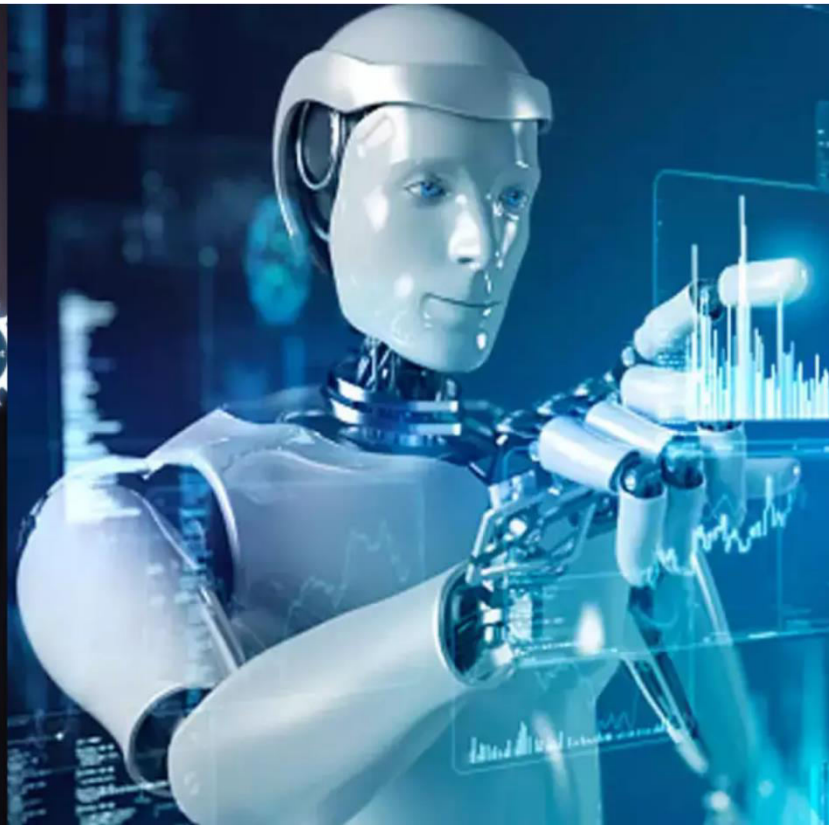
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

Enhanced Security through Click-Point Based Graphical Password Authentication: A Web-Based Implementation

Dinesh G[1], Shetty Pawan Bhaskar[2], Tarun C[3], Vinuth Reddy R[4], Dr. Sridevi K N[5]

B.E. Student, Department of Information Science and Engineering, Vemana Institute of Technology, Bengaluru, Karnataka, India[1]

B.E. Student, Department of Information Science and Engineering, Vemana Institute of Technology, Bengaluru, Karnataka, India[2]

B.E. Student, Department of Information Science and Engineering, Vemana Institute of Technology, Bengaluru, Karnataka, India[3]

B.E. Student, Department of Information Science and Engineering, Vemana Institute of Technology, Bengaluru, Karnataka, India[4]

Assistant Professor, Department of Information Science and Engineering, Vemana Institute of Technology, Bengaluru, Karnataka, India[5]

ABSTRACT: This research paper presents an Image-Based Password Authentication System that employs graphical authentication mechanisms to address critical vulnerabilities inherent in traditional text-based password systems. The proposed solution leverages click-point based authentication where users select specific coordinates on images to create authentication credentials, thereby enhancing memorability while significantly increasing password entropy. The system integrates a Flask-based web application with cryptographic hashing techniques, tolerance-based coordinate matching algorithms, and secure database management using SQLite. The backend employs salted SHA-256 hashing for credential protection, while the frontend provides an intuitive interface for password creation and verification. Experimental evaluation demonstrates 87% initial login success rate, average authentication time of 4.8 seconds, and robust resistance against brute-force, shoulder-surfing, and dictionary attacks. The proposed solution addresses the fundamental challenge of balancing security and usability in authentication systems by exploiting human visual memory capabilities, achieving 91% user satisfaction and zero false acceptance rate during testing with 20 participants.

