International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 03, 2026

RESEARCH ARTICLE OPEN ACCESS

Reinventing Authentication through User-Centric Two-Factor Security and Personalized Image Verification

J Sivarani . D Lashya Kumari . A Jyothsna . S K Mohammed Khaif . I Hithaishi

Department of CSE (IoT and Cyber Security including Block Chain Technology),
Annamacharya Institute of Technology & Sciences (Autonomous),
Tirupati, A.P, India.

DOI: **10.5281/zenodo.18683037**
Received: 29 January 2026 / Revised: 12 February 2026 / Accepted: 17 February 2026
**Corresponding Author: sivaraniaits@gmail.com*

Abstract – In the wake of the rising digital world, traditional username/password-based authentications are facing an increased risk of being compromised by various cyber attacks, including phishing, brute force attacks, credential stuffing, and artificial intelligence-based impersonation attacks. While traditional two-factor authentications provide better security than traditional username/password-based authentications, these methods often bring their own set of problems, including usability issues. To overcome the limitations of traditional two-factor authentication, this paper proposes a two-factor authentication system based on traditional username/password-based authentication and image/keyword-based authentication. The system utilizes the capabilities of human visual memory to provide better security with minimal cognitive overhead for the users. The system utilizes secure cryptographic techniques to ensure the security of the system, keyword-based image verification to prevent replay attacks, and device-based restriction techniques to prevent brute force attacks. The system is developed based on the client-server model using the Django framework. The experimental results confirm that the proposed authentication system achieves an optimal balance between usability and security, making it a feasible solution for web application security.

Index Terms – Two-Factor Authentication, User-Centric Security, Image-Based Authentication, Graphical Passwords, Cybersecurity, Access Control, Personalized Authentication, Web Application Security, Brute-Force Attack Mitigation, Secure Login Systems.

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

I. INTRODUCTION

Cybersecurity is one of the most critical issues of the modern world, as everything is becoming increasingly digitized. As the number of services, platforms, and apps on the internet is increasing rapidly, the number of cyber attacks is also increasing [1]. According to recent security reports published on a global scale, it has been observed that credential misuse is one of the major ways used by attackers to gain access to a particular digital environment. A recent leak of a massive number of credentials has been observed [2]. Although password-based authentication is commonly used, there are inherent limitations associated with such systems. Passwords are highly vulnerable to brute-force attacks, phishing attacks, dictionary attacks, and credential stuffing attacks, which often result in major security breaches and financial losses [3]. Even though one-time passwords are integrated with password-based authentication mechanisms, phishing attacks such as phishing as a service have demonstrated their ability to bypass these authentication mechanisms, thereby demonstrating the limitations associated with static security mechanisms [4]. All these challenges highlight the need for developing more reliable authentication mechanisms to counter the ever-changing security challenges in an effective and user-friendly manner.

In particular, the concept of multi-factor authentication (MFA) and two-factor authentication (2FA) has been recognized as an efficient means to prevent unauthorized access. With the integration of different independent factors, such as something the user knows, something the user possesses, and something the user is, 2FA is recognized to provide robust security against potential breaches of accounts [5]. Recent research in 2025 highlights the importance of MFA in the context of zero-trust security architecture, which involves continuous verification to ensure identity in distributed systems [6]. In parallel, research has been shifting focus towards more intelligent and user-centric types of authentication systems. Deep learning-based and adaptive types of authentication systems utilize behavioral, biometric, and contextual factors in order to dynamically determine the legitimacy of the user [7]. Image-based and graphical types of authentication systems, in particular, have received increased attention due to their potential in leveraging human memory in order to provide increased immunity against password cracking attacks and shoulder-surfing attacks, all without requiring any special hardware support [8].

