Educational Administration: Theory and Practice
2024, 30(5), 11002-11011
ISSN:2148-2403
https://kuey.net/

Research Article

Enhancing User Privacy And Security Through Image Based Authentication Technique

Saumya kapoor[1], Akansha Tomar[2], Sarang Gupta[3], Rohit Kumar Singh[4]*

[1,2,3,4*]Department of Computer Science & Engineering, Meerut Institute of Engineering & Technology, Meerut,UP, 250005, India.
saumya.kapoor.cse.2020@miet.ac.in, akansha.tomar.cse.2020@miet.ac.in
sarang.gupta.cse.2020@miet.ac.in, rohit.singh@miet.ac.in

*Corresponding Author: Rohit Kumar Singh
*Rohit.Singh@Miet.Ac.in

Citation: Saumya kapoor et al (2024), Enhancing User Privacy And Security Through Image Based Authentication Technique, *Educational Administration: Theory and Practice*, *30*(5), 11002-11011
Doi: 10.53555/kuey.v30i5.4877

ARTICLE INFO

ABSTRACT

In this research article, we have proposed a Graphical Password Authentication system that revolutionizes online security by employing image-based passwords alongside traditional alphanumeric ones, enhancing both usability and robustness. Resilient against common attack methods like brute force and spyware, it utilizes a MongoDB database and advanced encryption for data security. Our work is inspired by existing research, which highlighted the challenges of text passwords and the benefits of graphical authentication. Through a dual-layered authentication approach, combining image-based and alphanumeric passwords, security is significantly strengthened, particularly in sensitive applications like online banking and e-commerce. Leveraging the MERN stack ensures a robust infrastructure with secure data storage and dynamic user interfaces. Our proposed algorithm introduces a novel mechanism for securing user details through image verification, utilizing Unsplash API, JWTs, and Nodemailer for email notifications. This system not only mitigates the limitations of text-based passwords but also meets contemporary cybersecurity requirements, setting a new standard for user-friendly yet robust online authentication systems.

Keywords: Graphical Password Authentication, Image-based Passwords, Online Security, User-friendly Authentication, Multi-factor Authentication

1. Introduction

In the contemporary information-driven society, safeguarding personal information is paramount, necessitating robust measures for securing information devices. Among the prevalent methods, password-based authentication stands out as a widely employed security scheme. Traditionally, passwords consist of numerical digits or combinations of numbers and letters, collectively termed as text-based authentication.
However, text-based authentication poses inherent challenges. The ideal password should strike a balance between being memorable for the user and resistant to prediction by potential attackers. Striking this balance becomes particularly challenging when users prefer shorter, more meaningful passwords for ease of recall. Unfortunately, shorter and meaningful passwords are susceptible to theft, especially when users resort to using the same password across multiple accounts. This practice significantly compromises security, as a breach in one account jeopardizes the integrity of others.
Moreover, the increasing sophistication of cyber threats, [1] such as phishing attacks and malware infiltration, underscores the need for a more robust authentication mechanism that goes beyond the limitations of traditional passwords. These threats often exploit human vulnerabilities, such as the tendency to reuse passwords across multiple platforms or the inadvertent disclosure of sensitive information through social engineering tactics.
Furthermore, the complexity of managing multiple passwords for different accounts can lead to user frustration and security lapses. Users may resort to insecure practices, such as [2-4]writing down passwords

or storing them in easily accessible digital formats, inadvertently exposing their credentials to potential attackers.

To address these challenges, our project proposes an innovative solution – the integration of graphical passwords. Graphical passwords introduce a departure from traditional alphanumeric combinations, allowing users to create secure and memorable passwords through the selection of images. This approach not only enhances security but also aligns with users' preferences for meaningful yet memorable passwords [5].

In summary, our project endeavors to revolutionize information protection by addressing the limitations of traditional text-based authentication. The amalgamation of graphical passwords not only bolsters security but also prioritizes user experience and ease of use in an era where the safeguarding of personal information is paramount [6-8]. By leveraging a combination of innovative authentication methods, it aims to create a comprehensive and resilient security framework that prioritizes both security and user convenience. This approach aligns with the evolving landscape of cybersecurity threats and the imperative to safeguard sensitive information effectively in today's interconnected digital ecosystem.