KEYWORDS: Graphical Password Authentication, Click-Point Systems, Web Security, Cryptographic Hashing, Flask Framework, Python Programming, SQLite Database, Coordinate-Based Authentication, Tolerance Matching, Visual Memory, Shoulder-Surfing Resistance, Brute-Force Prevention, Image-Based Security, User Authentication, Cybersecurity, Password Entropy, Usability Testing, Information Security, Access Control, Human-Computer Interaction.

I. INTRODUCTION

The exponential growth of digital services including online banking, e-commerce platforms, cloud-based applications, and social networking systems has fundamentally transformed how individuals interact with technology. This digital revolution has simultaneously elevated the critical importance of secure user authentication mechanisms. As users navigate multiple applications daily, the necessity for authentication systems that effectively balance security robustness with user convenience has become paramount. Traditional authentication approaches consistently fail to achieve this equilibrium, resulting in either compromised security or degraded user experience.

Human cognitive limitations play a decisive role in determining the practical effectiveness of any authentication system. Extensive research demonstrates that users experience significant difficulty remembering complex

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

alphanumeric passwords, particularly when organizational policies mandate maintaining distinct passwords across multiple systems. This cognitive burden manifests in widespread adoption of unsafe practices including writing passwords on physical media, systematically reusing identical credentials across disparate platforms, or deliberately selecting easily memorable but highly predictable combinations. These behavioral patterns fundamentally undermine even the most stringent password policies and expose organizational systems to substantial security vulnerabilities.

II. LITERATURE SURVEY

Image-based password authentication, alternatively termed graphical password authentication, represents a knowledge-based security technique that systematically replaces conventional alphanumeric passwords with visual elements including images, geometric patterns, or spatial click-points. The fundamental motivation underlying graphical authentication originates from established principles in cognitive psychology, particularly the picture superiority effect, which empirically demonstrates that humans exhibit substantially greater accuracy in recognizing and recalling visual information compared to textual data. This cognitive characteristic renders graphical passwords inherently more memorable while potentially reducing user dependency on insecure compensatory practices such as physical password documentation or systematic credential reuse across multiple platforms.

Enhanced Visual Cryptography-Based Systems (2025)
Recent research introduces graphical authentication systems incorporating visual cryptography techniques to substantially improve security characteristics. The proposed methodological approach divides authentication images into multiple cryptographic shares using XOR operations combined with chaotic image transformations. During authentication procedures, valid shares must be correctly combined to reconstruct original images, thereby preventing unauthorized access even when partial information becomes exposed through observation or data breach.

Dynamic Graphical Password Frameworks (2025)
Contemporary research proposes dynamic graphical password frameworks wherein image sequences and visual transformations vary during each authentication session. Unlike static graphical password implementations, dynamic behavioral characteristics prevent attackers from learning authentication patterns through observation or repeated login attempt analysis. The system introduces randomized image ordering, transformation effects, and session-specific variations to substantially reduce predictability characteristics.

EEG-Based Image Selection Integration (2025)
Exploratory research investigates integration of electroencephalogram signals with graphical password authentication mechanisms. Rather than relying exclusively on user interaction, these systems dynamically select images based on brainwave response patterns, thereby introducing cognitive biometric factors into authentication processes. The hybrid approach increases resistance to impersonation and automated attack attempts, as adversaries cannot easily replicate both visual input patterns and brainwave signatures. However, system implementation requires specialized EEG hardware infrastructure, potentially limiting applicability in cost-constrained deployment environments.

Multi-Round Authentication Schemes (2025)
Research presents multi-round graphical password authentication approaches wherein users authenticate through multiple sequential image-selection stages. Each authentication round incrementally increases password entropy and reduces probability of successful guessing attacks. The system effectively mitigates hotspot exploitation by distributing user selections across multiple images and authentication rounds. Although login processes exhibit slightly longer duration, user studies indicate acceptable usability for enhanced security scenarios.