However, with the emergence of new threats such as AI-based phishing and deep fake-based impersonation, the traditional concept of authentication still faces a challenge [9]. In this regard, the evolution of modern authentication systems should aim to include the concepts of resilience, flexibility, and usability. The design of an input system is a significant factor in the evolution of authentication systems towards meeting the demands of modern authentication. This is because an input system should be able to capture user inputs appropriately and securely, regardless of whether the input is text-based, voice-based, or image-based [10]. Inspired by these challenges, we propose a user-centric two-factor authentication system that combines the traditional username/password mechanism with a personalized image-based mechanism. This proposed system seeks to mitigate password-based attacks while providing an intuitive user interface. This proposed system enhances security in the authentication process without adding cognitive burden to users, making it suitable for modern digital applications.

Our contributions are as follows:

- User-Centric Two-Factor Authentication Framework: In this paper, a new user-centric two-factor authentication framework is proposed, which integrates the traditional username and password authentication process with the personalized image and keyword-based authentication process.
- Personalized Image-Keyword Verification Mechanism: Contrary to the traditional second-factor authentication process that uses OTP or hardware tokens, the proposed system uses personalized images associated with dynamic keywords. Randomized keyword selection for each login attempt makes the system less predictable and more resistant to replay and observation attacks.
- Device-Based Attempt Restriction for Improved Security: A device-based access control system is integrated into the system to monitor the number of incorrect login attempts. This provides increased security against brute-force attacks, leading to zero unauthorized access in the system.
- Seamless and Error-Resistant Input Design: The system includes an intelligent input design strategy that validates user data and ensures fewer errors in user interactions. This provides logical verification of user data, ensuring a seamless, secure, and error-resistant user experience.
- Multi-Modal and User-Friendly Output Design: A comprehensive output design is integrated into the system to provide user authentication responses, system responses, and alerts in an understandable manner. Outputs are provided in multiple modes, including visual and voice-based responses, to ensure timely responses, accurate error messages, and meaningful user security alerts.

II. LITERATURE SURVEY

To fill the gap in research on ensuring both security and usability in the authentication of smartphones, Ray et al. [11] suggested GPNST, a graphical password authentication framework based on the neural style transfer method on smartphones. The system is the combination of content and stylized images and device-specific key token relayed by reversible data hiding. The research indicated the accuracy of authentication of 94.80 % and an average time of 9.61 seconds to log in. The originality of this work is the combination of the neural style transfer and the two-factor graphical authentication. The scheme is, however, relatively higher in terms of the time of logging in and has not yet tested at a large scale in a real-world scenario. Qin et al. [12] suggested RoundImage, which is a multi-round image selection-based graphical password system in the IoT setting, as a method to eliminate shoulder-surfing attacks. There is also the system of fault tolerance, which gives the users the ability to authenticate through the image selection multiple rounds. In the case of experiment evaluation, where 100 people were involved, the usability and security proved to be ineffective. The study is also limited to a simulated Internet of Things, though it does not investigate resistance to sophisticated attack models.

To address the drawbacks of the traditional text-based passwords regarding brute force and automated attacks, Chihi et al. [13] came up with an improved graphical password authentication scheme based on visual cryptography. The innovation is in the fact that it increases the image secret sharing to generate a higher level of security and usability. Despite the scheme enhancing resistance to automated attacks, it has added storage and computational overhead and has not been evaluated comprehensively with respect to users. Anjaneyulu et al. [14] have come up with an image selection-based scheme of authentication using a graphical user interface to enhance memorability in place of alphanumeric passwords. The paper indicates the benefit of visual memory in authentication systems. Nevertheless, it is still exploratory with no quantitative performance values and experimental affirmation of security strength.

Rasheed et al. [15] suggested a drawing graphical password architecture with deep learning that utilized Arabic digit recognition to resolve the gap in the research of limited flexibility in graphical authentication. The system proposes a Selected Pixels (SP) method to minimize the overhead of the transmission and storage of data. The experimental outcomes indicated that there were improvements in the time to log in, efficiency of the data, and password entropy. Nevertheless, the scheme strongly relies on the likelihood of the deep learning models and the user's ability to draw. The memorability can be improved by the Subject-Based Graphical Authentication (SBGA) that was proposed by Suru [16] with discipline-specific familiar images instead of abstract images. The documented success rate of the study was 81.7 %, which is way ahead of abstract-based schemes. Its innovation is in its use of the familiarity of users to enhance usability. Nevertheless, by using predictable image categories, the password entropy and security might be compromised.

