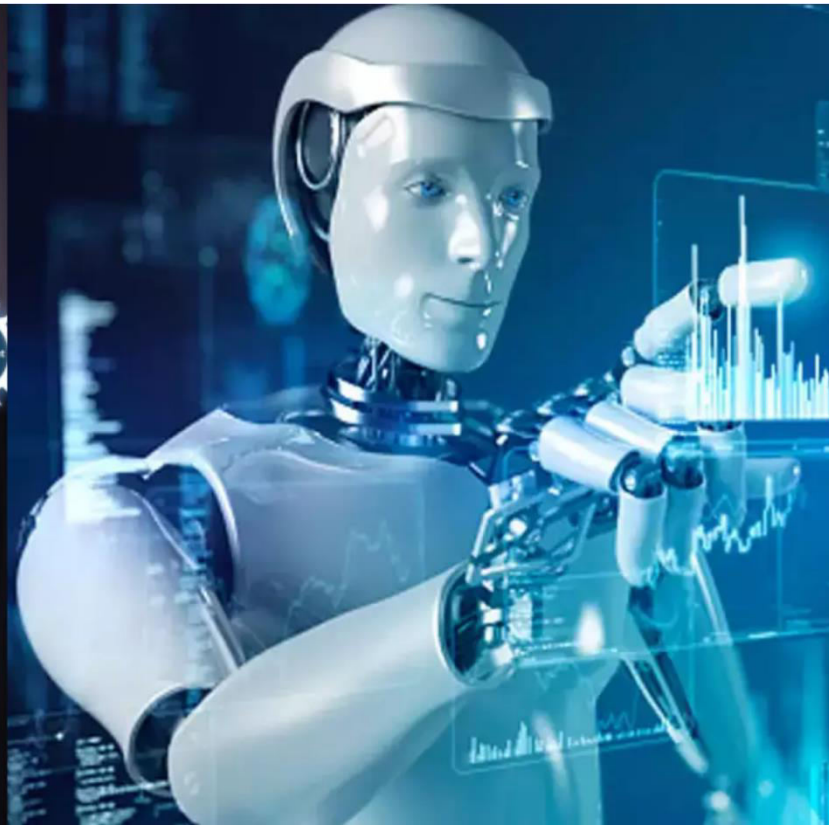
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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.2025.1412078|

Three-Phase user Verification Framework to Prevent Unauthorized access

Sahana K S, Ms Tejaswini A

P.G. Student, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

Assistant Professor, Department of Master of Computer Application, PES Institute of Technology and Management, Shivamogga, Karnataka, India

ABSTRACT: A Three-Level Password Authentication System enhances security by combining multiple layers of user verification to protect sensitive data and restrict unauthorized access. Traditional single-password mechanisms are vulnerable to attacks such as brute force, shoulder surfing, and password guessing. To address these limitations, the proposed system integrates three authentication levels: a textual password, a graphical or pattern-based password, and a cognitive or one-time dynamic password. The first level validates user credentials through a standard alphanumeric password. The second level adds robustness by using graphical selection or image-based authentication, making it difficult for intruders to replicate. The third level employs dynamic authentication—such as OTP generation, security questions, or system-generated challenges—to verify the user's identity even if the initial levels are compromised. This multi-layered approach significantly strengthens the authentication process by ensuring that breaching one level does not compromise the entire system. The proposed model offers improved reliability, enhanced security, and greater resistance to common cyber-attacks, making it suitable for applications requiring high levels of data protection.

I. INTRODUCTION

This document describes the design and implementation of a 3-Level Password Authentication System that adds a graphical password layer between a textual password and a one-time password (OTP) to increase the difficulty of unauthorized access. The goal is to create a practical, extensible MFA solution that can be integrated into web applications with minimal hardware or operational cost.

II. OBJECTIVES

- Develop a multi-factor authentication (MFA) system with three distinct security layers.
- Implement secure password storage using the bcrypt hashing algorithm.
- Design a graphical authentication layer based on click-point patterns with configurable tolerance.
- Integrate One-Time Password (OTP) generation and delivery (email) with expiry and single-use enforcement.
- Ensure session security (unique session identifiers, configurable lifetime, safe session teardown).
- Provide an intuitive user interface for smooth registration and three-step login.
- Maintain auditability for authentication events (OTP records, timestamps, used flags).
- Enforce brute-force protection via per-level attempt tracking and lockout.

III. LITERATURE SURVEY

Existing research on authentication systems highlights the limitations of traditional single-password mechanisms, which are frequently compromised through brute-force attacks, phishing, and shoulder surfing. To overcome these vulnerabilities, researchers have explored graphical passwords, pattern-based authentication, and multi-factor security models. Graphical password techniques—such as click-based and image-selection methods—offer improved memorability but remain susceptible to observation attacks. Pattern-based systems provide ease of use yet often reveal predictable user behavior. Meanwhile, dynamic authentication methods like One-Time Passwords (OTP) and security questions strengthen verification but may introduce usability challenges or depend heavily on secure delivery channels.

