Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Puzzle Based Password Authentication by using Grid Selection

1 J. Lin Eby Chandra, 2 M.Kumaran, 3 R. Chandrakala, 4. V.Seedha Devi, 5 S. Rajendran

1, 2, 3. Assistant Professor, Department of Computer Science and Engineering, Jaya Engineering College
Professor, Department of Mechanical Engineering, Jaya Engineering College Chennai 602024,INDIA.
4. Associate Professor Department of Computer Science Engineering, Jaya Engineering College
5. Professor, Department of Mechanical Engineering, Jaya Engineering College Chennai 602024,INDIA.
Email: ebyworld@gmail.com

Article Info
Page Number: 8630-8639
Publication Issue:
Vol. 71 No. 4 (2022)

Abstract
Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login into the system. In this method, the user is required to select some images (let's say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which are in turn followed by KitKat and so on). The next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially. Every time the user will have to use the same sequence while the images are placed in different ways. This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and provide better results to this process.This technique works in two styles, distorting a single image into multiple pieces where the images need to connect like a puzzle, and the other one is using multiple images and forming a pattern to login. In this method, each time while login user needs to place the image in a particular order which is made during registration time. Then the matched image will be converted into a grid of passcode where the rows and columns will be transposed dynamically. So, it will be difficult for the intruder to crack the passcode. Then the passcode will be matched with the passcode already generated and stored in the server. Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login into the system. In this method, the user is required to select some images (let's say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which are in turn followed by KitKat and so on). The next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially. Every time the user will have to use the same sequence while the images are

Article History
Article Received: 15 September 2022
Revised: 25 October 2022
Accepted: 14 November 2022
Publication: 21 December 2022

placed in different ways. This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and provide better results to this process.This technique works in two styles, distorting a single image into multiple pieces where the images need to connect like a puzzle, and the other one is using multiple images and forming a pattern to login. In this method, each time while login user needs to place the image in a particular order which is made during registration time. Then the matched image will be converted into a grid of passcode where the rows and columns will be transposed dynamically. So, it will be difficult for the intruder to crack the passcode. Then the passcode will be matched with the passcode already generated and stored in the server.

Key words: Puzzle, Brute Force, Passcode

1.INTRODUCTION

Authentication is the process by which a person's identity isverified in a large number of applications including websitesand mobile computing environments. It is also a way toestablish the truth of whether the data feature claimed by anentity is valid or not. The authentication system stores the identityprovided in the user information database within thecomputing system user information database. Duringverification, if the credentials entered match theinformation stored in the database, the verification process iscompleted, and the user gets permission to access the system.Throughout this process, hackers have many ways to break theuser password to access private information. Therefore,several challenges may confront the design of authenticationsystems. One of these challenges is how to maintain highsecurity, but also be convenient or simple to use. In theclassical textual passwords, using a string of characters maybe vulnerable to what is so-called the ‘Dictionary Attack’,which relies on frequent passwords that could be used by users.

2. ExistingSystem

The existed Pass numbers are designed to be resistant to shoulder attacks where it is very difficult for the attacker to monitor the method of entry because the password locations on the gird are constantly changed, which results from changing the numbering of rows and columns. In other words, the password does not send directly or encrypted by traditional methods, but it will be encoded using data from the image sent by the server.

3. Literature Survey

The paper **“A Puzzle Based Authentication Scheme for Cloud Computing” [1],** discusses a scheme developed as a graphical-based authentication mechanism by using a puzzle strategy that is attracted by cloud users. In this scheme, puzzles are developed and merged with the authentication of the cloud user.

In the paper **“Pass numbers: An Approach of Graphical Password Authentication Based on Grid Selection” [2],** mainly the proposed Pass numbersare designed to be resistant toshoulder attacks where it is very difficult for the attacker tomonitor the method of entry

because the password locationson the gird are constantly changed, which results fromchanging the numbering of rows and columns.

The paper **"Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password" [3]**, discusses the technique implements two-level graphical password schemes to provide more security to avoid should surfing attacks and key-logging attacks. The first level of authentication is the visual cryptography authentication and the second level of authentication is the cued click point recall-based authentication.

4. Proposed System

The proposed system overcomes some drawbacks of the existingsystem and adds two levels of additional security of authentication. This new proposed system will act as two-step authentication.Initial Authentication using Pattern Matching and Converting the matched pattern image into a grid of passcodes**.**

5. Product Perspective

The most important perspective of this project is to enhance user login security using GRAPHICAL passwords. Enhanced security measures will be taken to improve the security of the applications and data being authenticated using the same technology.To make the passwords user-friendly This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it.