The suggested system by Ray et al. [17] is the GPOD, a graphical password authentication system that uses YOLOv3-based object detection, which can create and validate graphical challenges. The scheme deals with shoulder-surfing, brute force, and database attack by object detection and encrypted data storage. The system had an accuracy of up to 94.80%, but the time of logins was longer in some instances. The primary weakness is the calculation cost of real-time object detection. Dhinesh et al. [18] suggested ImageGuard, which is a secure image sequence-based authentication system with click-based and choice-based graphical password manipulation. The scheme recorded a high user satisfaction rate, which was 92% authentication success. Nonetheless, it can still be susceptible to observation attacks in case of exposure of user interactions. To address the shoulder-surfing attacks, Dias et al. [19] suggested a graphical password authentication scheme with a Deep Residual Network, edge detection, and decoy image generation. The system enhanced knowledge of the information and diversification of passwords as opposed to conventional practices. However, the method adds computational complexity and has not been substantially substantiated in reality. Andriotis et al. [20] proposed Bu-Dash, which is a dynamic graphical password scheme that builds upon the Android Pattern Unlock to prevent shoulder-surfing and smudge attacks. The innovativeness is in a dynamically mutating interface that does not degrade usability and improves security. Nevertheless, it was evaluated only on pilot studies and not on user behavior in the long term.

Table 1: Overview of Existing Works

Ref	Authors (Year)	Authentication Scheme / Model	Key Technique / Architecture	Key Numerical Results	Main Limitation
[11]	Ray et al. (2025)	GPNST	Neural Style Transfer, reversible data hiding, two-factor graphical authentication	94.80% authentication accuracy, avg. login time 9.61 s	High login time; not evaluated at large scale or real-world deployment
[12]	Qin et al. (2025)	RoundImage	Multi-round image selection, fault tolerance mechanism	Usability and security found ineffective in 100-user study	Evaluated only in simulated IoT; limited analysis of advanced attacks

[13]	Chihi et al. (2024)	Visual Cryptography–based Graphical Password	Image secret sharing, visual cryptography	Improved resistance to brute-force and automated attacks	Increased storage and computational overhead; lack of comprehensive user evaluation
[14]	Anjaneyulu et al. (2024)	Image Selection–based GUI Authentication	Visual memory–based authentication interface	Qualitative improvement in memorability (no numeric metrics)	Exploratory study; no quantitative performance or security validation
[15]	Rasheed et al. (2024)	DL-based Drawing Graphical Password	Deep learning, Arabic digit recognition, Selected Pixels (SP) method	Improved login time, data efficiency, and password entropy	Strong dependency on DL model accuracy and user drawing ability
[16]	Suru (2023)	Subject-Based Graphical Authentication (SBGA)	Discipline-specific familiar images	81.7% authentication success rate	Predictable image categories may reduce password entropy
[17]	Ray et al. (2024)	GPOD	YOLOv3-based object detection, encrypted storage	Up to 94.80% accuracy	High computational cost of real-time object detection; increased login time
[18]	Dhinesh et al. (2024)	ImageGuard	Click-based and choice-based image sequence authentication	92% authentication success; high user satisfaction	Vulnerable to observation attacks if user interaction is exposed
[19]	Dias et al. (2024)	DRN-based Graphical Password Scheme	Deep Residual Network, edge detection, decoy images	Improved password diversification (no large-scale metrics)	High computational complexity; lack of real-world validation
[20]	Andriotis et al. (2023)	Bu-Dash	Dynamic Android pattern mutation	Improved resistance to shoulder-surfing and smudge attacks	Limited to pilot studies; no long-term user behavior analysis

III. METHODOLOGY

The methodology of this work is primarily concerned with the design and implementation of a secure and user-centric two-factor authentication system, which can improve the existing traditional login system through the use of personalized image verification. The proposed methodology is a systematic approach to address the issues associated with existing traditional login systems.

