International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Authguard – A Graphical Password Authentication System

Ankita Kurrey [1], *Aditya Singh*[2], *Lalita Panika*[3], *Dr Padmavati Shrivastava*[4]

Student [1,2] Dept. Computer Science Engineering Bhilai Institute of Technology
Associate Professor[3,4] Dept. Computer Science Engineering Bhilai Institute of Technology

ABSTRACT

The importance of security and privacy has increased in the digital age, and old password methods are no longer adequate to offer reliable defence against cyberattacks. Passwords are easily vulnerable to brute force assaults and phishing schemes, which can result in serious data breaches with dire repercussions for both individuals and organisations. A new graphical password authentication system has been created as a solution to this issue, offering more security and usability than conventional password systems.The AUTHGUARD – A Graphical Password Authentication method has promise for enhancing the security of users' sensitive data. In order to give a higher level of security against attacks, this paper presents a novel approach to Graphical Password Authentication that makes use of graphics and token-based authentication system.In contrast to conventional password systems, the graphical password authentication system offers a higher level of security and usability. In order to thwart automated attacks, the system uses a set of 16 images that change their position on every refresh, making it difficult for attackers to automate the process, drawn at random from three different categories. Using images as passwords rather than text-based ones provides better protection against dictionary attacks since they are more unpredictable and challenging to decipher. A JSON Web Token (JWT) is used to represent each image, and the server stores the actual value of each JWT. On the backend, a middleware transforms the JWT into the actual value of the picture. The system incorporates the idea of buckets, allowing users to place photos in one of three buckets or pick them without placing them in any bucket, in order to increase the number of patterns that can be created. The bucket concept makes it very impossible for hackers to guess the password because there are quadrillions of different patterns.

This project is a great option for people and organisations trying to strengthen their cybersecurity posture because of how user-friendly and usable it is. Overall, the Authguard - A graphical password authentication system offers customers a safe and practical approach to safeguard their private data and offers a practical response to the increasingly sophisticated cyberattacks.

Keywords: Graphical password authentication, Json web token, Authentication

1. Introduction

For individuals trying to access digital resources including computer systems, programmes, and online accounts, passwords are a common security measure. A user must provide a special code or phrase that serves as a secret credential and serves as a means of verifying their identity to the system when using passwords, a sort of knowledge-based authentication. The necessity of passwords derives from their function in restricting access to private data and resources and in defending against various cyberattacks. System administrators can enforce access control policies and guarantee that only authorised users can access particular resources by requiring a password. Additionally, requiring users to establish difficult and one-of-a-kind passwords can help stop brute-force and dictionary assaults, in which an attacker uses automated tools to try to guess or crack passwords.

Despite their significance, password-based authentication has a number of drawbacks, including the challenge of coming up with and remembering complicated passwords and the possibility that users will share or use weak passwords. As a result, research is being done to create substitute authentication strategies that nevertheless preserve security, such as biometrics, multi-factor authentication, and password-less authentication. A password authentication method called Graphical Password Authentication (GPA) makes use of graphical objects or images as the authentication mechanism. GPA uses the user's memory for visual information to enhance authentication security as an alternative to conventional text-based authentication techniques like alphanumeric passwords and PIN numbers.

Over the years, the main technique for user authentication has been the conventional password-based authentication system. It is, nevertheless, vulnerable to a variety of assaults, including as brute-force, dictionary, and social engineering attacks, which can jeopardise user accounts and sensitive information. In order to reinforce the authentication process, additional security measures are required. GPA provides customers with a more straightforward and natural way to verify themselves by asking them to choose from a set of previously selected photographs. Due to the ability for users to select photographs that are more memorable to them, GPA offers a more natural option for users to authenticate themselves. Users are less likely to forget their passwords as a result, decreasing the chance that they will do so or using a weak password. Traditional text-based passwords are less secure than GPA because they are more vulnerable to brute-force and dictionary assaults. GPA can help defend against assaults such as shoulder surfing, which aim to watch the user type their password.