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.2025.1412078|

Literature consistently shows that combining independent security layers significantly enhances protection compared to using any single method alone. This has led to an increased focus on multi-level authentication frameworks, where knowledge-based, graphical, and dynamic factors are integrated to reduce the likelihood of unauthorized access. These studies collectively support the development of a three-level authentication system that balances security, usability, and resistance to common attack vectors.

IV. PROBLEM STATEMENT

In today's digital landscape, the frequency and sophistication of cyberattacks have increased significantly, making the protection of user accounts and sensitive information more challenging than ever. Traditional single-factor authentication systems—primarily username and password combinations—are no longer sufficient to safeguard users against modern threats. These systems are highly vulnerable to brute-force and dictionary attacks, credential stuffing, phishing attempts, social engineering, password reuse across platforms, and keylogging or shoulder-surfing techniques. As a result, attackers can often compromise accounts with minimal effort, especially when users rely on weak or repeated passwords. While Two-Factor Authentication (2FA), such as SMS or email-based OTPs, provides an additional security layer, it also introduces new challenges.

V. EXPERIMENTAL RESULTS

Authentication mechanisms in widespread use today fall into several families, each with strengths and limitations. Text-based passwords remain the dominant method because they are simple to implement and familiar to users; however, extensive research and industry reports show that user-chosen passwords are often weak, reused across sites, and therefore vulnerable to dictionary attacks, credential stuffing, and database leaks. Two-factor authentication (2FA)—typically a password plus an OTP delivered by SMS, email, or generated by an authenticator app—improves security by adding a possession factor, but real-world incidents (e.g., SIM-swapping and phishing that capture OTPs) have exposed operational weaknesses.

Graphical password schemes (for example, click-point systems such as PassPoints) were proposed to increase memorability and resist simple keylogging. Empirical studies indicate that graphical methods can be more memorable than random alphanumeric strings, and they offer some resilience to keyboard-based malware. However, they create new usability and consistency challenges: image scaling, different screen resolutions, ordering constraints, and the potential for shoulder-surfing or screen-recording attacks must be addressed in a robust design.

Biometric systems (fingerprint, face, iris) deliver high assurance because they rely on inherence factors, but they require specialized sensors, raise privacy and false-positive/false-negative concerns, and are often costly to deploy at scale. Hardware token and smart-card solutions provide strong possession-based security but introduce logistics, provisioning, and replacement overhead. Reviews and textbooks (e.g., Stallings; Pfleeger et al.) emphasize that layered or hybrid approaches — combining independent factor types — are generally more resilient than any single method.

VI. EXISTING SYSTEM

Authentication mechanisms in widespread use today fall into several families, each with strengths and limitations. Text-based passwords remain the dominant method because they are simple to implement and familiar to users; however, extensive research and industry reports show that user-chosen passwords are often weak, reused across sites, and therefore vulnerable to dictionary attacks, credential stuffing, and database leaks. Two-factor authentication (2FA)—typically a password plus an OTP delivered by SMS, email, or generated by an authenticator app—improves security by adding a possession factor, but real-world incidents (e.g., SIM-swapping and phishing that capture OTPs) have exposed operational weaknesses.

Graphical password schemes (for example, click-point systems such as PassPoints) were proposed to increase memorability and resist simple keylogging. Empirical studies indicate that graphical methods can be more memorable than random alphanumeric strings, and they offer some resilience to keyboard-based malware. However, they create

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.2025.1412078|

new usability and consistency challenges: image scaling, different screen resolutions, ordering constraints, and the potential for shoulder-surfing or screen-recording attacks must be addressed in a robust design.

Biometric systems (fingerprint, face, iris) deliver high assurance because they rely on inherence factors, but they require specialized sensors, raise privacy and false-positive/false-negative concerns, and are often costly to deploy at scale. Hardware token and smart-card solutions provide strong possession-basedsecurity but introduce logistics, provisioning, and replacement overhead. Reviews and textbooks (e.g., Stallings; Pfleeger et al.) emphasize that layered or hybrid approaches — combining independent factor types — are generally more resilient than any single method.