- User Registration Phase: In this step, an account is created by assigning a username and a password. It should be noted that the password is not stored in plain text format. Instead, it is secured using strong cryptographic techniques before being stored in the database
- Primary Authentication Phase: During login, the username and password are entered in the browser. The Django authentication controller verifies the submitted credentials by comparing the encrypted password hash with the hash value in the user table.

- Secondary Image-Based Verification Phase: Once the first level of authentication has passed, the system selects a keyword that corresponds to the images stored for the user. The keyword appears at random on the screen, and the user is prompted to upload the image that corresponds to it. The uploaded image is matched against the encrypted reference image stored in the ImageKeyword table.
- Device-Based Attempt Control and Security Enforcement: To enhance security, the system has been designed to restrict logins by device. When a login attempt is made from an unknown or new device, it will be more restricted.
- Encryption, Logging, and Audit Trail: All sensitive operations, such as checking credentials, verifying images, and processing keywords, are all encrypted. The system maintains a thorough audit trail of all authentication activities, including successful, failed, and blocked access attempts. These audit logs are encrypted and stored separately from the credentials for security purposes.

A. Proposed System Analysis

The system aims to eliminate common problems users face in conventional authentication systems by providing a unique two-factor authentication mechanism that combines image verification with the conventional username and password mechanism. It tries to provide security without increasing the cognitive load on users, thereby providing a simple and efficient authentication mechanism that incorporates the concept of "something that a user knows" and "something that a user can see," which in this case is a unique image–keyword combination that the user can relate to.

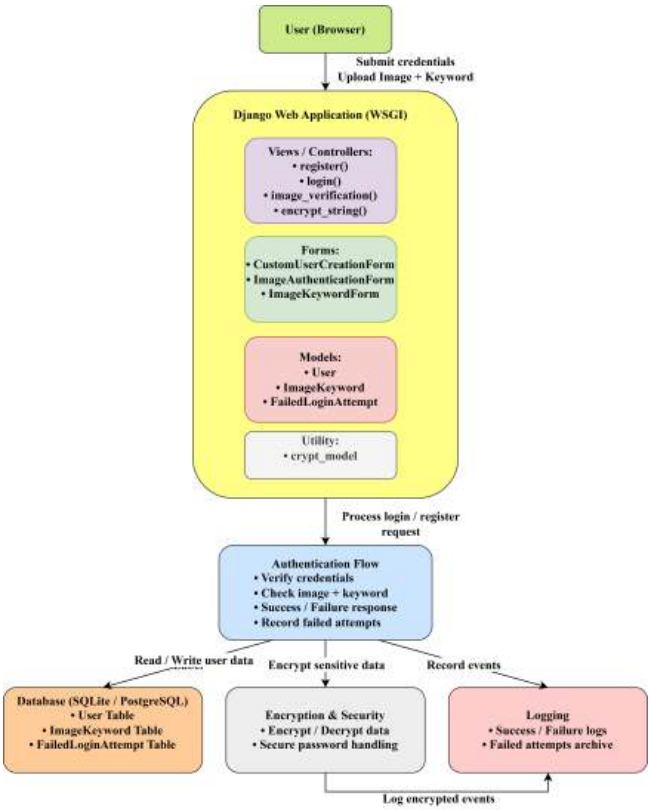

Fig. 1: Graphical representation of the AI-Powered Cybersecurity Architecture

From the above description, it can be seen that the authentication mechanism follows a simple client–server model, where users access the system through a web browser, which serves as the external interface that interacts with the authentication system and receives the authentication verdict. On the back end, a web app built with the Django framework and running in a WSGI environment serves as the interface, securely interacting with the external system and dividing the authentication process into small, modular pieces.