5.1 Product Function

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures betterthan words. Also, they should be more resistant to bruteforce attacks, since the search space is practically infinite.In general, graphical password techniques are classified into two main categories: recognition-based and recall-based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her toidentify one or more images he or she chooses during theregistration stage. In recall-based techniques, a user is askedto reproduce something that he or she created or selectedearlier during the registration stage.

5.2 Operating Environment

Software Requirement

- **Operating system:** Windows 7 and above can be used. The older version of the OS can also be used but impacts the performance.
- **HTML, CSS:** The markup languages used for designing the front end of the application.
- **JavaScript:** The scripting language used for performing some user actions in the front end of the application.
- **Java JDK 1.7.0:** It is the programming language used in this project, to implement the operations performed on the images.

- **Eclipse:** It is an IDE used to implement and build the application. It helps to connect the database part efficiently.
- **Tomcat 5.0/6.X:**It is a server that is used to launch the application and connects with SQL Server.
- **MySQL Server:** It is an open-source database tool used to store the image-related information and supports the query to fetch the data later.
- **Python:** It is a programming language used to communicate efficiently between the application and database and also perform some algorithmic executions.
- **Flask:** It is a python package used to bind the python operations with the front end and with the database.

5.3 EXTERNAL INTERFACE REQUIREMENT

User Interface

This section mainly describes how the interface interacts with the user for input and output, the user interface of the product is kept simple and clear in order to a user-friendly product. The interface between users and the system includes many provisions from which they can access the whole system. It contains the options list to move one form to another as well as searches form that is asLogin/Sign up page, Generates graphical password page.

Hardware Interface

The software needs an operating system (i.e.) Windows 7 and above, core processor i3 and above, and RAM 4GB and above.

6. SYSTEM FEATURES

This provides the various features of the project and their functionalities, and the major services provided by the product. These are the most important aspects of this system and are what define the product.

6.1 Description and Priority

The authorized users are able to access the system. To ensure the security of the user the administrator should monitor the activities of the User for every login. Users should take some self-care about their accounts by not sharingcredentials about their accounts. The user should be authorized by the administrator only.

6.2 Stimulus/Response Sequences

The User login can be processed so that the administrator accessed to enter the user into their account in a safe manner.

6.3 Graphical Password Generation

Graphical password generation is the process that will randomly generate a new key by the system in order to remove collisions. The GPG is a puzzle in which the user wants to select an image or upload an image to make it into a password-like puzzle. In the sign-up

process,the User needs to choose a Frame in the puzzle that would be his password for all files.

6.4 Stimulus/Response Sequences

The Graphical Password Generation (GPG) is used to generate a puzzle that would have been used to act as Gateway for users' documents or others. Thus, the puzzle is the key that is used to authenticate the users.

6.5 Grid-Based Authentication

Thedesigned grid size is displayed in grid cells to enable the user for choosing the cells corresponding to the password. Theselection is made by clicking on the required cellindependently. In other words, each button will be representedby a pair of coordinates resulting from the intersection of therow and the column. Thecell in the grid is represented by two indexes which are the rowindex (R) and the column index (C). Columns and rows of thegrid are numbered from (0 to 99), and the arrangement ofnumbers is varying dynamically at each login process tostrengthen the resistance to shoulder surfing attacks. Theapplied grid size is relatively large, so it is very difficult toguess the password of the attackers and this makes it resistant toguess attacks also.

6.6 Access server application with integrated security

The process of accessing server applications with integrated security means that user should upload their files with integrated security to prevent some unauthorized entries.

6.7 Stimulus/Response Sequences

To stimulate the process of accessing server applications integrated security is provided using graphical password technology.

7. SOFTWARE DESIGN

System Design is the process by which the software requirements are translated into a representation of software components, interfaces, and data necessary for the implementation phase.