VII. DISADVANTAGES

- Single-factor (password) systems: Highly vulnerable to brute-force, credential stuffing, phishing, and password reuse. They create a single point of failure that attackers commonly exploit.
- Traditional 2FA (SMS/Email OTP): While improving protection, these channels are susceptible to interception, SIM-swap attacks, and social-engineering techniques that defeat the second factor. Delivery delays and account recovery weaknesses also reduce reliability.
- Graphical-only systems: Although more memorable, they can be vulnerable to shoulder-surfing, screen capture, and device heterogeneity (different resolutions or responsive layouts can impair matching). Usability across devices and accessibility for visually impaired users remain concerns.
- Biometric systems: High implementation and maintenance cost, privacy implications (biometric data is sensitive and irrevocable), and possible spoofing or sensor vulnerabilities make them less practical for many deployments.
- Token-based systems: Hardware tokens and smart cards improve security but add procurement, distribution, and lifecycle management overhead—barriers for smaller organizations.

VIII. PROPOSED SYSTEM

The proposed 3-Level Password Authentication System is a hybrid MFA solution that sequentially enforces three complementary authentication types:

- Knowledge-based (Level 1): Traditional alphanumeric username and password. Passwords are hashed using bcrypt and validated server-side to provide a baseline knowledge factor.
- Recognition-based (Level 2): Graphical click-point authentication where a user selects exactly three points on an image during registration and must reproduce those points within a configurable tolerance at login. This recognition-based step reduces the effectiveness of keyboard-only attacks and improves memorability.
- Possession/time-based (Level 3): A one-time password (OTP) delivered via email (or displayed in console in demo mode). Each OTP is time-limited, single-use, and stored with metadata (created_at, expires_at, used flag) to support auditability and lifecycle enforcement.

IX. ADVANTAGES

- Enhanced Security multiple layers of authentication make it extremely difficult for attackers to bypass the system, reducing risks of unauthorized access.
- Protection Against Common Attacks the system provides resistance to brute-force, dictionary, phishing, and password-guessing attacks by adding multiple verification steps.
- User Verification Accuracy combining password, PIN/OTP, and security questions or CAPTCHA ensures that only legitimate users can log in.
- Cost-Effective Solution unlike high-cost biometric systems, this approach can be implemented with minimal hardware requirements.
- Flexibility and Scalability the system can be extended to include advanced authentication methods such as biometrics.

