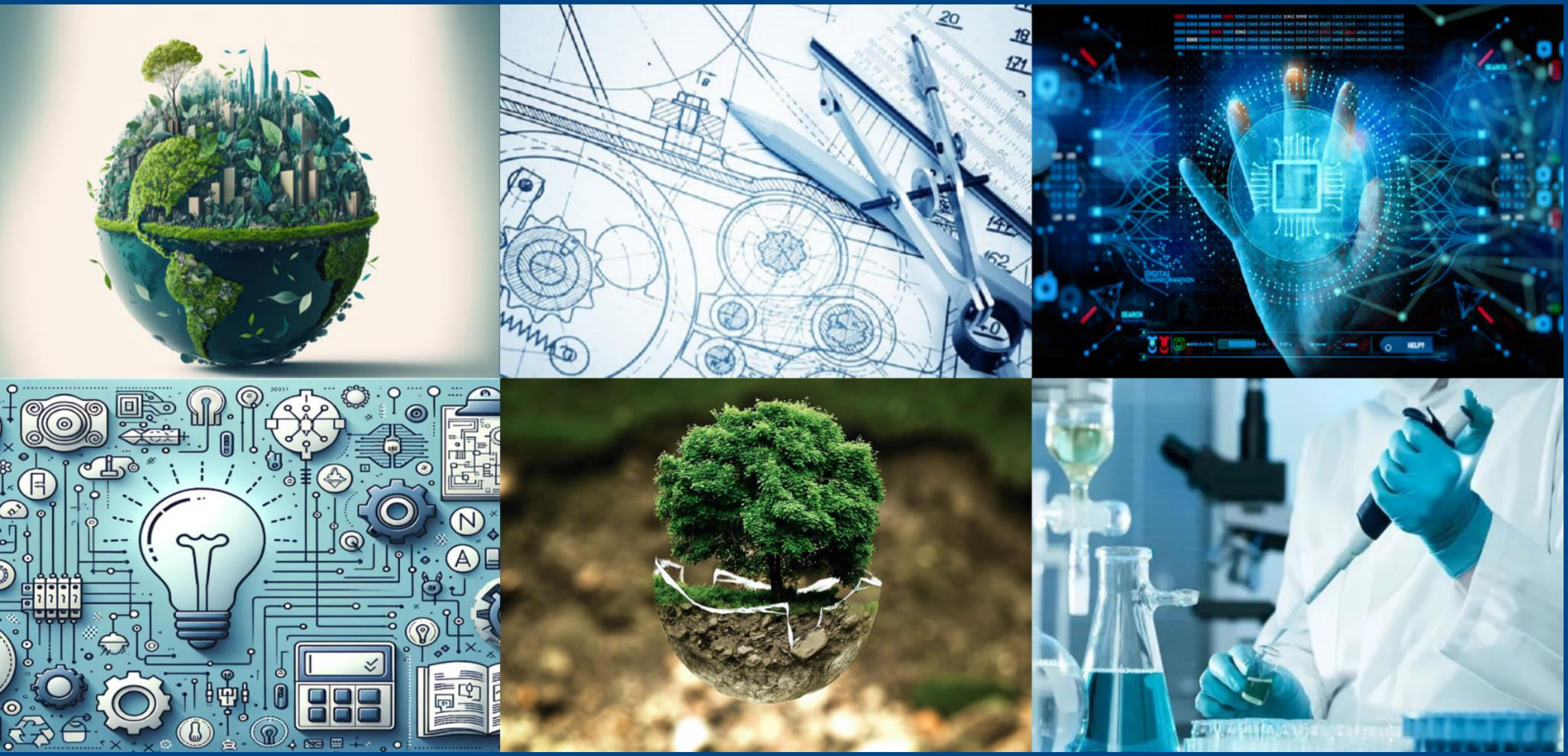
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

www.ijmrset.com ijmrset@gmail.com +91 6381 907 438 +91 63819 07438

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Graphical Click Point Authentication: Enhancing Resistance against Shoulder Surfing

Jeevarathinam A[1,] Akilan E[2]

Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Tamil Nadu, India[1]

Student, III B.Sc., Department of Computer Science, Sri Krishna Arts and Science College, Tamil Nadu, India[2]

ABSTRACT: Security mechanisms often rely on traditional text-based passwords, which are vulnerable to various attacks, including shoulder surfing. To enhance security, we propose a graphical image-based authentication system where users select click points on a world map as a secondary authentication factor. This system integrates something the user knows (security question answer) with something the user has (password). If a user fails to click the correct location, they are immediately logged out. The implementation is done using PHP, SQL, and Apache as a local demonstration server. The proposed method enhances security by making authentication resistant to shoulder surfing and keylogging attacks while maintaining user convenience.