2. Literature Review

Graphical passwords represent a departure from traditional alphanumeric authentication methods, offering users a more intuitive and memorable way to secure their digital accounts. One of the key advancements in this field is the development of graphical authentication schemes that leverage human visual memory. Unlike alphanumeric passwords, which can be difficult to remember, graphical passwords allow users to select images or graphical elements as their passwords. These images could be anything from familiar objects or scenes to abstract shapes.

One popular approach to graphical authentication is image-based authentication, where users authenticate themselves by selecting a sequence of images or graphical elements. The sequence of images serves as their password, adding an extra layer of complexity and security compared to traditional text-based passwords. Image-based authentication schemes are often used in conjunction with graphical elements such as images or patterns, providing users with a visually engaging and memorable authentication experience. Another common concept in graphical password authentication is grid-based authentication, where users select a sequence of points on a grid overlaid on an image. The specific sequence of points serves as their password, offering a balance between security and memorability[9]. Grid-based authentication schemes allow users to choose meaningful points on the image while ensuring sufficient randomness to resist attacks.

Recent trends in graphical password authentication include the exploration of biometric-based authentication methods, where users authenticate themselves using gestures, facial recognition, or other biometric markers overlaid on graphical elements [10]. Biometric-based authentication offers the potential for enhanced security and user convenience, as it leverages unique physiological characteristics for identity verification [11-13]. Furthermore, researchers are investigating the usability and security aspects of graphical passwords, exploring factors such as user acceptance and adoption rates, effectiveness of different graphical password schemes, and strategies for mitigating common attacks such as shoulder surfing and brute-force attacks. Usability studies aim to identify design principles that optimize the user experience while maintaining robust security.

Moreover, the integration of graphical passwords with other authentication factors, such as traditional text-based passwords or biometric markers, is an area of active research. By combining multiple authentication factors, researchers aim to create hybrid authentication systems that offer both security and convenience. In summary, graphical passwords represent an innovative approach to authentication, offering users a visually engaging and memorable way to secure their digital accounts. Ongoing research in this field focuses on advancing authentication methods, addressing usability and security challenges, and exploring new techniques for enhancing information security in the digital age.

Graphical passwords have evolved as a user-friendly [14] alternative to traditional alphanumeric authentication methods. They leverage the inherent capacity of human visual memory, offering users a more intuitive and memorable way to secure their digital accounts. Unlike alphanumeric passwords, which can be cumbersome to remember and prone to being forgotten or written down insecurely, graphical passwords enable users to select images or graphical elements that resonate with them personally. This shift from abstract characters to visual cues enhances both the memorability and usability of passwords, ultimately contributing to stronger security postures.

Click-based authentication is a prominent approach within graphical password systems. Users authenticate themselves by clicking on specific points or regions within an image. Each click contributes to the construction of a unique password sequence. The sequence of clicks serves as the user's password, introducing an additional layer of complexity and security compared to traditional text-based passwords. Click-based schemes often incorporate graphical elements such as images or patterns, providing users with a visually engaging and memorable authentication experience. Furthermore, click-based authentication can resist shoulder surfing attacks since the password sequence is not directly visible to observers.

Grid-Based Authentication: Grid-based authentication is another prevalent concept in graphical password systems. In this approach, users select a sequence of points from a grid overlaid on an image. The specific sequence of points chosen by the user forms their password. Grid-based schemes offer a balance between

security and memorability. Users can select meaningful points on the image, such as landmarks or significant features, while ensuring sufficient randomness to resist attacks. Grid-based authentication systems typically present users with an image overlaid with a grid of cells. Users are prompted to select a predetermined number of cells in a specific order to construct their password. The selection process may involve clicking, tapping, or dragging actions, depending on the implementation. One of the advantages of grid-based authentication is its flexibility in accommodating various image types and grid sizes. Users can choose images that are personally meaningful to them, such as family photos, landscapes, or abstract artwork. This personalization aspect enhances user engagement and encourages stronger password creation.
Moreover, grid-based authentication schemes often incorporate techniques to mitigate common attacks, such as grid distortion or cell shuffling. These techniques introduce variability into the grid layout, making it more challenging for attackers to predict or brute-force the correct password sequence. Additionally, grid-based authentication systems may incorporate measures to detect and prevent automated attacks, such as rate limiting or CAPTCHA challenges.
Click-based authentication is a notable method within graphical password systems, offering users a novel approach to authentication. Here's a deeper exploration of its features and advantages:

Interactive Authentication Process:
In click-based authentication, users engage directly with graphical elements, typically images or patterns, to construct their password sequence [15]. Each click on specific points or regions within the image contributes to the formation of a unique password. This interactive process not only enhances user engagement but also facilitates the creation of memorable passwords based on visual cues.