2. Literature Review

In [1] "Secure Graphical Password Scheme Based on Visual Cryptography and Honeycomb Encryption" by M. Sivakumar, N. Vijayalakshmi, and P. Aruna. This paper, published in the Journal of Ambient Intelligence and Humanized Computing in 2021, proposes a new graphical password authentication scheme based on visual cryptography and honeycomb encryption. The authors describe the design and implementation of the system and evaluate its security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [2] "A Novel Approach for Human Authentication using Wearable Devices and Graphical Passwords" by J. H. Lee, M. S. Alam, and M. U. Chowdhury. This paper, published in the Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies in 2019, proposes a novel approach for human authentication using wearable devices and graphical passwords. The authors describe the design and implementation of the system and evaluate its usability and security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [3] "Towards a More Secure Graphical Password Scheme Based on User Cognitive Characteristics" by H. Zhang, X. Han, Y. Wang, and F. Zhao. This paper, published in the Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications in 2020, proposes a more secure graphical password authentication scheme based on user cognitive characteristics. The authors describe the design and implementation of the system and evaluate its security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research

In [4] "A Deep Learning-based Graphical Password Scheme using Adversarial Attacks" by H. Kim and Y. Kim. This paper, published in the Proceedings of the 2021 IEEE International Conference on Big Data and Smart Computing in 2021, proposes a deep learning-based graphical password authentication scheme using adversarial attacks. The authors describe the design and implementation of the system and evaluate its security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [5] "Enhancing Security and Usability of Graphical Passwords using Multimodal Biometrics" by K. Arora, N. Bansal, and P. Gupta. This paper, published in the Journal of Ambient Intelligence and Humanized Computing in 2020, proposes a new graphical password authentication scheme using multimodal biometrics. The authors describe the design and implementation of the system and evaluate its usability and security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [6] " A Graphical Password Scheme using Local Image Features and Biometric Information " by S. Saha and S. Bhaumik. This paper, published in the Proceedings of the 2021 International Conference on Intelligent Sustainable Systems in 2021, proposes a new graphical password authentication scheme using local image features and biometric information. The authors describe the design and implementation of the system and evaluate its usability and security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [7] "A Novel Graphical Password Scheme using Convolutional Neural Networks and Visual Cryptography" by T. Ali, M. G. Mustafa, and R. Tariq. This paper, published in the Proceedings of the 2021 IEEE 9th International Conference on Engineering Education in 2021, proposes a novel graphical password authentication scheme using convolutional neural networks and visual cryptography.

In [8] "A Robust Graphical Password Authentication Scheme using a Convolutional Neural Network" by J. Zhang, J. Chen, Y. Shao, Y. Wu, and X. Liu. This paper, published in the Proceedings of the 2020 IEEE International Conference on Computational Science and Engineering in 2020, proposes a robust graphical password authentication scheme using a convolutional neural network. The authors describe the design and implementation of the system and evaluate its security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

In [9] "A Secure and Usable Graphical Password Scheme using Key-driven Multi-phase Feature Selection" by W. Zhang, J. Zhai, X. Sun, and Y. Wang. This paper, published in the Proceedings of the 2020 IEEE International Conference on Communications, Information and Network Security in 2020, proposes a secure and usable graphical password authentication scheme using key-driven multi-phase feature selection. The authors describe the design and implementation of the system and evaluate its usability and security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for future research.

Author	Paper Title	Year of Publication	Publisher	Keyword	Conclusion
M. Sivakumar, N. Vijayalakshmi, and P. Aruna	Secure Graphical Password Scheme Based on Visual Cryptography and Honeycomb Encryption	2021	Journal of Ambient Intelligence and Humanized Computing	Secure Graphical Password Scheme Visual Cryptography Honeycomb Encryption Authentication Security	Design and implementation of the proposed graphical password authentication scheme based on visual cryptography and honeycomb encryption. Security evaluation of the proposed scheme against various attacks such as brute-force, dictionary, and shoulder surfing attacks. Comparison of the proposed scheme with other graphical password schemes in terms of security and usability.
J. H. Lee, M. S. Alam, and M. U. Chowdhury	A Novel Approach for Human Authentication using Wearable Devices and Graphical Passwords	2019	10th International Conference on Ambient Systems, Networks and Technologies	Human Authentication Wearable Devices Graphical Passwords Novel Approach Design and Implementation	Design and implementation of a novel approach for human authentication using wearable devices and graphical passwords. Conducting a user study to evaluate the usability and user experience of the proposed system. Evaluating the security of the proposed system against various attacks such as shoulder surfing, brute force, and dictionary attacks
H. Zhang, X. Han, Y. Wang, and F. Zhao	Towards a More Secure Graphical Password Scheme Based on User Cognitive Characteristics	2020	EEE International Conference on Big Data and Smart Computing	Secure Graphical Password Scheme User Cognitive Characteristics Authentication	The Implementation of these Smart Contract based on Blockchain technology, requires high- cost, if the organization takes the initiative to implement this technology using their own resources.