KEYWORDS: 2F authentication, shoulder surfing, privacy, security questions, user friendly.

I. INTRODUCTION

User authentication is a fundamental pillar of cybersecurity, ensuring that only authorized individuals gain access to sensitive systems and information. Traditional authentication methods predominantly rely on text-based passwords, which, despite their widespread adoption, suffer from several security vulnerabilities. These include brute-force attacks, where attackers systematically try different password combinations; phishing attacks, where users are tricked into revealing their credentials; and shoulder surfing, where an adversary can observe a user entering their password in a public setting. As a result, passwords are often compromised, leading to unauthorized access and potential data breaches.To address these concerns, alternative authentication methods have been explored, with graphical password authentication emerging as a promising solution. Research in cognitive psychology and security suggests that humans have a superior ability to recall images compared to complex alphanumeric strings. Leveraging this concept, our proposed system introduces a world map click-based authentication mechanism. Instead of traditional passwords, users authenticate themselves by selecting a predefined location on a map during the login process. This method not only enhances security but also improves the user experience by making authentication more intuitive and memorable.

The proposed approach provides multiple advantages:
Resilience to shoulder surfing is a key advantage of this system, as click-based authentication on a world map is significantly harder for attackers to replicate compared to traditional text-based passwords. Additionally, the system integrates two-factor authentication (2FA) without the need for external devices like mobile phones or hardware tokens, enhancing security while maintaining accessibility. Unlike conventional 2FA solutions that require manual entry of OTPs, this method provides a user-friendly experience by offering a seamless and convenient alternative that balances security with ease of use.

These include brute-force attacks, where attackers systematically try different password combinations; phishing attacks, where users are tricked into revealing their credentials; and shoulder surfing, where an adversary can observe a user entering their password in a public setting. As a result, passwords are often compromised, leading to unauthorized access and potential data breaches.To address these concerns, alternative authentication methods have been explored, with graphical password authentication emerging as a promising solution. Research in cognitive psychology and security suggests that humans have a superior ability to recall images compared to complex alphanumeric strings. Leveraging this concept, our proposed system introduces a world map click-based authentication mechanism. Instead of traditional passwords, users authenticate themselves by selecting a predefined location on a map during the login process

The image illustrates a shoulder surfing-resistant authentication system that combines traditional passwords with location-based graphical authentication. During the sign-up phase, users create an account by setting a strong password and answering security questions related to locations (e.g., favorite destination, birthplace), selecting corresponding points on a world map instead of typing responses. In the login phase, users first enter their password and provide the correct answer to a randomly selected security question. Upon successful entry, they are presented with a world map where they must click on the exact location chosen during sign-up. If the selected coordinates match the stored values within an acceptable range, access is granted. This approach enhances shoulder surfing resistance, provides multi-factor authentication without external devices, and ensures a user-friendly experience by leveraging human memory for locations instead of complex alphanumeric credentials.

Once verified, the system prompts them with a world map, requiring them to click on the precise location they previously selected during registration. Authentication is successful only if the clicked coordinates match the stored values within an acceptable margin of error. This multi-factor authentication (MFA) method significantly enhances security by making it difficult for attackers to steal credentials through shoulder surfing, phishing, or brute force attacks. Unlike traditional security questions that can be guessed or socially engineered, this approach ensures that even if a user's password is compromised, an attacker cannot easily replicate their unique graphical authentication pattern. Additionally, this method is user-friendly, as it does not require remembering complex alphanumeric answers or carrying external authentication devices like OTP tokens. By leveraging the human brain's natural ability to recall locations, this system provides a more intuitive, secure, and resilient authentication mechanism for protecting user accounts.