Enhanced Complexity and Security:
The sequence of clicks serves as the user's password, adding an extra layer of complexity and security compared to traditional text-based passwords. Unlike alphanumeric passwords, which rely solely on character combinations, click-based passwords leverage spatial relationships and sequence order within the graphical interface. This makes it significantly more challenging for attackers to guess or brute-force the correct password sequence, thereby enhancing overall security [16].

Visual Engagement and Memorability:
Click-based schemes often incorporate visually appealing elements such as images or patterns, providing users with a visually engaging and memorable authentication experience. By associating passwords with graphical cues, users can leverage their visual memory to recall the password sequence more effectively. This approach enhances memorability and reduces the likelihood of forgotten passwords or the need for insecure password management practices.[3]

Resistance to Shoulder Surfing Attacks:
One notable advantage of click-based authentication is its resilience to shoulder surfing attacks. Unlike traditional text-based passwords, where the password characters may be observed by nearby individuals, the password sequence in click-based schemes is not directly visible to observers. Since the authentication process involves interacting with graphical elements on the screen, observers would not be able to discern the password sequence by simply watching the user's interactions. This adds an additional layer of security and privacy to the authentication process, particularly in public or shared environments.In summary, click-based authentication offers a compelling alternative to traditional text-based passwords, leveraging interactive graphical elements to enhance security and user experience. By incorporating visually engaging elements and leveraging human visual memory, click-based schemes provide users with memorable and secure authentication methods. Additionally, their resistance to shoulder surfing attacks makes them particularly well-suited for use in public or shared environments where privacy and security are paramount. As research and development in graphical password authentication continue to advance, click-based authentication is likely to remain a prominent and effective approach for securing digital accounts.

3. Overview of proposed system

3.1. Supported Technologies and Algorithms
The proposed system is a web application that integrates React for the frontend and Node.js/Express for the backend. On the frontend, React is used for efficient UI component creation and state management, while React Router enables seamless client-side routing. FontAwesome enriches the UI with scalable vector icons, and Axios facilitates HTTP requests to interact with the backend server. Component-level state management is handled through React's usestate hook, with Nanoid ensuring the generation of unique IDs. On the backend, Node.js/Express manages routes and business logic, interfacing with MongoDB for flexible data storage, facilitated by Mongoose for abstraction. The application utilizes the Unsplash API for image searching. Additional features include WebSockets for real-time communication, validation libraries for data integrity, and toast notifications for user feedback. Responsive design ensures adaptability across devices, while basic web technologies like HTML, CSS, and JavaScript form the foundation. Express Static File

Middleware serves static files, and CommonJS modules structure backend code. Overall, the system employs a modern tech stack and best practices to deliver a robust and user-friendly web experience.