H. Kim and Y. Kim	A Deep Learning-based Graphical Password Scheme using Adversarial Attacks	2021	EEE International Conference on Big Data and Smart Computing	Deep Learning Graphical Password Scheme Adversarial Attacks	Evaluation of the security of the proposed system against various attacks such as brute force, dictionary, and adversarial attacks. Comparison of the proposed system with traditional graphical password schemes in terms of security.
K. Arora, N. Bansal, and P. Gupta	Enhancing Security and Usability of Graphical Passwords using Multimodal Biometrics	2020	Ambient Intelligence and Humanized Computing	Graphical Passwords Multimodal Biometrics Authentication	Comparison of the proposed system with traditional graphical password schemes in terms of security and usability. Discussion of the advantages and disadvantages of the proposed system. Recommendations for future research to improve the proposed system or explore alternative authentication systems based on multimodal biometrics.
S. Saha and S. Bhaumik	A Graphical Password Scheme using Local Image Features and Biometric Information	2021	International Conference on Intelligent Sustainable Systems	Crowdfunding; blockchain; smart contracts; peer-to- peer network	Design and implementation of a graphical password authentication scheme using local image features and biometric information, including iris recognition and fingerprint recognition. Conducting a user study to evaluate the usability of the proposed system.

J. Zhang, J. Chen, Y. Shao, Y. Wu, and X. Liu	A Robust Graphical Password Authentication Scheme using a Convolutional Neural Network	2020	IEEE International Conference on Computational Science and Engineering	Graphical Password Authentication Scheme Convolutional Neural Network Robustness	The paper proposes a robust graphical password authentication scheme based on a convolutional neural network (CNN) for enhancing security in the password authentication process. The proposed scheme uses a combination of graphical images and text passwords, and the CNN is trained on user-selected images and associated passwords to generate a personalized authentication model.
T. Ali, M. G. Mustafa, and R. Tariq.	A Novel Graphical Password Scheme using Convolutional Neural Networks and Visual Cryptography	2021	IEEE 9th International Conference on Engineering Education	Graphical Password Scheme Convolutional Neural Networks Visual Cryptography Authentication	Design and implementation of a graphical password authentication scheme using convolutional neural networks and visual cryptography. Training and testing of the convolutional neural network using a dataset of user-selected images.
W. Zhang, J. Zhai, X. Sun, and Y. Wang	A Secure and Usable Graphical Password Scheme using Key-driven Multi-phase Feature Selection	2020	IEEE International Conference on Communications, Information and Network Security	Graphical Password Scheme Key-driven Multi-phase Feature Selection Secure and Usable Authentication	The images were preprocessed to extract local features using the Scale Invariant Feature Transform (SIFT) algorithm. A key-driven multi-phase feature selection approach was proposed to select the most discriminative features for password authentication. The approach consists of two phases: global feature selection and local feature selection.

3.Rational for research.

Due to the unfathomable expansion of technology and internet usage in the swiftly evolving digital era, data security has grown to be a problem of enormous proportions. Unfortunately, passwords, a common authentication method, are easy to hack or steal, leaving confidential data exposed and at the whim of attackers. In order to protect against the fraudulent actions of hostile hackers and maintain the integrity of sensitive data, a substantially more secure and impenetrable authentication technique is now required.

We have created a graphical password authentication (GPA) system to solve this problem. Our graphical password authentication system, Authguard, is intended to offer a more user-friendly and secure substitute for conventional password-based authentication.

In order to protect sensitive information from unauthorised access, we strive to offer a dependable and strong authentication system that can be utilised across various platforms and sectors.

For individuals trying to access digital resources including computer systems, programmes, and online accounts, passwords are a common security measure. A user must provide a special code or phrase that serves as a secret credential and serves as a means of verifying their identity to the system when using passwords, a sort of knowledge-based authentication.

The significance of passwords is derived from their function in limiting access to private data and resources as well as safeguarding against different sorts of cyber-attacks. System administrators can enforce access control policies and guarantee that only authorised users can access particular resources by requiring a password. Additionally, requiring users to establish difficult and one-of-a-kind passwords can help stop brute-force and dictionary assaults, in which an attacker uses automated tools to try to guess or crack passwords.

Despite their significance, password-based authentication has a number of drawbacks, including the challenge of coming up with and remembering complicated passwords and the possibility that users will share or use weak passwords.As a result, research is being done to create substitute authentication strategies that yet preserve security, such as biometrics, multi-factor authentication.