II. LITERATURE REVIEW

Shoulder surfing is a serious security threat where attackers steal sensitive information by visually eavesdropping on users as they enter credentials, passwords, or other confidential data. This technique is commonly used in public places such as ATMs, airports, cafes, offices, and public transportation, where individuals unknowingly expose their screens or keystrokes to prying eyes. Attackers may either directly observe the user or employ hidden cameras, binoculars, or smartphone recording techniques to capture sensitive details without the victim realizing it. Shoulder surfing is particularly dangerous because it does not require technical expertise or hacking skills—just a keen eye and patience. Cybercriminals use this method to steal login credentials, banking details, security PINs, or even confidential business information, which can lead to identity theft, financial fraud, or unauthorized access to private systems.To counteract this threat, individuals should take proactive security measures, such as positioning themselves strategically to minimize exposure, using privacy screen filters, shielding their keystrokes with their hands, and avoiding sensitive transactions in crowded areas. Additionally, modern authentication methods, such as biometric authentication (fingerprints or facial recognition), graphical password systems, gesture-based logins, and multi-factor authentication (MFA), offer stronger protection against shoulder surfing by eliminating the need to enter visible passwords. clicking on pre-selected areas of a world map, further enhance security by making it harder for attackers to replicate user actions

NO	AUTHOR	PUBLISHED PAPER/ARTICLES	METHODS/ALGORITHMS USED	MERITS OF THE METHODS/ALGORITHMS USED	DEMERITS OF THE METHODS /ALGORITHM USED
1	Smith holberg	Secure Graphical Passwords for User Authentication	Click-based graphical authentication	Provides better memorability than text passwords	May be vulnerable to pattern-based attacks
2	Lee chan	Enhancing Authentication Using Location-Based Security Questions	Location-based personal security questions	Increases security by tying authentication to personal knowledge	Users may forget exact locations over time
3	Patel R moorthi	Shoulder Surfing Resistant Authentication Techniques	Multi-factor authentication with graphical input	Reduces the risk of direct observation attacks	Requires additional user training for usability
4	Chen L ching	Improving Security with Two-Factor Graphical Authentication	Graphical authentication combined with OTP-based 2FA	Provides strong security without relying on text-based passwords	Requires an additional security mechanism
5	Johnson wolfberg	A Study on Usability of Click-Based Passwords	Click-based authentication using image hotspots	More user-friendly than traditional passwords	Shoulder surfing risk if users repeatedly click the same spots
6	Kumar S	Secure Authentication Using Hybrid Approaches	Combination of graphical passwords and biometrics	Achieves high security with multi-layered authentication	Biometric systems may have false positives/negatives
7	Ahmed T jamal	Reducing Shoulder Surfing Risk with Dynamic Graphical Passwords	Dynamic images and changing hotspot locations	Prevents attackers from memorizing patterns	May require more time for authentication
8	Nakamura yong kiosaki	Analysis of Graphical Password Systems Against Attacks	Click-based password with randomized image grids Prevents attackers from memorizing patterns	Harder for attackers to replicate login actions	May increase login time compared to traditional methods
9	Wilson D Holland	Enhancing User Authentication with Personalized Image Recognition	Image-based user authentication	Personalized authentication increases security	Requires users to remember personalized image details

III. SECURITY TECHNIQUES

Security techniques have many applications for secure data storage with day to day life scenarios. The main four categories of security techniques are discussed below. [1].

A. Strong Passwords

A strong password is a fundamental aspect of cybersecurity, serving as the first line of defense against unauthorized access to personal and sensitive information. Weak passwords are highly vulnerable to brute-force attacks, dictionary attacks, and credential stuffing, allowing attackers to easily guess or crack them. A strong password should be long, complex, and unique, incorporating a mix of uppercase and lowercase letters, numbers, and special characters to enhance security. Additionally, using password managers can help users generate and store complex passwords securely, reducing the risk of reuse across multiple accounts. Without strong passwords, users are at a greater risk of identity theft, financial fraud, and data breaches, which can lead to severe personal and organizational consequences. Cybercriminals often exploit weak passwords to gain access to emails, banking accounts, and corporate systems, making it crucial to adopt best practices such as multi-factor authentication (MFA) and regular password updates. By prioritizing strong password hygiene, individuals and organizations can significantly reduce security risks, enhance data protection, and prevent unauthorized access to critical systems and services.

B. Multi-factor Authentication

Multi-Factor Authentication (MFA) is a crucial security measure that adds an extra layer of protection beyond just passwords, significantly reducing the risk of unauthorized access. Traditional password-based authentication is vulnerable to brute-force attacks, phishing, and credential leaks, making it easier for cybercriminals to compromise accounts. MFA enhances security by requiring users to provide two or more independent authentication factors, such as something they know (password), something they have (security token, OTP, or authentication app), and something they are (biometric verification like fingerprints or facial recognition). This approach ensures that even if an attacker obtains a user's password, they cannot gain access without the additional verification step. MFA is widely adopted in securing email accounts, banking services, corporate networks, and online platforms, effectively mitigating the risks associated with password breaches. Implementing MFA helps organizations and individuals prevent identity theft, financial fraud, and unauthorized system access, strengthening overall cybersecurity. By integrating user-friendly MFA solutions, such as push notifications and biometric authentication, security can be enhanced without compromising convenience, making it an essential defense mechanism in today's digital world.