7.1 SYSTEM ARCHITECTURE

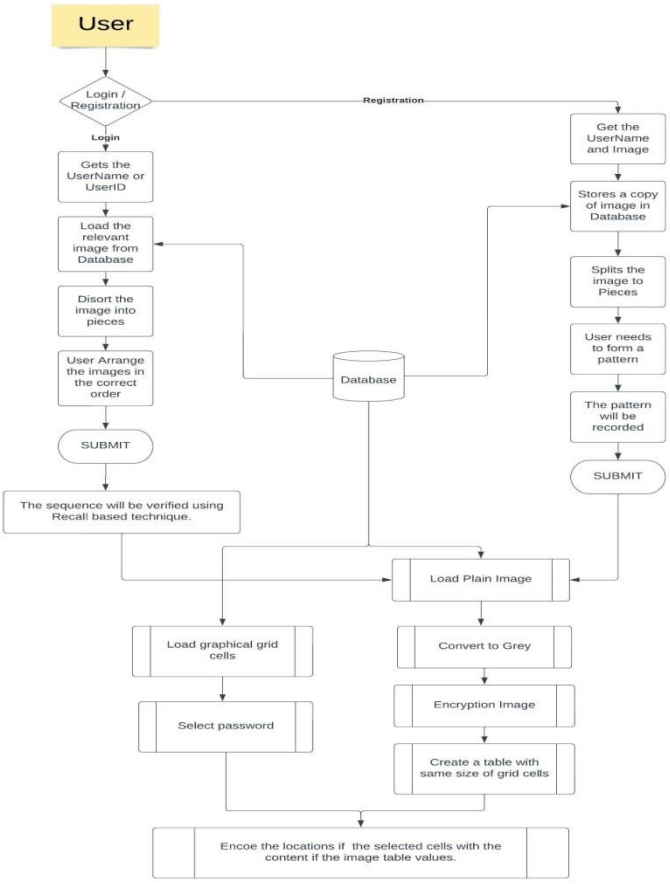


Fig 1.1 : Architecture Diagram

The fig1.1 is used to show the architecture view of the project, where the user interface and processing are shown. From the architecture diagram, it can be clearly said that the system is comprised of several modules, the major module is thePuzzle Solving implementation module and the Grid Selection model.

The user will do Registration with their details (i.e.) their names and with their email id. The process will be followed with a graphical password. The user will log in to the page once they complete the sign-up. On the login page the user login by giving the registered email id with the appropriate password. The password can be position-based or image-based. The image-based can be split into several pixels to make a puzzle that should be solved by the user onthe login page. The access will be gained from the server(i.e.) from the administrator. The administrator will have a check with the database whether both were the same. If both are the same, they will get access from the administrator.

8. DECOMPOSITION DESCRIPTION

8.1 Image Processing

In this module, the image will be uploaded by the user. The uploaded image will be split into multiple pieces to make the image in the form of a grid. Then the uploaded image will be converted to greyscale images. The grey images are encrypted to Hash Code using the RSA

Algorithm.

8.2 Puzzle Solving

The unsolved Puzzle will be given as a jumbled one the user will sign up by solving or either by changing any number of boxes with appropriate or inappropriate (i.e., incorrect way so that the hacker/visitor won't get accessed by others) way. The User should login with the same format that they used or solved as their input. If both the puzzles solved were correct it will move to the next step.

8.3 Grid selection based on image

When the user signs up for the web application the image will be loaded to the user and that image will divideinto many pieces. Those pieces will become a puzzle that has to be solved. The sequence of image selection will be recorded and stored in the database. While logging in to the web application the same sequence needs to be implemented to verify the user.

8.4 Grid selection based on position

When the user signs up for the web application the position will be chosen by the user. Those positions will be changed from the list of given positions. The sequence of image selection will be recorded and stored in the database. While logging in to the web application the intersection point of those images needs to be selected for the authentication.

9. COMPONENT DESIGN

9.1 User Component

The user will do Registration with their details (i.e.) their names and with their email id. The process will be followed with a graphical password. The user will log in to the page once they complete the sign-up. On the login page the user login by giving the registered email id with the appropriate password. The password can be position-based or image-based. The image-based can be split into several pixels to make a puzzle that should be solved by the user onthe login page. The access will be gained from the server(i.e.) from the administrator. The administrator will have a check with the database whether both were the same. If both are the same, they will get access from the administrator.

9.2 Human Interface Design

The graphical user interface of the Pass numbers system involves important features which are the random changing of the image and grid indexing numbering at each log-in session to enable the authentication system to be more secure. The user interface of the Passnumbers approach has a grid of cells on-screen that most users are familiar with. However, the difference is in the number selection process, which is resulted from the intersection of the row and the column. Hence, the user can easily complete the login process. The time factor and cost of implementing the authentication system is one of the most important success points in adopting an authentication system. Hence, it can summarize the advantages of

implementation and improvement in the procedures of the work when using the proposed authentication technique.

10. RESULTS

The output of the project is to provide high-level security to the user, by uploading the image it will split as a puzzle which can be solved in anyway in a user-friendly manner. The administrator will give access to the user once they login into the webpage without the access of the administrator the user cannot be login into the webpage. The user can upload the files either with or without Integrated security thus the expected result has come as an outcome. The objectives of the project are successfully accomplished and implemented.