A password authentication method called Graphical Password Authentication (GPA) makes use of graphical objects or images as the authentication mechanism. GPA uses the user's memory for visual information to enhance authentication security as an alternative to conventional text-based authentication techniques like alphanumeric passwords and PIN numbers.

Over the years, the main technique for user authentication has been the conventional password-based authentication system. It is, nevertheless, vulnerable to a variety of assaults, including as brute-force, dictionary, and social engineering attacks, which can jeopardise user accounts and sensitive information. In order to reinforce the authentication process, additional security measures are required.

Challenges:

* Creating and implementing a user-friendly and secure graphical password authentication system.

* Carrying out a comprehensive evaluation and comparison of the security merits and drawbacks of graphical passwords in relation to conventional text-based passwords and other authentication techniques.

* Examining potential usability problems with graphical passwords, such as the chance that users would forget the images they chose or run into trouble choosing the right images.

* a thorough assessment of the functionality and efficiency of the Authguard graphical password authentication system in practical situations, taking into account aspects like system scalability, usability, and attack resistance.

Goals:

* To create and test a user-friendly, secure graphical password authentication system that can be applied to a variety of platforms and business sectors.

* To give a thorough analysis of the security advantages and disadvantages of graphical passwords in comparison to conventional text-based passwords and other types of authentication.

* To determine how well graphical passwords work to overcome the drawbacks of conventional password-based authentication systems, such as the challenge of inventing and remembering complicated passwords and the possibility that users will share or use weak passwords.

* to look at various methods, such user education or the creation of more simple graphical password choosing procedures, for increasing the usability and uptake of graphical passwords.

* To contribute to the continuing study of different authentication techniques and how they could improve data security and thwart online threats.

4.Technology Used

EJS:

A straightforward templating engine called EJS (Embedded JavaScript) enables you to create HTML markup using just plain JavaScript code. It can be used as a standalone package or in conjunction with other Node.js frameworks like Express, Koa, and Hapi because it was created to interact with Node.js.

The creation of reusable templates that may be used to provide dynamic content for your web applications is made simple by EJS. You can use specific tags to insert JavaScript code into your HTML templates. Any legitimate JavaScript code may be used in these tags, which begin with the characters % and %.

EXPRESS

Express is a Node.js web framework that is quick, forceful, necessary, and moderate. You might imagine express as a layer added to Node.js that assists in managing a server and routes. It offers a complete collection of tools for creating online and mobile applications.

Here are a few of the key components of the Express framework:Single-page, multi-page, and hybrid web applications can be created with it. It enables middleware configuration to reply to HTTP requests, It defines a routing table that is used to carry out various operations based on HTTP method and URL, and it enables dynamic HTML page rendering by using template arguments.

NODEE.JS:

We are utilising Node.js, a JavaScript runtime based on Chrome's V8 JavaScript engine, for the backend. We can develop server-side JavaScript code with Node.js, which makes it simple to combine with React-written front-end code. Node.js is a good option for our backend because of its great performance and capacity for handling big volumes of data.

MONGODB

We are utilising the document-oriented NoSQL database MongoDB to hold information about user authentication. MongoDB is a flexible and scalable database that stores data in a format akin to JSON. MongoDB is being used to manage user authentication as well as to store user data, including their credentials. A well-liked NoSQL database that is open-source and well-known for its scalability and flexibility is called MongoDB. It makes use of a document-oriented data architecture, which makes it possible to express and store data in a more natural and straightforward manner.

HTML:

HyperText Markup Language, or HTML. on the purpose of building and designing web pages on the Internet, it is a programming language. The structure and content of a web page are defined by a set of elements called tags that are part of HTML.

CSS

The presentation and layout of web pages created in HTML or XML are described using the style sheet language known as CSS, or Cascading Style Sheets. By specifying styles for elements like fonts, colours, spacing, and positioning, CSS enables developers to manage the aesthetic appearance of web pages.