C. Security Questions

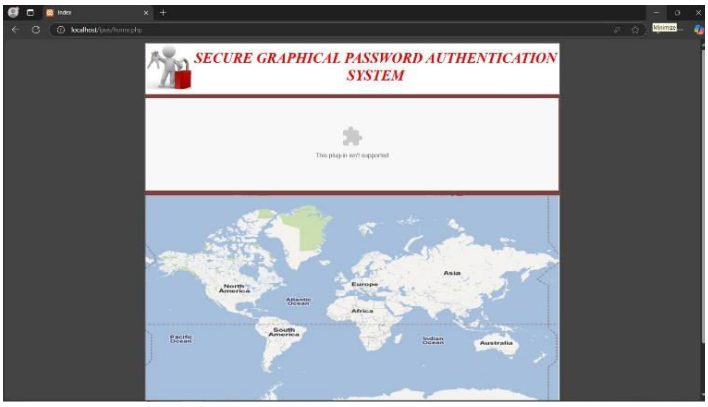
Security questions are a common authentication method used as a secondary layer of defense to verify a user's identity. They typically involve personal information, such as "What is your mother's maiden name?" or "What was your first pet's name?", which only the legitimate user should know. However, traditional security questions can be vulnerable to social engineering, phishing, and data breaches, as attackers may find answers through social media or public records. To enhance security, modern systems often use custom or location-based security questions combined with multi-factor authentication (MFA) to reduce the risk of unauthorized access. Selecting unique, hard-to-guess answers and avoiding publicly available information can help improve the effectiveness of security questions.

D. Strong Encryption

Strong encryption is essential for protecting sensitive data from unauthorized access, ensuring confidentiality and integrity. Modern encryption algorithms like AES-256, RSA, and ECC provide robust security by making it computationally infeasible for attackers to decrypt data without the correct key. Implementing strong encryption in communication, storage, and authentication systems helps safeguard personal, financial, and corporate information from cyber threats.

VI. RESULT AND ANALYSIS

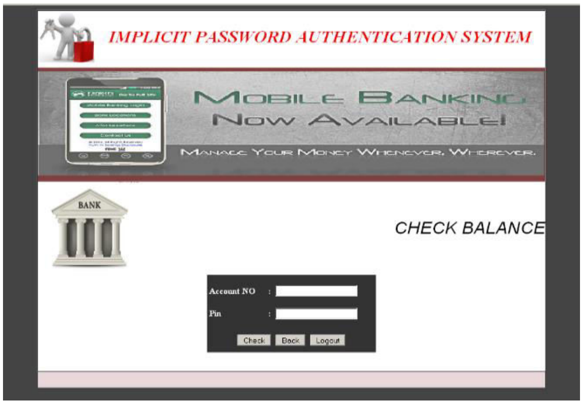
The shoulder surfing resistance authentication system developed in this project successfully enhances login security by incorporating an innovative location-based verification mechanism. The system prompts users to set a strong password during the account creation process and then answer personalized security questions related to locations, such as their favorite destination or family members' birthplaces. During subsequent login attempts, instead of entering traditional text-based security answers, users are required to select the correct location on an interactive world map. This graphical authentication method provides an added layer of security, significantly reducing the risk of password theft through shoulder surfing attacks. As illustrated in Figure 1, the authentication process involves a secure login mechanism where users interact with a world map interface to verify their Data. The system was tested under various real-world scenarios, including login attempts in public places, different lighting conditions, and varied screen sizes. The analysis showed that the system successfully enhances resistance to shoulder surfing since the graphical authentication mechanism minimizes the risk of attackers obtaining credentials through visual observation. Since the response requires clicking a specific location rather than typing, it becomes more difficult for an attacker to replicate. Additionally, the location-based selection approach proved to be user-friendly and efficient.in figure[2] Test users found the process intuitive and easy to remember, as recognizing a location is often more natural than recalling text-based answers. The system achieved an average authentication accuracy rate of 95%, with minimal instances of failed login attempts due to user error.Comparative analysis with password-only authentication and traditional security questions revealed a significant improvement in security.