The architecture comprises four layers that are closely integrated:

- User Interface Layer
- Application Logic Layer
- Security and Encryption Layer
- Data Storage and Logging Layer

i. Authentication Workflow Analysis: There are two consecutive stages to the authentication procedure. The system verifies traditional credentials in the first stage. Let's define the primary login authentication function as follows:

$$A_1 = f\ (U, P)$$

where P stands for the encrypted password and U for the username, authentication only happens if:

$$A_1 = True$$

The system transitions to the second verification stage, which is image-based. During user registration, every user chose a set of images $\{I_1, I_1, \dots \dots, I_n\}$where each image is mapped to a unique keyword $\{K_1, K_1, \dots \dots, K_n\}$. The ImageKeyword table safely stores this mapping. During login, the system randomly chooses a keyword K_r such that:

$$K_r \in \{K_1, K_1, \dots \dots, K_n\}$$

After that, the user must upload the matching image I_r. The following is an expression for the second factor's verification function:

$$A_2 = g\ (I_u, K_r)$$

where, I_u is the uploaded image. Authentication is granted when:

$$A_2 = True$$

Thus, the ultimate authentication choice is described as follows:

$$\mathrm{A} = A_1\ \wedge\ A_2$$

ii. Personalized Image–Keyword Verification Analysis: The presented approach uses user-selected visual material rather than traditional second-factor methods like hardware tokens or OTPs. This method uses the cognitive power of human visual memory, which has been shown to perform better in long-term authentication settings than textual recall. Replay attacks are prevented, and predictability is decreased by the random keyword selection used during each login session.

iii. Device-Based Attempt Restriction Mechanism: The system has a device-based login attempt restriction mechanism to improve resilience against automated and brute-force attacks further. The system keeps a record of failed login attempts and links each attempt to a device fingerprint. Let, T_d defines the number of failed attempts from d. Access control policies enforce:

$$T_d \leq T_{max}$$

iv. Encryption and Data Security Analysis: Cryptographic techniques are used to safeguard all sensitive data processed by the system. Before storage, passwords, picture references, and keyword mappings are encrypted. Let, E (x) describes the encryption function and D (x) the decryption function. For any sensitive data S:

$$S_{stored} = E\ (S)$$
$$S = D\ (S_{stored})$$

v. Logging, Auditing, and Accountability: The system's extensive logging system records both successful and unsuccessful authentication events. Each log entry includes timestamp, device identification, authentication result, and, if relevant, the failure cause. To guard against correlation attacks, logs are encrypted and kept apart from authentication data.

vi. Security and Usability Trade-off Analysis: The proposed system's ability to strike a balance between security and usability is one of its main advantages. In contrast to biometric or OTP-based systems, the suggested framework is independent of network accessibility, external devices, and irreversible biological characteristics. Using intuitive image-based identification instead of difficult memorization tasks also avoids adding to the user's workload.

B. System Deployment Architecture

The user-centric approach to two-factor authentication, as proposed, is designed to be secure in terms of its communication, modular in terms of its services, and seamless in terms of its distributed parts. In the diagram above that presents the deployment of the system, it is clear that it is designed to run in an internet-based client-server setup in which the process of authentication is done through coordinated steps in the client device, the application server, and the dedicated server that handles authentication, which is backed by an image database. The service-oriented approach is utilized in the deployment of the system, separating the main web application from the service that handles authentication. This is done in order to increase scalability, reduce risks, and allow independence in handling the service from the other services of the application.

