for the generation of OTP or Image based segmentation technique which is a type of graphical based password.

After successful login it will take us to a Bank portal which can include confidential information related to that field. Users would be given privilege to set passwords according to their wish. Many users find the most widespread text-based password systems unfriendly, so in the case of multilevel passwords we tried creating a simple user interface and providing users with the best possible comfort in solving passwords.

***Key Words*: Authentication, Multi-Factor, Image based segmentation, Security, Three-factor authentication.**

1. INTRODUCTION

This system is a modern way through advanced technology due to which the information of each and every account as well as the updated information is available. By this system the information is protected with different levels of authentication. It helps both users and administrators. Bank portal is for the customers who trust the bank with their money. The customer creates their account, deposit their money in the bank. After that they wish to see the details about their account every now and then. So, this portal is for that, so that customers, Bank managers and staff can see and modify the details of the account depending on their authorization to do so.

2. LITERATURE SURVEY

A. Survey

Various techniques are provided by Sanjar Ibrokhimov and a few others for authentication purposes. It presents the state of the Art and discusses the main issues related to the security problem. This paper discusses the evolution from single authentication to Multi-Factor Authentication (MFA) starting from Single Factor Authentication (SFA) and through Two-Factor Authentication (2FA).

B. Image Based Password.

It was developed by Subhradeep Biswas and Sudipa Biswas. It presents the survey and experiments of the two authentication related techniques. It combines different techniques and shows how they are better based on evaluation and performance. This fact has provided incentive for research in security for improved performance. It proposes a hybrid approach that gives better results.

C. Image Pattern lock

Nida Asmat and Hafiz Syed Ahmed Qasim applied a similar technique on different datasets. It introduces the flow of the security system. The proposed technique allows the user to keep the ease-to-use property of the pattern lock while minimizing the risk of shoulder surfing and password guessing. Results show that this technique in this domain has shown great performance.

D. Biometrics

Andrew Bisada and Aspen Olmsted have presented an approach of authentication technique for Security purposes. It explores a different approach for solving the problem of security authentication. This paper shows how authentication can be used on mobile devices using

biometrics as third level authentication next to Username as the first level and text password as the second.

2.1 Summary of Related Work

The summary of methods used in literature is given in Table.

Literature	Advantages and Disadvantages
Sanjar Ibrokhimov, Kueh Lee Hui, Ahmed Al-Absi, Hoon Jae Lee and Mangal Sain. 2019 [1]	Advantage: The paper presents five high-level categories of features of user authentication. High security. Disadvantages: Implementing all the five categories will make the system. More complex for the user and the administrator.
Nida Asmat and Hafiz Qasim 2019[2]	Advantage: Minimizes infiltration attacks like Shoulder surfing, eavesdropping and other similar attacks that could affect the privacy of user.
Subhradeep Biswas and Sudipa Biswas 2017[3]	Advantages: The unauthorized access cannot be prohibited if both the text password and the image are compromised. Disadvantages: If the image is lost by the user password won't work or can't be reset.
Andrew Bisada and Aspen Olmsted 2017[4]	Advantage: Mobile devices are more secure. Disadvantage: Salting is not used.

3. PROPOSED WORK

The system overview is presented in this Section. The classification of various techniques is given in Figure.

3.1 System Architecture

In order to achieve better domain results, researchers combined both techniques to build Multi Level domain systems.

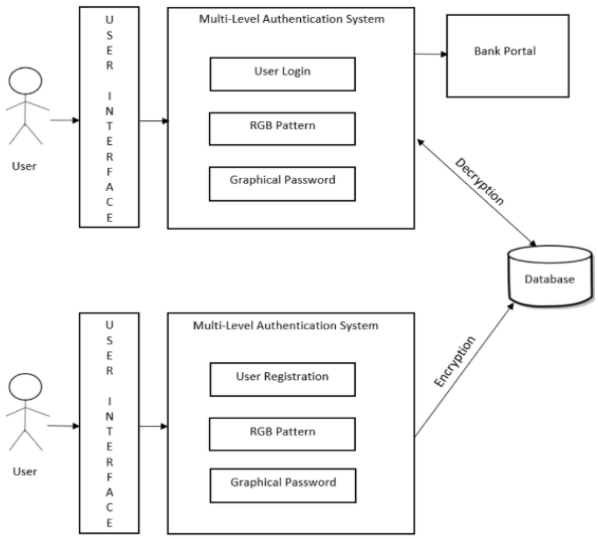


Fig –3.1: Proposed system architecture

The following list describes several techniques used in the System.

It strengthens the master password and encryption key against large-scale, brute-force attacks by slowing down guesses.