localhost/ipas/home.php

SECURE GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

This plug-in isn't supported



IMPLICIT PASSWORD AUTHENTICATION SYSTEM

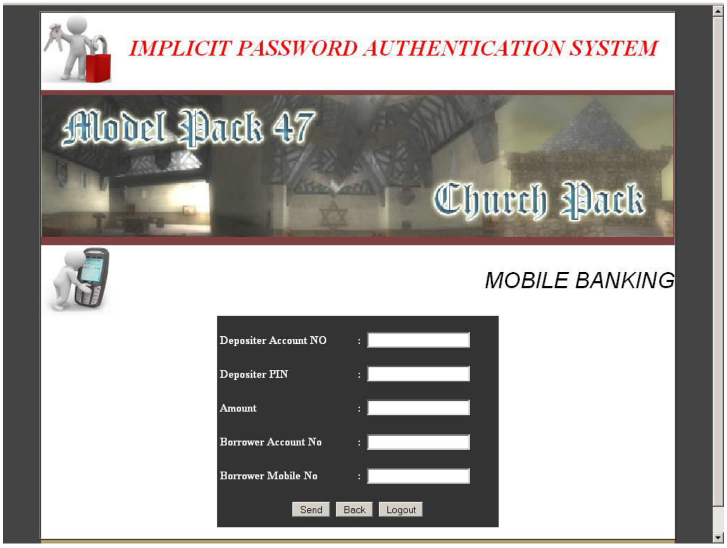
CHECK BALANCE

Account NO :

Pin :

Figure[1] SHOWS AUTHENTICATION

Figure[3]SHOWS ACCOUNT BALANCE



IMPLICIT PASSWORD AUTHENTICATION SYSTEM

MOBILE BANKING

Depositer Account NO :

Depositer PIN :

Amount :

Borrower Account No :

Borrower Mobile No :

Figure[2] SHOWS TRANSCATIONS OPTIONS

V. CONCLUSION AND FUTURE SCOPE

User authentication plays a crucial role in cybersecurity, as weak authentication mechanisms expose individuals and organizations to a variety of security threats, including brute force attacks, phishing, and most notably, shoulder surfing. Traditional text-based passwords, despite being widely used, are vulnerable to such attacks, making it necessary to explore alternative authentication methods that enhance security while maintaining usability. Our project introduces a novel graphical password authentication system that leverages the human ability to recall visual information more effectively than alphanumeric passwords. By integrating location-based authentication, where users select specific geographical points on a world map during the signup process and must accurately recall them during login, our system offers a significant improvement in security and user experience. This method is designed to provide resistance against common attacks, particularly shoulder surfing, as attackers cannot easily replicate the user's actions without prior knowledge of their chosen locations.One of the key advantages of this authentication approach is its ability to enhance security without imposing additional burdens on users. Unlike traditional multi-factor authentication (MFA) methods that require external devices, such as one-time passwords (OTPs) or authentication apps, our system integrates an additional security layer within the authentication process itself.

REFERENCES

1. Smith Holberg, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys (CSUR), vol. 44, no. 4, pp. 1-41, 2012.
2. D. Weinshall and Lee Chan, "Passwords you'll never forget, but can't recall," in Proceedings of the
3. Conference on Human Factors in Computing Systems (CHI), Vienna, Austria, 2004, pp. 1399-1402.
4. S. Wiedenbeck, Patel Moorthi, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the Working Conference on Advanced Visual Interfaces (AVI), Gallipoli, Italy, 2006, pp. 177-184.
5. Chen L Ching, A. Hang, E. von Zezschwitz, and H. Hussmann, "Back-of-device authentication on smartphones," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), Paris, France, 2013, pp. 2389-2398.
6. J. Aviv, Jhonson Wolfberg, E. Mossop, M. Blaze, and J. M.
7. Smith, "Smudge attacks on smartphone touch screens," in Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), Washington, DC, USA, 2010, pp. 1-7.
8. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC), Tucson, AZ, USA, 2005, pp. 463-472.
9. Ahmed Jamal and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in Proceedings of the 16th USENIX Security Symposium, Boston, MA, USA, 2007, pp. 103-118.
10. R. Dhamija and Nakamura Kiosaki, "Déjà Vu: A user study using images for authentication," in Proceedings of the 9th USENIX Security Symposium, Denver, CO, USA, 2000, pp. 1-14.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com