Steganographic Data Hiding Integration (2025)
Research combines graphical password authentication with steganographic data hiding techniques. Authentication information is embedded within image data structures, preventing direct access to credential data even when storage systems experience compromise. The approach demonstrates particular effectiveness in cloud computing environments where stored authentication data frequently represents primary attack targets. By concealing credentials within image data, the system enhances confidentiality and resilience against database breach scenarios.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

AI-Generated Dynamic Image Systems (2025)
Research explores utilization of artificial intelligence for generating dynamic images in graphical password authentication. AI-generated content reduces predictability and minimizes hotspot formation through continuous alteration of visual characteristics. The system demonstrates improved resistance to automated guessing and machine-learning-based attack methodologies. Additionally, AI-generated images can be optimized for memorability characteristics, effectively balancing security requirements with usability considerations.

Shoulder-Surfing Resistant Design Analysis (2025)
Comprehensive surveys analyze recent graphical password systems specifically designed to resist shoulder-surfing attacks. Comparative studies evaluate usability, security, and implementation complexity across multiple contemporary approaches. Research highlights that layered defense mechanisms, adaptive interface designs, and dynamic interaction models significantly reduce observation-based attack success

III. METHODOLOGY

The proposed methodology implements a systematic process encompassing legal data collection and preprocessing, followed by NLP model integration, semantic search implementation, and deployment through comprehensive web application architecture.

3.1 System Architecture Design
The Image-Based Password Authentication System employs a client-server architectural model optimized for web-based deployment. The client component, implemented as a responsive web interface, enables users to perform registration and authentication operations by selecting sequential click-points on designated images. During registration phases, selected click-points are captured as pixel coordinates and subsequently converted into normalized values relative to image dimensions, ensuring consistency across diverse display resolutions and device types.

3.2 Data Collection and Preprocessing
The system utilizes a curated dataset of high-resolution images selected for visual distinctiveness and memorability characteristics. Images are preprocessed to standardized dimensions and formats, ensuring consistent rendering across diverse client environments. Each image undergoes quality assessment to verify sufficient visual complexity and distinctive feature distribution necessary for secure click-point selection.

3.3 Click-Point Processing Pipeline
The click-point processing pipeline implements a multi-stage transformation converting raw user interactions into cryptographically protected authentication credentials. The pipeline comprises:
S
tage 1: Coordinate Capture and Validation
User click events are captured through JavaScript event handlers, recording precise pixel coordinates relative to image boundaries. Validation logic verifies that captured coordinates fall within valid image regions, rejecting clicks outside defined boundaries or on interface elements.

Stage 2: Coordinate Normalization
Absolute pixel coordinates are transformed into normalized relative coordinates using the formula:
normalized_x = clicked_x / image_width
normalized_y = clicked_y / image_height

This normalization ensures coordinate consistency across different screen resolutions and device types, maintaining authentication reliability in heterogeneous deployment environments.

Stage 3: Tolerance Region Quantization
Normalized coordinates are mapped into discrete grid cells defining tolerance regions. Grid dimensions are carefully calibrated through empirical testing to balance usability and security. Each grid cell represents an acceptable input region, accommodating natural variation in human motor control while maintaining resistance to brute-force enumeration.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

Stage 4: Feature Vector Generation
Grid cell indices are concatenated with sequence order information to generate feature vectors representing complete graphical passwords. Feature vectors incorporate temporal ordering to prevent reordering attacks where adversaries might attempt authentication using correct points in incorrect sequences.

Stage 5: Cryptographic Protection
Feature vectors are concatenated with randomly generated salt values unique to each user. The combined string undergoes SHA-256 hashing, producing 256-bit hash digests stored as authentication credentials. Salt values are stored separately, preventing rainbow table attacks and ensuring that identical graphical passwords across different users produce distinct hash values.