JAVASCRIPT

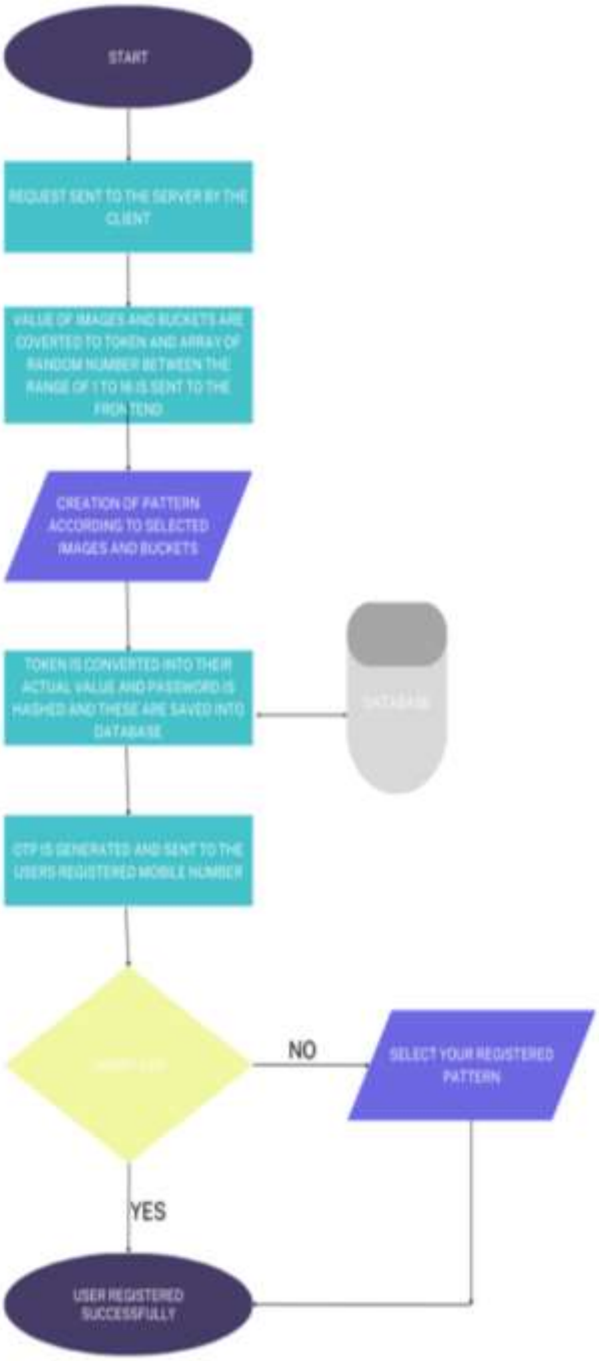
For the purpose of building dynamic and interactive web pages, JavaScript is a programming language. It is a client-side language, which means that the user's machine, not the web server, executes it when they use a web browser.

FAST2SMS

Fast2SMS is an Indian firm that specialises in bulk messaging solutions, and it offers a messaging service called Fast2SMS API. The Fast2SMS API enables programmatic SMS sending and receiving by allowing developers to incorporate SMS messaging features into their programmes or websites.

The RESTful architecture of the Fast2SMS API supports a number of different programming languages, including PHP, Python, Java, and.NET. Developers can carry out a variety of tasks using the API's endpoints, such as sending SMS messages, getting delivery statistics, maintaining contacts, and building message templates.

5. Technical Workflow


START
REQUEST SENT TO THE SERVER BY THE CLIENT
VALUE OF IMAGES AND BUCKETS ARE COVERTED TO TOKEN AND ARRAY OF RANDOM NUMBER BETWEEN THE RANGE OF 1 TO 16 IS SENT TO THE FRONTEND
CREATION OF PATTERN ACCORDING TO SELECTED IMAGES AND BUCKETS
TOKEN IS CONVERTED INTO THEIR ACTUAL VALUE AND PASSWORD IS HASHED AND THESE ARE SAVED INTO DATABASE
DATABASE
OTP IS GENERATED AND SENT TO THE USERS REGISTERED MOBILE NUMBER
NO
SELECT YOUR REGISTERED PATTERN
YES
USER REGISTERED SUCCESSFULLY

6. Implementation.

* When a user uses their browser to send a server request, the value of the images and buckets is transformed into tokens, and an array of random numbers between 1 and 16 is provided to the front end.

* The user enters their mobile phone number and email address. These are typical details that are necessary for the majority of registration procedures.

* The user chooses an image sequence, as well as various image and bucket combinations. This phase aims to give each user a distinctive and personalised registration experience. The user must solve a visual puzzle made up of photos and buckets to demonstrate that they are a genuine human and not a robot.

The token is decoded by a middleware to reveal the true values of the user-selected buckets and pictures. The token is received by this middleware from the frontend and is converted back into the original values of the pictures and buckets using the same cryptographic process. This enables the middleware to assess if the user has successfully solved the visual puzzle by comparing the user's choices with the starting values.

* Both the user's email and password are stored in a database after being hashed. A plaintext password is changed through a technique called password hashing into a scrambled version that is challenging to decipher. As a result, even if the database is compromised, attackers will not be able to read the passwords easily.