● User Interface: The user interface (UI) is the point of human-computer interaction and communication in a device. It is the way through which a user interacts with an application.

● Multi-level Authentication: Multi-level authentication (MLA) is a security mechanism in which users are authenticated through more than one required security and validation procedure. In this we have used three levels for now they are as follows.

● User Login: It is a set of credentials used to authenticate a user. Most often, these consist of a username and password. However, a login may include other information, such as a PIN number, passcode, or passphrase. In this during registration, AES encryption is used on the username and password and stored in the database.

● AES Encryption: The Advanced Encryption Standard, or AES, is a symmetric block cipher used to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks

of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively.

● RGB Pattern: It is used as the second level for authentication. In this user selects a different color pattern as a password. The pattern stores a combination of texts after the pattern is created. Various encryption methods can be used to store this created password.

● Graphical Password: A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI).

For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). The third level uses Image as a way for the user to create more complex passwords compared to the other two levels. Users have to select their own image for this to work. The image is then segmented and the user can then click on different areas on the image which creates a password.

● Image Hashing: Image hashing or perceptual hashing is the process of examining the contents of an image. Constructing a hash value that uniquely identifies an input image based on the contents of an image. In this path of the image file or its name can be hashed to protect its location and identity.

4. REQUIREMENT ANALYSIS

The experiment setup is carried out on a computer system which has different hardware and software specifications as given in Table 4.1 and Table 4.2 respectively.

4.1 Software

Table 4.1 Software details

Operating System	Windows 10
Programming Language	C#
Database	SQL Server Management Studio

4.2 Hardware

Table 4.2 Hardware details

Processor	2.90 GHz Intel
HDD	1 TB
RAM	8 GB

5. IMPLEMENTATION DETAILS

The system overview is presented in this Section. The classification of various techniques is given in Figure 5.1

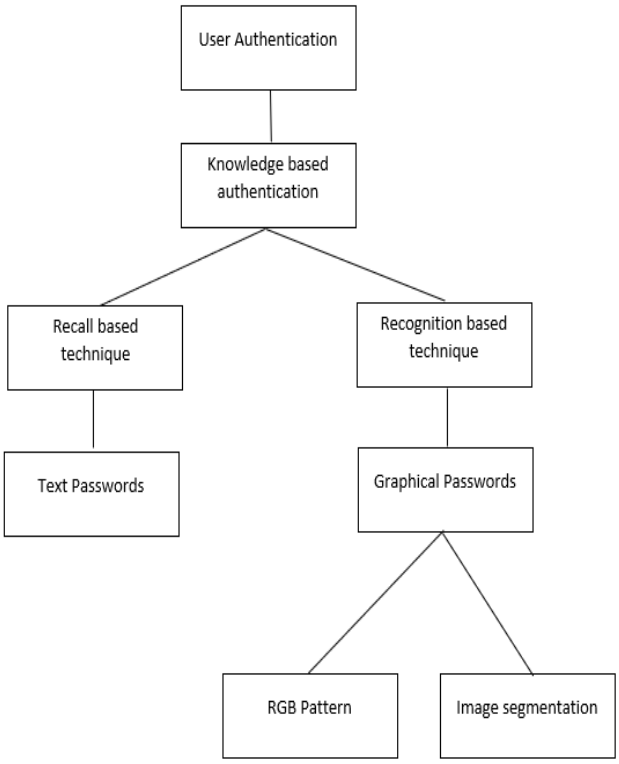


Fig –5: User Registration & Login Window

This system helps users to find information by providing them with personalized suggestions. Based on the above problems of researchers, recommendation techniques will have great influence in all aspects of our life.

- **User Authentication:** User authentication is the verification of an active human-to-machine transfer of credentials required for confirmation of a user's authenticity; the term contrasts with machine authentication, which involves automated processes that do not require user input.
- **Knowledge based authentication:** Knowledge-based authentication, commonly referred to as KBA, is a method of authentication which seeks to prove the identity of someone accessing a service such as a financial institution or website. As the name suggests, KBA requires the knowledge of private information of the individual to prove that

the person providing the identity information is the owner of the identity.

- **Recall based techniques:** Recall based technique, require the user to repeat or reproduce a secret that the user created before. One of the common examples for recall based authentication schemes is textual passwords. One of the major limitations of textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.
- **Recognition based techniques:** Recognition based technique, consists of Graphical passwords. Graphical passwords show how the user can recall and recognize pictures better than words. Some of the graphical password schemes require a long time to be performed.