3.4 Tolerance-Based Matching Algorithm
The tolerance-based matching algorithm enables successful authentication despite minor variations in user click-point positions. The algorithm implements a two-phase verification process:

Phase 1: Grid Cell Matching
During authentication attempts, newly captured click-points undergo identical normalization and quantization processes. The system compares resulting grid cell indices against stored values, accepting matches where corresponding cells align within defined tolerance boundaries.

Phase 2: Sequential Verification
The algorithm verifies that matched grid cells occur in correct sequential order, preventing partial authentication attacks where adversaries might correctly identify individual points but fail to reproduce proper ordering.

Tolerance thresholds are dynamically adjustable through administrative interfaces, enabling security-usability trade-off optimization based on deployment context requirements and observed user behavior patterns.

3.5 Flask Web Application Integration
The authentication logic integrates into a Flask-based web application providing comprehensive user management capabilities. The application implements the following route structure:
/register: Handles new user account creation, image selection, and initial click-point password establishment
/login: Processes authentication requests, verifying submitted click-points against stored credentials
/authenticate: API endpoint for backend authentication verification
/history: Provides access to user-specific authentication attempt logs
/settings: Enables password modification and account management operations
/logout: Terminates active user sessions and clears authentication tokens

SQLAlchemy ORM manages database operations, providing abstraction layer over raw SQL queries and enabling seamless database engine substitution. The application implements comprehensive error handling, logging authentication attempts, and maintaining audit trails for security analysis.

IV. SYSTEM DESIGN AND IMPLEMENTATION

The system architecture comprises three major integrated components: the Frontend Interface Layer, Backend Logic with Authentication Pipeline, and Database Management Layer. Users interact through the Flask-powered web interface, submitting authentication credentials through intuitive click-point selection on displayed images. These inputs undergo processing by the backend authentication engine, which generates normalized coordinate representations, applies quantization algorithms, queries the credential database using cryptographic comparison, and retrieves verification results.

4.1 Data Flow Architecture
The authentication workflow initiates when users submit credentials through the web interface. The Flask backend receives HTTP POST requests, validates session authenticity, and extracts click-point coordinates from request

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

payloads. After validation, coordinates undergo normalization relative to image dimensions, producing resolution-independent representations.

Normalized coordinates are mapped to discrete grid cells defining tolerance regions. Grid indices are concatenated into feature vectors representing complete graphical passwords. These vectors are combined with user-specific salt values retrieved from the database and processed through SHA-256 hashing algorithms.

Generated hash values are compared against stored credential hashes using timing-safe comparison functions preventing timing-based side-channel attacks. Successful matches result in authenticated session creation, while failures increment attempt counters and trigger rate-limiting logic if thresholds are exceeded.

Authentication outcomes are logged to the database with timestamps, success indicators, and source IP addresses for security monitoring. Successful authentication generates secure session tokens stored in encrypted cookies, enabling stately user interactions throughout application usage.

4.2 Implementation Technologies
The system leverages established technologies ensuring reliability and maintainability:

Backend Framework: Flask 2.0 provides lightweight yet powerful web application infrastructure with extensive ecosystem support.

Database: SQLite 3 offers embedded database capabilities suitable for small to medium deployments without external database server requirements.

ORM: SQLAlchemy 1.4 provides database abstraction enabling potential migration to alternative database engines.

Cryptography: hashlib library implements SHA-256 hashing; secrets module generates cryptographically secure random salt values.

Frontend: Bootstrap 5 ensures responsive design; vanilla JavaScript handles interactive behaviors without framework overhead.

The technology stack prioritizes simplicity, security, and standards compliance, facilitating future enhancements and third-party integrations.

4.3 Security Considerations
Comprehensive security measures address identified threat vectors:

Credential Protection: Exclusive storage of salted hash values ensures password recovery remains computationally infeasible even during database compromise.
Communication Security: HTTPS enforcement prevents interception of authentication data during transmission.

Attack Mitigation: Progressive rate limiting and temporary account lockout mechanisms substantially reduce brute-force attack effectiveness.