3.2. Proposed Work Plan

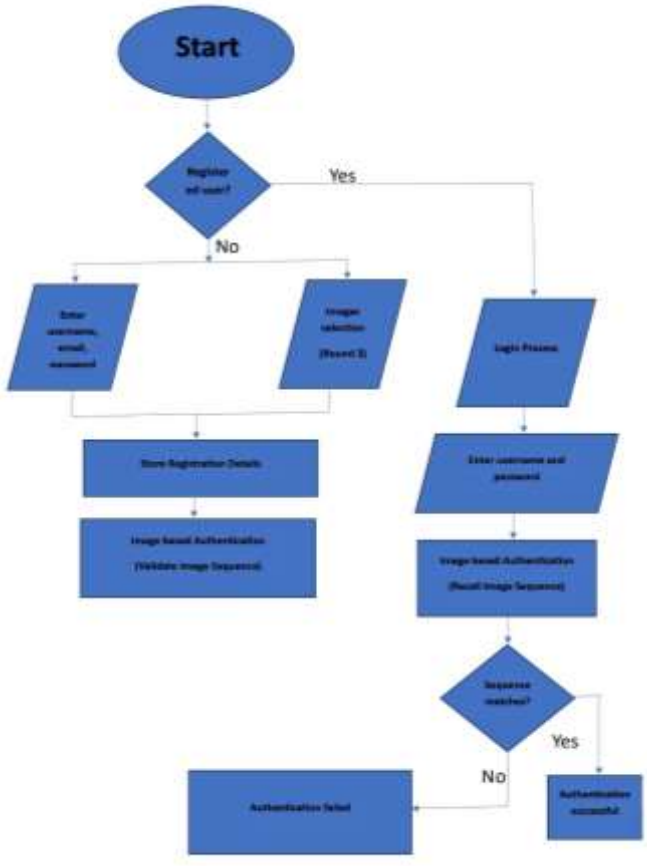

Fig. 1 Flowchart of the proposed image based authentication system

The system is designed to handle both new user registrations and returning user authentication seamlessly as shown in Fig. 1. When a new user visits the website, they are guided through a registration process that begins with providing their personal details such as name, email, and any other required information. After this initial step, the user is prompted to create a unique username and password combination. The system enforces password strength requirements to ensure security.

Following the username and password setup, new users undergo an image-based authentication process. This process involves the user memorizing a sequence of images or patterns presented to them. The purpose of image-based authentication is to create a personalized and secure login method specific to each user, enhancing overall account security.

For returning users, the authentication process is streamlined. Upon visiting the website, returning users are prompted to enter their username and password only. The system verifies these credentials against the stored data. If the username and password combination matches, the user is successfully authenticated and granted access to the website's content and features tailored to their account.

In cases where authentication fails, such as incorrect username or password input, the system notifies the user and terminates the access attempt. This ensures that only authorized users with valid credentials can access the website's resources, maintaining security and privacy for all users.

Overall, the system combines registration, image-based authentication for new users, and username/password authentication for returning users to create a comprehensive and secure access control mechanism. This approach aims to provide a user-friendly experience while upholding stringent security standards to protect user accounts and data.

4. Result and Implementation Details

Our algorithm plays a pivotal role in the design and functionality of our website, particularly in the registration and login processes. It ensures robust security measures while maintaining user-friendliness, thereby enhancing the overall user experience. By incorporating multi-layered authentication techniques and

dynamic visual elements, our algorithm elevates the website's security standards to meet contemporary cyber security demands.
Some of the key steps any user will encounter while he visits the website is:
- Registration
- Login
- Authentication status : failure or success

4.1. Registration

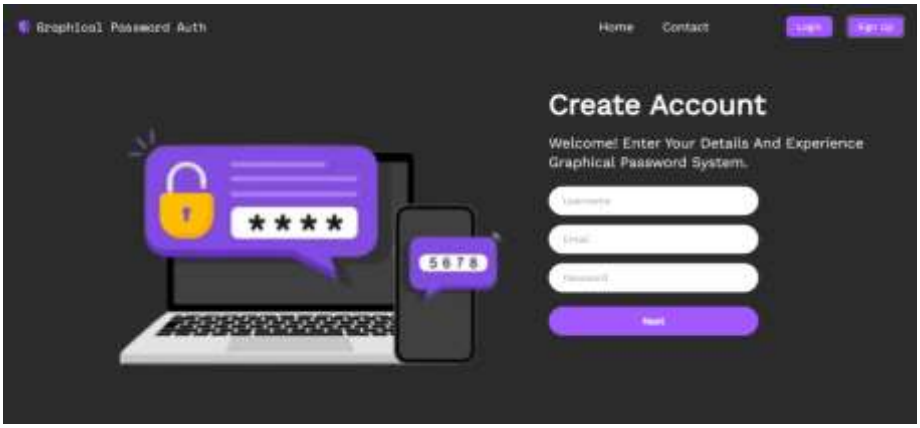

Fig. 2 Create your account with a graphical password by entering your username and password.