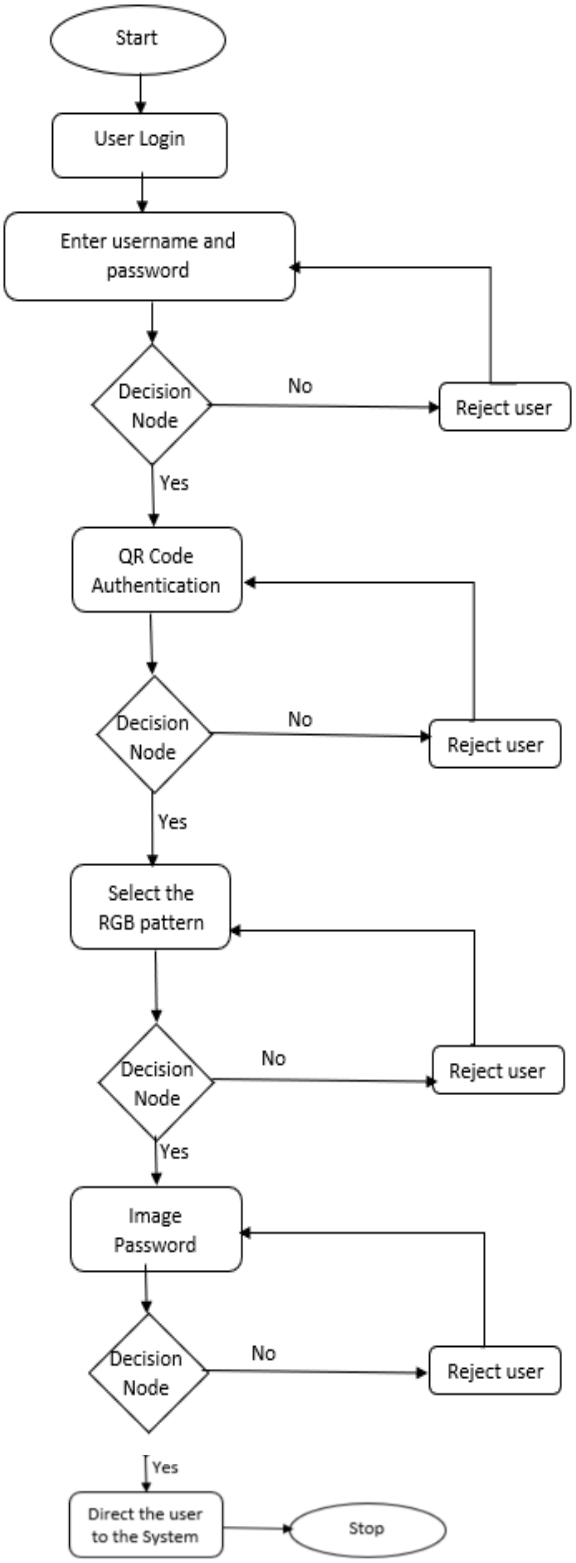
Some examples of these techniques are:

1. RGB Pattern.
2. Image Segmentation.

- **OTP Verification:** A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters. It is used to authenticate and verify users before a transaction or a session in an app/website. Used by businesses to ensure a secure user flow, an OTP SMS service provider ensures timely delivery of these messages.

5.1 Basic Activity Diagram

Basic activity flow of the system is illustrated below.