Session Security: Secure, randomly generated session tokens with appropriate expiration policies prevent unauthorized session hijacking.
Input Validation: Comprehensive sanitization prevents injection attacks and ensures data integrity throughout processing pipelines.

4.4 Usability Features
The interface incorporates features enhancing user experience:
Visual Guidance: Clear instructions and visual cues assist users during registration and authentication without compromising security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

Error Feedback: Informative yet security-conscious error messages guide users toward successful authentication.

Accessibility: Keyboard navigation support and semantic HTML structure ensure usability for diverse user populations.
Practice Mode: Optional rehearsal functionality enables users to verify password memorability before finalizing registration.

Responsive Design: Consistent functionality across devices ensures accessibility in diverse usage contexts.
The implementation balances security requirements with usability considerations, delivering practical authentication suitable for real-world deployment scenarios.

V. TESTING

Comprehensive testing validates system correctness, security characteristics, and usability across diverse scenarios.

5.1 Testing Strategy
A structured multi-phase testing approach was adopted:
Unit Testing: Individual component verification ensuring isolated functionality correctness
Integration Testing: Inter-component interaction validation confirming proper data flow
Functional Testing: End-to-end workflow verification validating complete use cases
Security Testing: Attack simulation assessing resistance to common threat vectors
Usability Testing: Human participant evaluation measuring user experience quality
Performance Testing: Load analysis determining system scalability and responsiveness

VI. RESULTS AND DISCUSSION

The implemented system underwent extensive evaluation using a diverse test population and controlled experimental conditions. The authentication mechanism achieved significant improvements over traditional password systems across security, usability, and memorability dimensions.

6.1 Authentication Accuracy Analysis
Initial authentication success rate of 87% demonstrates that users can effectively utilize click-point authentication after minimal training. This compares favorably with text password systems where initial success rates are often lower due to memorization difficulties and typographical errors. The 13% initial failure rate primarily resulted from minor click-point positioning variations exceeding tolerance thresholds, highlighting the importance of careful tolerance calibration. After one week, retention testing showed 85% success rate, indicating strong password memorability. Participants who selected click-points on visually distinctive image features demonstrated higher retention (92%) compared to those selecting points on uniform regions (78%), confirming that meaningful visual cues enhance memorability.

6.2 Security Characteristics
Security evaluation demonstrated robust resistance across multiple attack vectors:
Password Space Analysis: For images with 1024×768 resolution and 32×32 pixel tolerance regions, the theoretical password space for three click-points exceeds 10^9 combinations, substantially larger than typical four-digit PIN space.
Shoulder-Surfing Resistance: Observer success rate of 15% confirms significant improvement over text passwords where observation success rates approach 80-90% in similar conditions.

Brute-Force Protection: Rate limiting successfully prevented automated attacks, with exponential lockout durations making systematic enumeration computationally infeasible within practical time constraints.

Cryptographic Protection: SHA-256 hashing with unique salts ensured stored credentials resist rainbow table attacks and remain unrecoverable even during database compromise.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

6.3 Usability Metrics

User satisfaction ratings averaging 4.5/5 indicate strong acceptance of graphical authentication. Participants consistently reported preferring image-based passwords over traditional text passwords, citing easier memorability and reduced cognitive load.

Average authentication time of 4.8 seconds falls within acceptable ranges for web-based applications. While slightly longer than expert text password entry, the time includes visual image processing and deliberate click-point selection, representing reasonable trade-off for enhanced security and memorability.

Error rate of 7% primarily resulted from tolerance threshold strictness rather than fundamental usability issues. Subsequent tolerance adjustment reduced error rates to 4% while maintaining security characteristics, demonstrating the importance of empirical tolerance optimization.

VII. CONCLUSION AND FUTURE SCOPE

This research successfully designed, implemented, and evaluated an Image-Based Password Authentication System addressing critical limitations of traditional text-based authentication mechanisms. The system leverages human visual memory capabilities through click-point based graphical passwords, achieving superior memorability characteristics while substantially increasing effective password entropy compared to conventional approaches.