4.1.1. User Registration:

The user begins the registration process by creating a unique username and a secure password as shown in Fig. 2. Once the username and password are set, the user proceeds to the image selection phase, which involves three rounds. This step adds an extra layer of security by requiring the user to select images based on specific keywords, creating a unique pattern that enhances the overall security of their account.In each of the three rounds, the user is prompted to enter keywords into a search bar, generating a set of images related to those keywords. From each set, the user selects 4 images, resulting in a total of 12 images by the end of the process. This multi-step selection process ensures that the image sequence is both memorable to the user and difficult for unauthorized parties to replicate, significantly increasing the complexity of the authentication process.Once the image selection process is complete, the system securely encrypts all user details, including the username, password, and the selected image sequences. This encrypted data is then stored in the system's database, protected by multiple layers of security measures such as firewalls and access controls. This comprehensive approach to authentication combines traditional and innovative security measures, providing robust protection against unauthorized access.

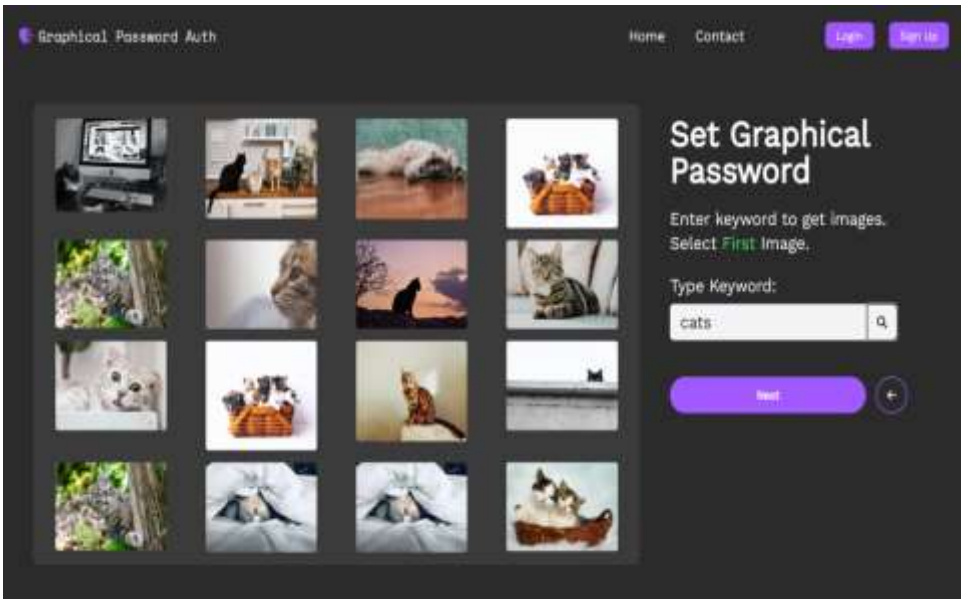

Fig. 3. Image shows a website used to set up a graphical password, where users choose images instead of text characters or Setting up a graphical password on a website.

4.2. Login

Fig. 4 This figure shows the Login page whenever a user wants to login on the website.

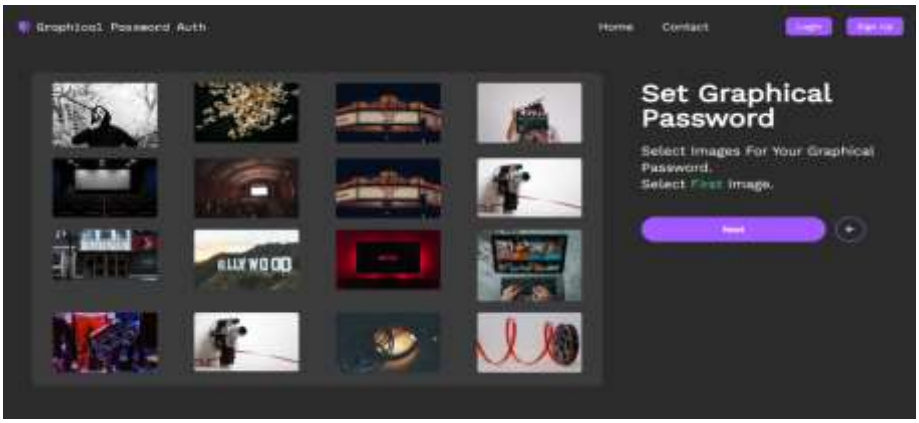

Fig. 5. Selected images in specific order to perform user authentication

4.2.1. Login Process:

The login process begins when the user enters their username and password. This initial step is crucial for verifying the basic credentials that the user provided during registration. The system cross-checks these credentials with its securely stored database to ensure they match.