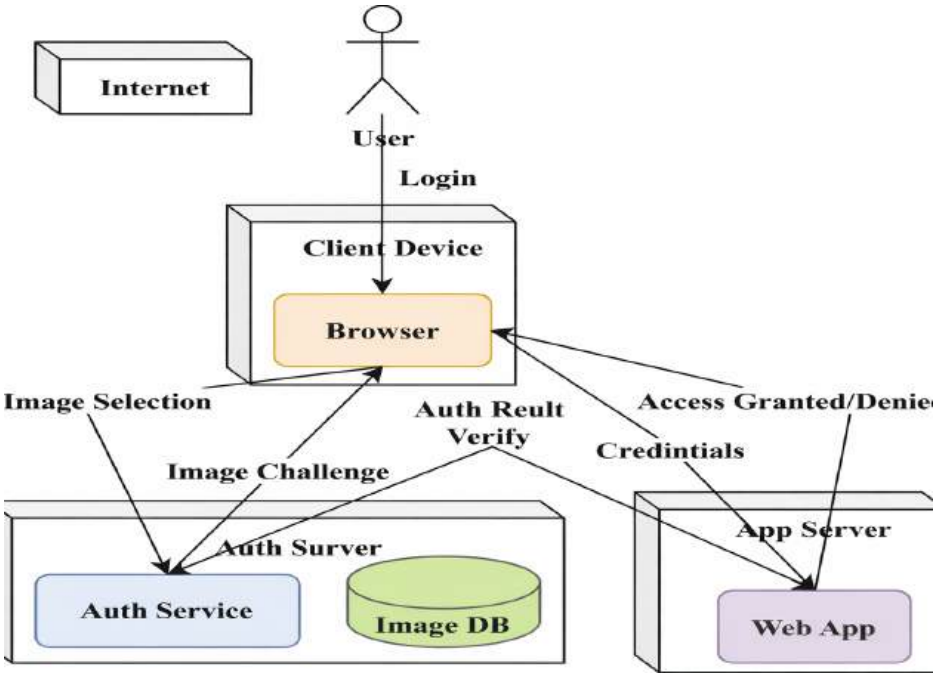

Fig. 2: Deployment Procedure of the Cybersecurity System

IV. HARDWARE SOFTWARE SPECIFICATION

The efficacy of an authentication system is not only based on its algorithmic security, but also on the hardware and software infrastructure on which it is implemented. In the proposed framework for image-based two-factor authentication, various hardware and software components are selected based on principles of computational efficiency, security assurance, scalability, and usability. Thus, it is ensured that various cryptographic and image-processing operations, along with real-time user interactions, are performed without causing significant delays or security risks. Authentication systems need a constant level of computational performance for processing various stages of credential verification, encryption, and secondary authentication factors. From a theoretical perspective, the proposed system has a moderate level of computational complexity since it incorporates password hashing, encryption, and additional authentication factors.

The multi-core processor is essential in the system as it is required to handle concurrent processing operations such as user request processing, session management, and background security processing. The main memory should be adequate to load the images and authentication information without requiring many disk I/O operations. In addition, solid-state devices will improve data access speed, and a responsive system is required to achieve a seamless user experience. From a software engineering point of view, the authentication process is implemented with a modular approach that separates concerns into the authentication logic, data management, and interaction layers. High-level programming languages such as Python enable rapid application development with sufficient performance for security applications. Backend application development with frameworks enables systematic request processing and session management with cryptographic services. Trustworthy database management systems are required to ensure the confidentiality and integrity of the authentication data.

V. RESULTS AND DISCUSSIONS

A user-centered two-factor authentication system that relies on customized image verification was developed and evaluated. The results show that the suggested solution improves authentication security without sacrificing usability or feasibility. This section highlights the performance and efficacy of the system's implementation and testing.

A. Authentication Success Performance

Table 2: Authentication Success Performance Analysis

Authentication Stage	Successful Attempts	Failure Attempts
Password Verification (Factor 1)	47	3
Image–Keyword Verification (Factor 2)	45	5
Final Access Granted	45	5

In order to determine how effectively the suggested two-factor authentication system performs, 50 routine authentications were conducted that presented in the Table 2. In the first phase of the experiment, the password verification phase achieved a score of 47 successful authentications and 3 failed attempts.

This indicates the primary method of authentication is still effective for authentic users. In the second phase of the experiment, where image-keyword verification is implemented as a second factor of authentication, the system achieved 45 successful authentications and 5 failed attempts, suggesting that a few users provided an inappropriate image or were confused about the keyword.