Sign Up: Image-Based Graphical Password

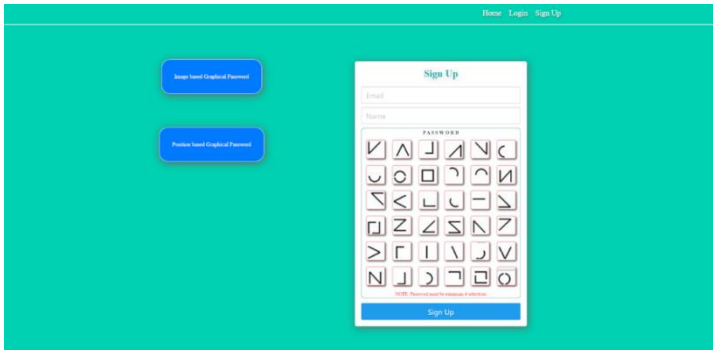
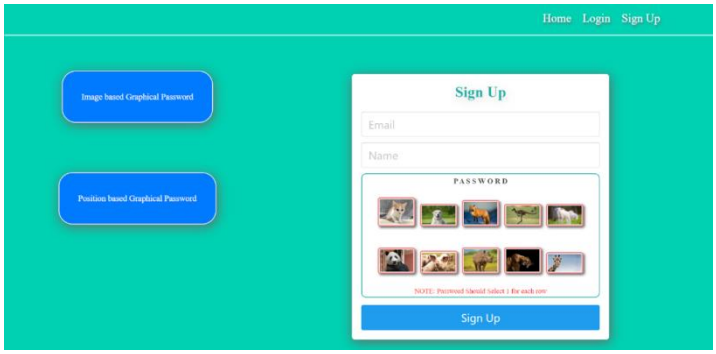
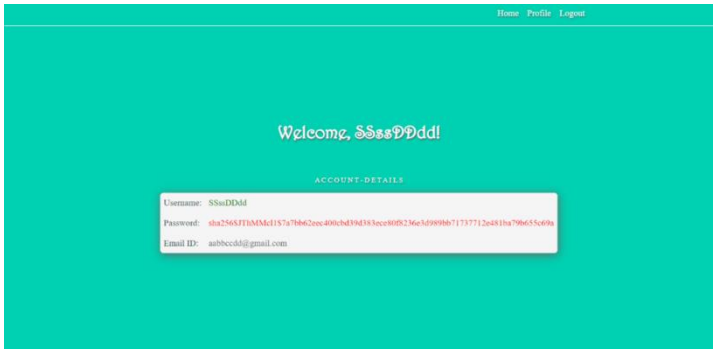


Fig1.2 : **Sign Up: Image-Based Graphical Password**

Signup –Position-Based Graphical Password



Application Launch



11. Observation

The puzzle authentication scheme is reliable, more secure and robust and there is always drastic improvement in future. The analysis of the scheme shows that there is great opportunity to develop new ways to protect the confidentiality of cloud user data and information. The security levels of cloud environment can be further improved by using puzzle-based scheme which overcome the loopholes present in the traditional authentication methods.

CONCLUSION

This project helps to solve conflicts of hard to remember password and creating easily attack password. By using GBA as an approach, most of attackers' problem such as brute-force attack, dictionary and shoulder surfing attack can be solved. In this paper, we develop an implementation of pattern-based password authentication scheme for minimizing shoulder surfing attack. With the combination of two techniques, we can prove that this method is secure. The grid selection technique during the user registration process requires users to select the grids as their chosen password. Users can choose any patterns or styles as there is no limit for the user to select how many grids they like for their password. Lastly, recall based technique during the user login process significantly increase the grid password space.

FUTURE WORK

In the future, this web application can be integrated with several applications to provide high level security to hide the personal data's from the hacker's.

REFERENCES

1. A systematic review of PIN-entry methods resistant to shoulder-surfing attacks, Binbeshr F., Kiah, Zaidan, A.A.2021.
2. Cybersecurity threats based on machine learning-based offensive technique for password authentication, Lee, K., Yim, K., 2020.
3. An efficient security model for password generation and time complexity analysis for cracking the password,Kumar, B.P., Reddy, E.S. 2020.
4. Improvements in a Puzzle Authentication Method, Yutaka Hirakawa, Ayaka Shimoda, Isao Sasano, Kazuo Ohzeki,2018,
5. A Puzzle Based Authentication Scheme for Cloud Computing, Sulochana.V , Parimelazhagan.R. 2013.
6. A Study on Graphical Password Authentication in Cloud Computing. S. Kaushal1, Dr. B. Buksh. 2018
7. Graphical Authentication Based Techniques.
8. V. Bhusari. 2013 4-stage graphical password authentication scheme for cloud. k. Gangadhara Rao, R.Vijayakumari, B.Basaveswara rao. 2017
9. Authorization using captcha as graphical password. S.A. Gulave, S.G. Mungal, N.B. Dhawale, S.S. Chavan .2015.

10. Visual Cryptography and Secure Graphical Password Transaction in Online Banking System. J V N Raghava Deepthi , Unnam Ramya , Gurram Srivalli , Raya Divyasree, Pothineni Haritha.2020.