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.2025.1412078|

X. SYSTEM REQUIREMENTS

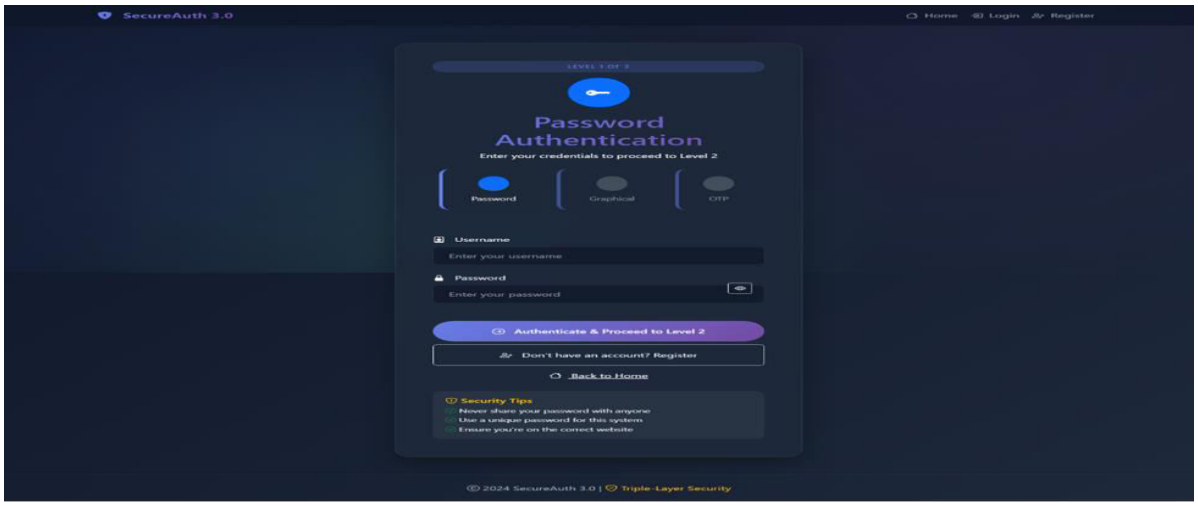
Hardware Requirements

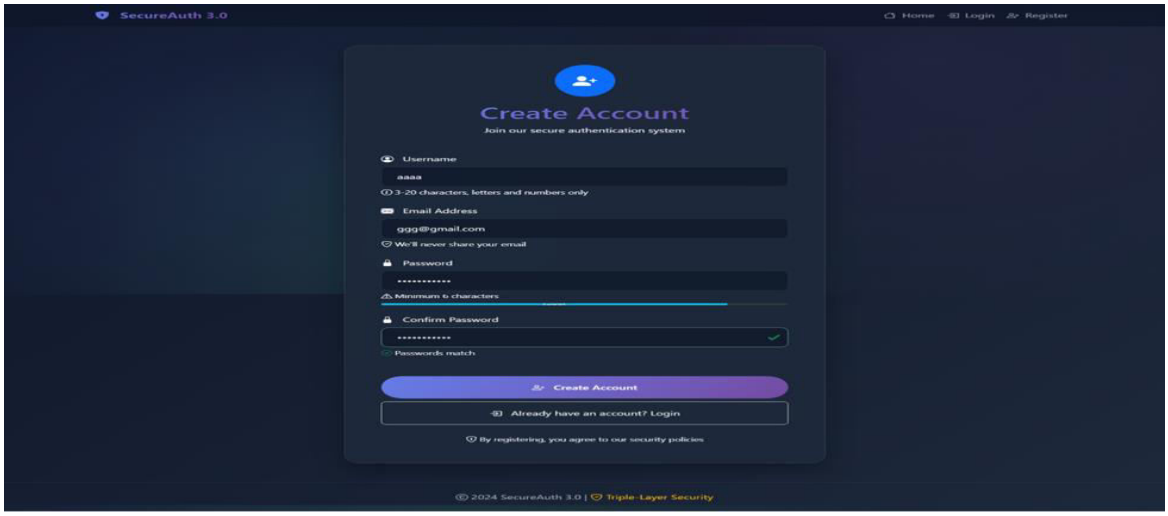
- Processor: Intel i5 or equivalent
- RAM: 4 GB minimum
- Storage: 256 GB SSD
- Network: Stable internet connection

Software Requirements

- Operating System: Windows 11 / Linux / macOS
- Backend: Python 3.8+, Flask, SQLAlchemy
- Frontend: HTML5, CSS3, JavaScript (ES6+)
- Database: SQLite (development), MySQL/PostgreSQL (production)
- Email Service: SMTP server (Gmail/Outlook)
- Development Tools: VS Code, Git, Postman

XI. RESULTS





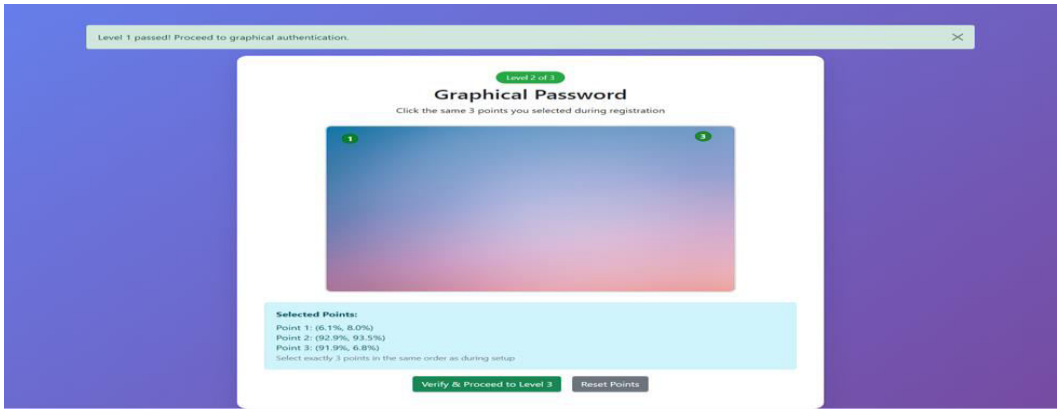
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

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.2025.1412078|



XII. CONCLUSION

The 3-Level Password Authentication System successfully addresses the limitations of traditional authentication methods by implementing a multi-factor approach that combines knowledge-based, recognition-based, and possession-based authentication.

The system provides:

- Enhanced Security: Three independent layers requiring simultaneous compromise
- Cost-Effectiveness: No specialized hardware requirements
- User Acceptance: Progressive authentication that doesn't overwhelm users
- Scalability: Modular design allowing easy integration with existing systems
- Auditability: Comprehensive logging for security monitoring

The implementation using Flask and modern web technologies ensures maintainability, while the use of established cryptographic algorithms (bcrypt, SHA-1) provides robust security foundations.

REFERENCES

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.
2. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing. Pearson Higher Ed.
3. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of Applied Cryptography. CRC Press.
4. Sushma Y, S., & Prabhudeva, S. (2022). Three Level Graphical Password Authentication System with File Encryption. International Journal of Advanced Research in Science Communication and Technology.
5. M, D., & S, N. (2020). Biometric Based Three-Factor Mutual Authentication Scheme for Electronic Payment system using ellipse curve cryptographic. Malaysian Journal of Computer Science.

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