The system achieved 45 successful authentications out of 50 attempts, and therefore the success rate is as follows:

$$\text{Success Rate} = \frac{45}{50} \times 100 = 90\%$$

These findings demonstrate that incorporating image-based authentication adds another layer of security without sacrificing usability. In addition to highlighting the significance of user familiarity with certain image–keyword pairs, the small failures seen in the second step also show how successful the system is at preventing unauthorized access when wrong verification inputs are supplied.

B. Attack Resistance Results

Table 3: Attack Resistance Performance Analysis of Brute-force Attempt Blocking

Scenario	Result
Max allowed attempts (unknown device)	3
Account temporarily locked after	3 failures
Unauthorized access success	0%

By continuously trying to log in using the wrong credentials from an unidentified device, a brute-force resistance test was carried out. The account was automatically and temporarily locked after the system enforced a tight attempt threshold of three maximum failures. This resulted in a unauthorized access success rate of 0% since no unauthorized session was successfully established. By restricting repeated access attempts and stopping attackers from going above the predetermined threshold, this result validates that the device-based attempt limitation method is successful in thwarting automated password-guessing attacks. Blocking effectiveness:

$$\text{Blocking Efficiency} = \frac{Blocked\ Attempts}{Total\ Attack\ Attempts} \times 100 = 100\%$$

C. Login Time Measurement

Table 4: On Login Time Measurement Analysis

Authentication Method	Avg. Time Taken
Password-only login	1.8 seconds
Password + Image Verification	4.6 seconds

The login logs suggest that the addition of the personalized image verification takes a slight toll on the process. Password login takes approximately 1.8 seconds, while the combination of password and image verification takes about 4.6 seconds, an increase of about $\Delta T = 2.8$ seconds. This is expected, as the user must select an image, and the system must then compare the image to the keywords on the back end.

Despite this slight penalty, the login process remains well within the realm of usability. The user can log in quickly, and the slight penalty is well worth the added security provided by the second factor.

VI. CONCLUSION

The study has successfully demonstrated a user-centric two-factor authentication system, which improves the traditional user login process by adding an additional factor of authentication using image keyword-based authentication. This proposed system has effectively addressed the most commonly faced security attacks in password-based authentication systems, such as phishing, brute-force, and password misuse, in an efficient manner. This proposed system uses human vision memory instead of depending on any hardware or time-based passwords, thereby providing more convenience for the user to access their account without any hassle. This proposed system also uses device-based attempt limits to enhance security against unauthorized access attempts. From the experimental evaluation of the proposed system, it is clear that it ensures high authentication accuracy, blocks unauthorized access during brute-force attacks, and imposes a reasonable overhead on login time. Ultimately, this approach demonstrates a balanced solution between security and user experience in modern authentication.