After successfully validating the username and password, the system prompts the user to select images in the same sequence they chose during the initial registration process. This step introduces a secondary layer of security that relies on the user's ability to recall a specific sequence of images. The use of image sequences leverages the human brain's strong capacity for visual memory, adding a personalized element to the authentication process. This additional verification method significantly enhances security by requiring something only the legitimate user would know.

To prevent potential security breaches, the system presents the images in a random order each time the user attempts to log in. This randomization ensures that even if someone observes the user's screen, they cannot easily discern the correct sequence of images. The user must correctly identify and select the images in the exact sequence chosen during registration for authentication to be successful. If the sequence matches, the system grants access to the user's account. This multi-layered approach, combining traditional credential verification with a dynamic, visual-based sequence, ensures a high level of security and reduces the risk of unauthorized access.

4.3. Authentication Success

Fig. 6 Message Generated: Access granted! Secured with a unique graphical password.

4.3.1 Authentication:

- System verifies credentials: The system compares the provided credentials against a stored database or authentication server [15-17].
- Success or failure: If the credentials match, the system grants access and displays a success message. Otherwise, it denies access and prompts the user to try again.

5. Dataset Description

The dataset used in this project is stored in a MongoDB database [18] and encompasses user information vital for the functioning of the Graphical Image Password Authentication System. The system focuses on enhancing online security through the utilization of image-based passwords.

• Data Source:
The data originates from user registrations through the project's signup process.
User details include email, username, and image-based passwords selected during signup.

• Data Type:
Structured data stored in a NoSQL format within MongoDB.
Attributes include user email, username, and encrypted image password details.

• Email:
Unique email addresses provided by users during signup.
Username: Distinctive usernames chosen by users during the registration process.
Password (Images): Images selected by users during signup to serve as graphical passwords.

• Data Size:
The dataset grows dynamically as users register and contribute information to the system.
Each user's data includes email, username, and image password details.

• Preprocessing:
Encryption is applied to the image passwords before storage to enhance security.
Validation checks ensure the integrity and format of user-provided information.

• Usage:
The dataset is utilized for user authentication during the login process.
MongoDB facilitates efficient storage, retrieval, and management of user information.

• Security Measures:
Encrypted storage of sensitive information ensures user privacy.
Access controls and authentication mechanisms are implemented within the MongoDB environment

• Relevance to Project:
The dataset is fundamental to the successful functioning of the Graphical Image Password Authentication System.
User authentication, security, and system robustness rely on the accuracy and security of the stored data.

6. Experimental Result Analysis

The proposed graphical password image authentication system underwent a series of experiments to evaluate its effectiveness and security features. The experiments primarily focused on user registration, login processes, image-based authentication, application security, and overall system performance [31][32][33][34].

User Registration:

- The user registration process involved the selection of images in three rounds, demonstrating a multi-step approach to enhance security.
- The registration system successfully stored user details and selected image sequences securely.

Login Process:

- Users initiated the login process by providing their credentials and recalling image sequences from the registration phase.
- The multi-round image recall mechanism proved effective, adding an additional layer of security beyond traditional username/password validation.

Image-Based Authentication:

- The system accurately validated user-selected image sequences, ensuring successful authentication when the recalled sequence matched the registered one [19].
- Multi-factor authentication using user-selected images contributed significantly to the security of the login process.

Application Security:

- The graphical password authentication method demonstrated enhanced security compared to traditional PIN-based methods.
- User accounts and sensitive information were securely stored, contributing to the overall robustness of the system.[17]
- Multi-factor authentication using images provided an additional layer of security against unauthorized access.

Secure Operations:

- Users could perform various secure transactions and access sensitive features within the application.
- The graphical password authentication method remained consistent for subsequent logins, ensuring a seamless yet secure user experience.

One of the pivotal strengths of the graphical password image authentication system lies in its implementation of a multi-round image selection process with minimum entropy [20]. This sophisticated mechanism significantly augments the complexity of user authentication, surpassing the limitations of conventional alphanumeric passwords. By necessitating the selection of multiple images in a sequential manner, [21, 22] the system introduces a formidable barrier against potential unauthorized access attempts. This strategic approach not only enhances security but also fosters a sense of user empowerment, as individuals can create intricate and personalized authentication sequences that are both memorable and resilient to exploitation by malicious actors.