6. ILLUSTRATIONS (CONCEPTUALISED)

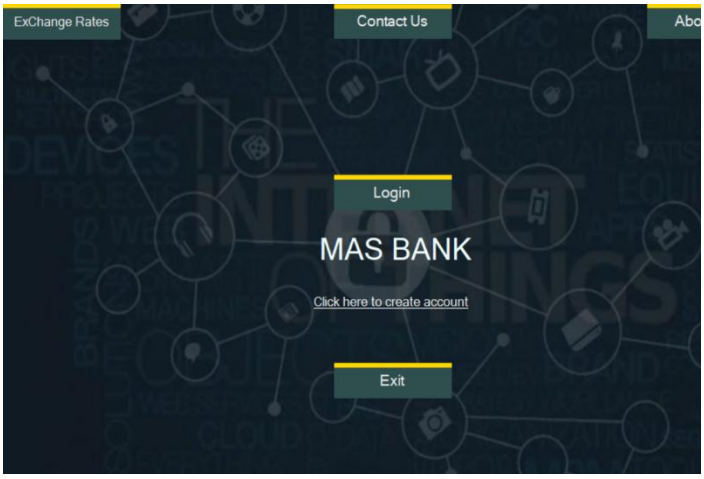


Fig –6.1: User Registration & Login Window

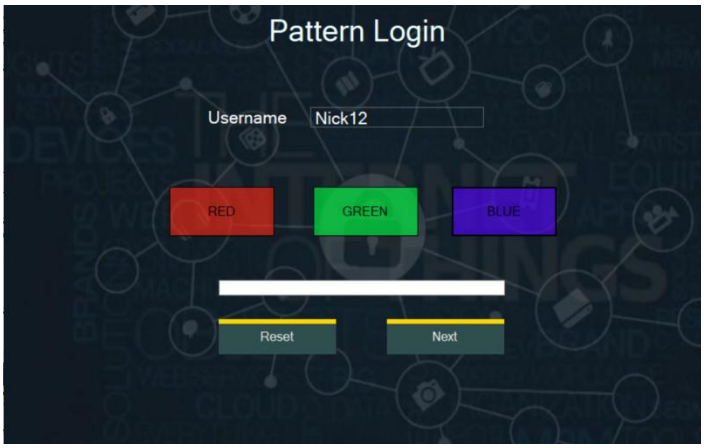


Fig –6.2: Pattern Authentication & Login Window

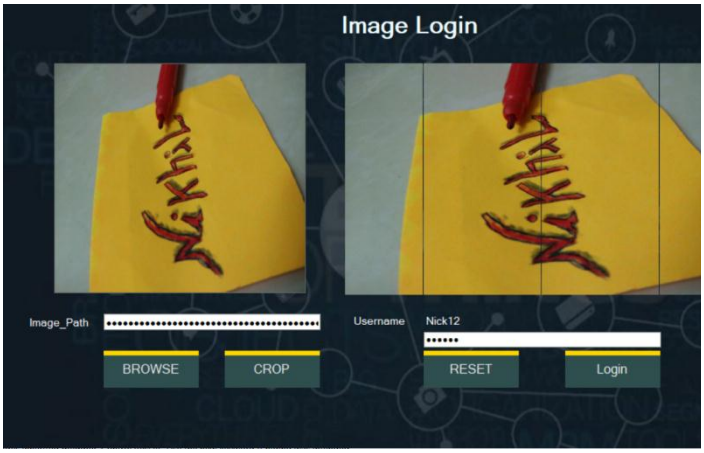


Fig –6.3: Picture Authentication & Login Window

Fig –6.4: QR Code Authentication & Login Window

Fig –6.5: OTP Verification & Login Window

CONCLUSION

In this paper, the study of different domain techniques is presented. The different techniques such as Authentication techniques are explained. Bank Portal is used to protect it using the multiple authentication level. Authentication for any application or website is very important. It has been set up to increase security, prevent password cracking and identity theft and also focuses on better user-friendly interface. The primary goal of this report is to provide the importance of user authentication and how it can be used to protect users during the login process.

ACKNOWLEDGMENT

It is our privilege to express our sincerest regards to our supervisor Prof.Dhiraj Amin for the valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of this work. We deeply express our sincere thanks to our Head

of the Department Dr. Sharvari Govilkar and our Principal Dr. Sandeep M. Joshi for encouraging and allowing us to present this work.

REFERENCES

[1]Multi-Factor Authentication in Cyber Physical System: A State of Art Survey, Dongseo University, Sanjar Ibrokhimov, Kueh Lee Hui, Ahmed Abdulhakim Al-Absi, hoon jae lee and Mangal Sain.

[2]Conundrum-Pass: A new Graphical Password approach, Nida Asmat and Hafiz Syed Ahmed Qasim.

[3]Password Security system with 2-way authentication, Subhradeep Biswas and Sudipa Biswas.

[4]Mobile Multi-Factor Authentication, College of Charleston, Andrew Bissada, Aspen Olmsted

[5]"Image Hashing [online]. Available: https://www.pyimagesearch.com/2017/11/27/image- hashing-opencv-python/

[6]Three Level Password Authentication System: Available: https://nevonprojects.com/three-level-password-authentication-system/

[7]LastPass Architecture. Available: https://www.lastpass.com/enterprise/security

BIOGRAPHIES

Gaurav N. Wadke, Student of Pillai College of Engineering, pursuing bachelor's degree in Computer Engineering from University of Mumbai.

Nikhil Sable, Student of Pillai College of Engineering, pursuing bachelor's degree in Computer Engineering from University of Mumbai.

Jisha Samuel, Student of Pillai College of Engineering, pursuing bachelor's degree in Computer Engineering from University of Mumbai.

Sudesh Kajava, Student of Pillai College of Engineering, pursuing bachelor's degree in Computer Engineering from University of Mumbai.

Asst. Prof. Dhiraj Amin, Assistant Professor (Department of Computer Engineering) at Pillai College of Engineering, Panvel.