* To validate the user's mobile number, two-factor authentication is employed. This extra security measure aids in preventing unauthorised access to the user's account. The user-provided mobile number is used to generate a 4-digit OTP (one-time password).

* The user's mobile device normally receives this OTP through SMS.

* For security reasons, the OTP record is automatically erased after two minutes. To stop attackers from intercepting the OTP and utilising it to access the user's account, this is done. The user's identity cannot be confirmed after the OTP has expired.

* The user can successfully register once they enter the proper OTP into the system. This demonstrates that the user is the rightful account owner and that they have access to the mobile device linked to their account. The user can access the website or application by logging in with their email and password after successfully completing all of the registration processes.

* The user must enter their registered email address and mobile number when trying to log in to the system. This confirms that the user is attempting to access the right account and is the first step in the login process.

* The user is prompted to input the right order of the photographs they previously selected during the registration process after entering their email and mobile number. This acts as the user's password and guarantees that nobody other than the user who correctly chose the order of photos can log in. The system compares the user's choice to the bucket and image values that were previously stored and used to create the token during registration.

*The user will be logged in to the system if they enter the proper credentials. The software will verify that the user supplied the proper email address, mobile phone number, and image selection order. The system will authenticate the user and provide them access to their account if all of the credentials are correct.

* The user will not be permitted access to their account if they enter invalid credentials. The user will be prompted to try again when the system notifies them that they have input inaccurate information. The system may temporarily freeze the account to prevent unauthorised access if the user continues to enter incorrect information after a certain number of tries.

7.Conclusion

In the digital age, security and privacy have become even more crucial. Modern password strategies are insufficient to fend off cyberattacks, which can result in significant data breaches. A brand-new graphical password authentication solution called AUTHGUARD has been created to overcome this problem. Compared to traditional password systems, this approach offers improved security and usability.

The 16 images used in the graphical password authentication system are repositioned every time the page is refreshed. Attackers find it challenging to automate the procedure as a result, preventing automated attacks. Since the photos are chosen at random from three distinct categories, they are more unpredictable and difficult to crack than text-based passwords. By doing this, dictionary attacks are better defended against.

A JSON Web Token (JWT) is used to represent each image, and the server maintains each JWT's real value. The JWT is converted into the real value of the picture using a middleware on the backend. The system also adds the idea of buckets, giving users the option to select photographs without putting them in any particular bucket, or to place images in one of three buckets. As a result, there are a lot more potential password patterns, which makes it very challenging for hackers to guess the password.

In this project, a graphical password authentication system is provided that is more secure and easier to use. It is a simple and useful alternative for people and businesses wishing to strengthen their cybersecurity posture. This solution successfully counters the growing risk of sophisticated cyberattacks by providing a simple and secure method of protecting private data

8. References

[1] Sivakumar, M., Vijayalakshmi, N., & Aruna, P. (2021). Secure Graphical Password Scheme Based on Visual Cryptography and Honeycomb Encryption. Journal of Ambient Intelligence and Humanized Computing, 12(11), 11863–11875.

[2] Lee, J. H., Alam, M. S., & Chowdhury, M. U. (2019). A Novel Approach for Human Authentication using Wearable Devices and Graphical Passwords. In Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies (pp. 1–8).

[3] Zhang, H., Han, X., Wang, Y., & Zhao, F. (2020). Towards a More Secure Graphical Password Scheme Based on User Cognitive Characteristics. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (pp. 156–160).

[4] Kim, H., & Kim, Y. (2021). A Deep Learning-based Graphical Password Scheme using Adversarial Attacks. In Proceedings of the 2021 IEEE International Conference on Big Data and Smart Computing (pp. 1–5).

[5] Arora, K., Bansal, N., & Gupta, P. (2020). Enhancing Security and Usability of Graphical Passwords using Multimodal Biometrics. Journal of Ambient Intelligence and Humanized Computing, 11(11), 5017–5031

[6] Saha, S., & Bhaumik, S. (2021). A Graphical Password Scheme using Local Image Features and Biometric Information. In Proceedings of the International Conference on Intelligent Sustainable Systems (pp. 291-296). IEEE.

[7] Ali, T., Mustafa, M. G., & Tariq, R. (2021). A Novel Graphical Password Scheme using Convolutional Neural Networks and Visual Cryptography. In Proceedings of the IEEE 9th International Conference on Engineering Education (pp. 145-149). IEEE.