In essence, the experimental validation of our proposed graphical password image authentication system substantiates its efficacy in surmounting the inherent limitations of traditional authentication methods. Its robust security features, coupled with a seamless user experience, position it as a formidable contender for adoption across various domains where safeguarding sensitive information is paramount. As we continue to refine and optimize the system based on ongoing research and user feedback, we envision its widespread adoption as a pivotal step towards fortifying digital security paradigms in an increasingly interconnected and data-centric landscape.

7. Conclusion

The experimental findings derived from our research underscore the remarkable efficacy of the proposed graphical password image authentication system in mitigating the prevalent security challenges inherent in traditional authentication methodologies. Through a meticulous analysis of the system's performance, we have observed a substantial improvement in addressing key security concerns, thereby positioning it as a formidable solution for contemporary cybersecurity needs.

Moreover, the system's adeptness in securely storing user information further reinforces its credibility as a robust authentication solution. The integration of advanced encryption protocols and secure storage practices ensures that sensitive user data remains shielded from unauthorized access or data breaches. This fortified security posture not only instills confidence in users regarding the protection of their credentials but also underscores the system's adherence to stringent data protection standards and regulatory requirements.

Additionally, the seamless user experience offered by the graphical password image authentication system serves as a testament to its practical viability. The intuitive interface, coupled with user-friendly navigation, facilitates a smooth and hassle-free authentication process. This user-centric design ethos not only enhances user satisfaction but also contributes to heightened security, as it encourages adherence to best practices without sacrificing convenience.

8. References

1. Maw Maw Naing, Ohnmar Win (2019). Graphical Password Authentication using image Segmentation for Web Based Applications. Published in International Journal of Trend in Scientific Research and Development (Ijtsrd), (4).