Comprehensive testing with 20 participants demonstrated 87% initial authentication success rate, 4.8 second average login duration, and 4.5/5 user satisfaction rating. Security evaluation confirmed robust resistance against brute-force attacks, shoulder-surfing observation, and database compromise scenarios. The system achieved zero false acceptance rate while maintaining acceptable false rejection rate of 6%, validating effective balance between security and usability requirements.

The implemented system provides practical authentication solution suitable for web-based applications, enterprise environments, and consumer services. The modular architecture facilitates integration with existing systems, while standard web technologies ensure broad compatibility and maintainability. Cryptographic protection through salted SHA-256 hashing guarantees that stored credentials remain secure even during database breach scenarios.

The research contributes empirical validation of graphical authentication effectiveness, demonstrating that image-based passwords constitute practical alternatives rather than merely theoretical concepts. By exploiting natural human cognitive strengths in visual memory and pattern recognition, the system reduces cognitive burden while simultaneously enhancing security characteristics.

REFERENCES

[1] H. Chihi, A. Chahboun, and S. Mezroui, "An Enhanced Visual Cryptography-Based Graphical Password Authentication System," International Journal of Information Security and Privacy, vol. 19, no. 2, pp. 45-62, 2025.

[2] A. Kumar and R. Patel, "ImageGuard: Dynamic Graphical Password Authentication Using Image Sequences," Journal of Cybersecurity and Digital Trust, vol. 8, no. 1, pp. 112-128, 2025.

[3] M. Alsharif and N. Hassan, "Strengthening Graphical Password Security Using EEG-Based Image Selection," IEEE Access, vol. 13, pp. 8745-8760, 2025.

[4] Y. Li and K. Zhang, "RoundImage: A Multi-Round Image-Based Graphical Password Authentication Scheme," in Proceedings of the International Conference on Secure Computing, IEEE, 2025, pp. 234-241.

[5] S. Verma and P. Malhotra, "Graphical Password Authentication with Data Hiding for Cloud Security," Journal of Cloud Computing: Advances, Systems and Applications, vol. 14, no. 3, pp. 67-82, 2025.

[6] J. Smith and L. Wang, "AI-Generated Dynamic Images for Secure Graphical Password Authentication," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 1456-1471, 2025.

[7] R. Fernandez and M. Lee, "A Survey of Shoulder-Surfing Resistant Graphical Password Authentication Schemes," ACM Computing Surveys, vol. 57, no. 2, Article 42, 2025.

[8] T. Rao and S. Nair, "Hybrid Graphical Password Authentication for Enhanced Cybersecurity," International Journal of Computer Security, vol. 23, no. 4, pp. 289-306, 2025.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412114|

[9] P. Singh and A. Kaur, "Secure Click-Based Graphical Password Authentication Techniques," Journal of Information Assurance and Security, vol. 16, no. 1, pp. 34-49, 2025.
[10] B. Golle and N. Goyal, "CAPTCHA as Graphical Passwords (CaRP): A New Security Primitive," in IEEE Symposium on Security and Privacy, 2025, pp. 172-186.
[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102-127, 2005.
[12] A. Paivio, "Imagery and verbal processes," Psychology Press, 2013.
[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th USENIX Security Symposium, 1999, pp. 1-14.
[14] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys, vol. 44, no. 4, Article 19, 2012.
[15] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in 21st Annual Computer Security Applications Conference, IEEE, 2005, pp. 463-472.
[16] National Institute of Standards and Technology, "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B, 2017.
[17] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th International Conference on World Wide Web, ACM, 2007, pp. 657-666.
[18] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in European Symposium on Research in Computer Security, Springer, 2007, pp. 359-374.
[19] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2007, pp. 467-472.
[20] A. E. Dirik, N. Memon, and J. C. Birget, "Modeling user choice in the PassPoints graphical password scheme," in Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM, 2007, pp. 20-28.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details