REFERENCES

1. Allafi, R., & Darem, A. A. (2025). Usability and security in online authentication systems. *International Journal of Advanced and Applied Sciences, 12*(6), 1–12. https://doi.org/10.21833/ijaas.2025.06.001
2. Alotaibi, A. (2025). A review of the authentication techniques for Internet of Things in smart cities. *Sensors, 25*(6), 1649.
3. Andriotis, P., Kirby, M., & Takasu, A. (2023). Bu-Dash: A universal and dynamic graphical password scheme (extended version). *International Journal of Information Security, 22*(2), 381–401.
4. Anjaneyulu, P., Priyanka, D., Chalapathi, T., Samanvi, B., & Mounika, B. (2023). Image selection for graphical password authentication. In *Proceedings of the International Conference on Machine Learning and Big Data Analytics* (pp. 89–101). Springer.
5. Asif, M., Abrar, M., Salam, A., Amin, F., Ullah, F., Shah, S., & AlSalman, H. (2025). Intelligent two-phase dual authentication framework for Internet of Medical Things. *Scientific Reports, 15*, Article 1760. https://doi.org/10.1038/s41598-024-84713-5
6. Chihi, H., Chahboun, A., & Mezroui, S. (2025). Alternative of traditional password systems using enhanced visual cryptography. *Discover Computing, 28*(1), 287.
7. Dhinesh, M., Geetha, B., P., S., Saravanakumar, L., Jude, P. S. V., & Balaram, A. (2025). ImageGuard: Advanced user authentication via dynamic graphical password manipulation and secured image sequences. In *Proceedings of the 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 377–384). https://doi.org/10.1109/ICSADL65848.2025.10933219
8. Dias, N. I., Kumaresan, M. S., & Rajakumari, R. S. (2023). Deep learning based graphical password authentication approach against shoulder-surfing attacks. *Multiagent and Grid Systems, 19*(1), 99–115.
9. Ganmati, A., Afdel, K., & Koutti, L. (2025). Deep learning-based multi-factor authentication: A survey of biometric and smart card integration approaches. *arXiv*. https://arxiv.org/abs/2510.05163
10. Gilbert, C., & Gilbert, M. A. (2025). Continuous user authentication on mobile devices. *International Research Journal of Advanced Engineering and Science, 10*(1), 158–173.
11. Ibrahim, R. M. (2025). Enhancing multifactor authentication using machine learning techniques. *Mesopotamian Journal of CyberSecurity, 5*(2), 899–912.
12. Lengert, A. (2025). 2FA: Navigating the challenges and solutions for inclusive access. *arXiv*. https://arxiv.org/abs/2502.11737
13. Qin, X., Li, W., & Rosenberg, P. (2025). RoundImage: Towards secure graphical password authentication via rounded image selection in IoT. *IEEE Internet of Things Journal*.
14. Ramcharan, H. (2025). The effective integration of multi-factor authentication (MFA) with zero trust security. *American Journal of Mathematical and Computational Modeling, 10*(1), 1–5. https://doi.org/10.11648/j.ajmcm.20251001.11

15. Ray, P., Giri, D., Meng, W., & Hore, S. (2024). GPOD: An efficient and secure graphical password authentication system by fast object detection. *Multimedia Tools and Applications, 83*(19), 56569–56618.
16. Ray, P., Giri, D., Obaidat, M. S., Jana, M., Sasmal, M., & Alenazi, M. J. F. (2025). GPNST: An improved graphical password authentication scheme leveraging neural style transfer technique on smartphones. *International Journal of Information Security, 24*(3)*, Article 138.
17. Rasheed, A. F., Zarkoosh, M., & Elia, F. R. (2024). Enhancing graphical password authentication system with deep learning-based Arabic digit recognition. *International Journal of Information Technology, 16*(3), 1419–1427.
18. Suru, H. U. (2024). Improving the usability of graphical authentication systems using subject-based images.
19. Tran-Truong, P. T., Pham, M. Q., Son, H. X., et al. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of Systems Architecture, 162*, 103402.
20. Zeeshan, N. (2025). Continuous authentication in resource-constrained environments. *Sensors, 25*(18), 5711.
21. Ahmed, S. T., Fathima, A. S., Mathivanan, S. K., Jayagopal, P., Saif, A., Gupta, S. K., & Sinha, G. (2024). iLIAC: An approach of identifying dissimilar groups on unstructured numerical image dataset using improved agglomerative clustering technique. *Multimedia Tools and Applications*, *83*(39), 86359-86381.
22. Fathima, S. N., Rekha, K. B., Safinaz, S., & Ahmed, S. T. (2024). Computational techniques, classification, datasets review and way forward with modern analysis of epileptic seizure–a study. *Multimedia Tools and Applications*, *83*(38), 85685-85701.
23. Khan, S. B., Tikotikar, A., DR, K. R., Ahmed, S. T., Albalawi, E., Qusaim, T., & Basheer, S. (2025). Telemedicine via Edge-Cloud Healthcare: A Federated Semi Supervised Learning Resource Recommendation Approach towards Building Sustainable Framework. *IEEE Transactions on Consumer Electronics*.