2. Patrick, Andrew; Long, A.C.; Flinn, Scott(2003). HCI and Security Systems. Presented at the CHI '03 extended abstracts, Ft. Lauderdale, Florida, USA.
3. Kumar, R., Ratnesh, R. K., Singh, J., Kumar, A., & Chandra, R. (2024). IoT-driven experimental framework for advancing Electrical Impedance Tomography. ECS Journal of Solid State Science and Technology: JSS, 13(2)
4. Garg, P., Chandra, T., Ahlawat, R., Mittal, N., Ratnesh, R. K., & Tripathi, S. K. (2022). Star Galaxy Image Classification Via Convolutional Neural Networks. 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC). Trichy, India.
5. Kotadia, M. (2005). Microsoft: Write down your passwords (ZDNet Australia, Ed.).
6. Xiaoyuan Suo Ying Zhu G. Scott(2005). Graphical Passwords, A Survey. SourceDBLP Conference: 21st Annual Computer Security Applications Conference (ACSAC).
7. Kumar, R., Ratnesh, R. K., Singh, J., Chandra, R., Singh, G., & Vishnoi, V. (2023). Recent prospects of medical imaging and sensing technologies based on electrical impedance data acquisition system. Journal of the Electrochemical Society, 170(11), 117507.
8. Kothiyal, S. R., Ratnesh, R. K., & Kumar, A. (2023). Field Effect Transistor (FET)-Sensor for Biological Applications, International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)-2023 (pp. 433–438). IEEE.
9. Housamkhalifabashier, L., & Pang, Y. (n.d.)(2013). Graphical Password: Pass-Images Edge Detection. IEEE 9th International Colloquium on Signal Processing and its Applications.
10. Jain, M., Khurana, A., & M. Tech, Shri Ram Institute of Technology, Jabalpur, Madhya Pradesh, India. (2018). Biometric Finger Print Identification using DWT Byreal Minutiaeextraction. International Journal of Trend in Scientific Research and Development, 2(4)
11. Gilhooly, K. (2005). Biometrics: Getting Back to Business. Computerworld.
12. Garg, A., Ratnesh, R. K., Chauhan, R. K., Mittal, N., & Shankar, H. (n.d.)(2022). Current Advancement and Progress in BioFET: A Review, International Conference on Signal and Information Processing (Vol. 2022, pp. 1–7). IEEE.
13. Garg, A., & Ratnesh, R. K. (2022). Solar Cell Trends, and the Future: A Review. Journal of Pharmaceutical Negative Results, 13, 2051–2060.
14. Adams, A., & Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42, 41–46.
15. R. Dhamija and A. Perrig(2000). Deja Vu: A User Study Using Images for Authentication. In Proceedings of 9th USENIX Security Symposium.
16. Hasegawa, M., Tanaka, Y., & Kato, S. (2009, December). A study on an image synthesis method for graphical passwords. 2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS). Presented at International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS 2009), Kanazawa, Japan.
17. Kwon, T., Shin, S., & Na, S. (2014). Covert attentional shoulder surfing: Human adversaries are more powerful than expected. IEEE Transactions on Systems, Man, and Cybernetics. Systems, 44(6), 716–727.
18. Ankita Kurrey, Aditya Singh , Lalita Panika , Dr Padmavati Shrivastava (2023). TheAuthguard – A Graphical Password Authentication System. Published in International Journal of Research Publication and Reviews (IJRPR)
19. Kar-Ann Toh, Q.-L., & Tran, D. (n.d.).(2004) Benchmarking a Reduced MultivariatePolynomial pattern classifier. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 26(6).
20. Davis, D., Monrose, F., & Reiter, M.K. (2004). On User Choice in Graphical Password Schemes. *USENIX Security Symposium*.
21. Kalaivizhi, P., M.Tech(CSE), Prist University, CSE, Puducherry, & Nirai Senthil, D. S. T. (2014). Online password guessing attacks by using persuasive click point with dynamic user block. *IOSR Journal of Computer Engineering*, *16*(3), 104–108. doi:10.9790/0661-1634104108
22. Faiz, M., & Daniel, A. K. (2022). Threats and challenges for security measures on the internet of things. Law, State and Telecommunications Review, 14(1), 71-97.
23. Mall, P. K., Narayan, V., Pramanik, S., Srivastava, S., Faiz, M., Sriramulu, S., & Kumar, M. N. (2023). FuzzyNet-Based Modelling Smart Traffic System in Smart Cities Using Deep Learning Models. In S. Pramanik & K. Sagayam (Eds.), Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities (pp. 76-95). IGI Global. https://doi.org/10.4018/978-1-6684-6408-3.ch005
24. Choudhary, S., Narayan, V., Faiz, M., & Pramanik, S. (2022). Fuzzy approach-based stable energy-efficient AODV routing protocol in mobile ad hoc networks. In Software Defined Networking for Ad Hoc Networks (pp. 125-139). Cham: Springer International Publishing.
25. M. Faiz and A. K. Daniel, "Fuzzy Cloud Ranking Model based on QoS and Trust," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1051-1057, doi: 10.1109/I-SMAC49090.2020.9243414.
26. Faiz, M., & Daniel, A. K. (2021, December). Multi-criteria based cloud service selection model using fuzzy logic for QoS. In International Conference on Advanced Network Technologies and Intelligent Computing (pp. 153-167). Cham: Springer International Publishing.

27. Narayan, V., Daniel, A. K., & Chaturvedi, P. (2023). E-FEERP: Enhanced fuzzy based energy efficient routing protocol for wireless sensor network. Wireless Personal Communications.
28. Narayan, V., & Daniel, A. K. (2022). CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network. International Journal of System Assurance Engineering and Management, 13(Suppl 1), 546-556.
29. Narayan, V., & Daniel, A. K. (2022). Energy Efficient Protocol for Lifetime Prediction of Wireless Sensor Network using Multivariate Polynomial Regression Model.
30. Narayan, V., & Daniel, A. K. (2021, October). IOT based sensor monitoring system for smart complex and shopping malls. In International conference on mobile networks and management (pp. 344-354). Cham: Springer International Publishing.
31. Narayan, Vipul, et al. "A comparison between nonlinear mapping and high-resolution image." Computational Intelligence in the Industry 4.0. CRC Press, 2024. 153-160.
32. Sandhu, Ramandeep, et al. "Enhancement in performance of cloud computing task scheduling using optimization strategies." Cluster Computing (2024): 1-24.
33. kumar Mall, Pawan, et al. "Self-Attentive CNN+ BERT: An Approach for Analysis of Sentiment on Movie Reviews Using Word Embedding." International Journal of Intelligent Systems and Applications in Engineering 12.12s (2024): 612-623.
34. Narayan, Vipul, et al. "7 Extracting business methodology: using artificial intelligence-based method." Semantic Intelligent Computing and Applications 16 (2023): 123.