

# Artificial Intelligence-Based Graphical Password Authentication for Enhanced Security

**Jinal Divyeshkumar Patel<sup>1</sup>, Dr Papri Das<sup>2</sup>**

<sup>1</sup>Research Scholar, <sup>2</sup>Associate Professor

<sup>1,2</sup>School of information technology

Auro University, Surat, Gujarat, India

## Abstract

Graphical password authentication has emerged as an alternative to conventional text-based passwords by allowing users to authenticate through images, visual patterns, and graphical interactions. However, traditional graphical password schemes remain vulnerable to attacks such as shoulder surfing, brute-force attempts, password guessing, and pattern-based exploitation. Moreover, many existing approaches primarily rely on static authentication information and do not sufficiently adapt to changes in user behaviour or emerging security threats. This research proposes an Artificial Intelligence-Based Graphical Password Authentication approach aimed at enhancing authentication security through intelligent analysis of user interactions and authentication behaviour. The proposed approach integrates graphical password mechanisms with artificial intelligence techniques to identify legitimate and anomalous authentication patterns. User interaction features, such as selection behaviour, interaction sequence, timing characteristics, and authentication patterns, can be analysed to support adaptive authentication and risk-based decision-making. Based on the assessed risk level, the system can strengthen authentication requirements when suspicious behaviour is detected while maintaining a convenient authentication experience for legitimate users. The proposed framework is intended to improve resistance against common graphical password attacks while reducing dependence on static password information. The effectiveness of the approach can be evaluated using security, authentication accuracy, false acceptance rate, false rejection rate, usability, and computational performance. The research aims to demonstrate how AI-driven behavioural analysis can contribute to a more secure, adaptive, and intelligent graphical password authentication framework.

## Keywords

Artificial Intelligence, Graphical Password Authentication, Behavioural Analysis, Adaptive Authentication, Risk-Based Authentication, User Authentication, Authentication Security, Anomaly Detection, Password Attacks.

## 1. Introduction

Authentication is a fundamental component of information security. Most real-world systems still rely on **text-based passwords**, despite their well-known limitations. Users tend to choose weak and predictable passwords due to memorability issues, making systems vulnerable to cyber-attacks.

Graphical Password Authentication (GPA) has been investigated as an alternative to conventional textual passwords, using image recognition, click-points, and other graphical interactions for authentication [1], [2].

However, traditional GPA systems validate only the correctness of the graphical input and do not analyse user behaviour. As a result, attackers using scripts or automated tools can still bypass such systems if the graphical password is compromised.

To address this limitation, this paper introduces **Artificial Intelligence (AI) and Machine Learning (ML)** into graphical password authentication. By analysing **behavioural patterns**, the system can differentiate between genuine users and malicious entities, even when the graphical password is correct.

## 2. Materials and Methods

### 2.1 Related Work

Early authentication systems relied on text passwords, which were later enhanced using CAPTCHAs, OTPs, and biometric systems. While biometrics such as fingerprints and facial recognition offer strong security, they require additional hardware and raise privacy concerns.

Graphical password techniques such as:

#### Pass Points

- ✓ **Category:** Recall-based & Click-based
- ✓ **Authentication Method:** User clicks on a sequence of specific points on **a single image**.
- ✓ **Key Feature:** Password = ordered set of coordinates.
- ✓ **Security Notes:** Vulnerable to **hot-spot attacks** (users tend to choose common areas) and **shoulder surfing**.
- ✓ **Type of Memory Required:** Exact location recall (no system hints).

Pass-Points uses a sequence of user-selected points on an image as the authentication secret [1], [2].

#### Cued Click Points

- ✓ **Category:** Cued recall-based & Click-based
- ✓ **Authentication Method:** User clicks **one point per image** across **multiple images** in sequence.
- ✓ **Key Feature:** Each click leads to the next image → provides **visual cues** to aid memory.

- ✓ **Security Notes:** More resistant to hot-spot attacks than Pass Points; variants like **PCCP** further improve security using persuasive click guidance.
- ✓ **Type of Memory Required:** Location recall with image cues (easier usability)

Cued Click Points uses one click per image and provides visual cues to support password memorability [4].

## Image-based selection schemes

- ✓ **Category:** Recognition-based (sometimes hybrid depending on design)
- ✓ **Authentication Method:** User selects previously chosen images from a larger set.
- ✓ **Key Feature:** No need to recall coordinates—only recognize and choose images.
- ✓ **Examples:** Pass faces, Story-based image selection, Image sequence recognition.
- ✓ **Security Notes:** Better usability, but can still be weak against shoulder surfing and guessing attacks if image choices are predictable.

## Shoulder Surfing

- ✓ **Category:** Observation-based attack
- ✓ **Authentication Method:** An attacker observes the user while they enter their graphical password, either directly or through video recording.
- ✓ **Key Feature:** The attacker can remember the **click locations, image sequence, and user interaction pattern** and later reproduce them.
- ✓ **Security Notes:** Graphical passwords can be vulnerable when click points are clearly visible during authentication. Techniques such as **image/position randomization, dynamic interfaces, and shoulder-surfing-resistant designs** can reduce this risk.

Graphical password schemes have also been studied specifically to address observation and shoulder-surfing attacks [3], [5].

## Hotspot

- ✓ **Category:** Statistical / Predictability-based attack
- ✓ **Attack Method:** The attacker targets **commonly selected or predictable areas (hot spots)** in images instead of knowing the exact user's password.
- ✓ **Key Feature:** Many users tend to select visually attractive, memorable, or meaningful regions, creating **popular click points** that can be predicted.
- ✓ **Security Notes:** Hot-spot attacks can be reduced using randomization, persuasive click guidance, larger password spaces, and mechanisms that discourage predictable click locations.

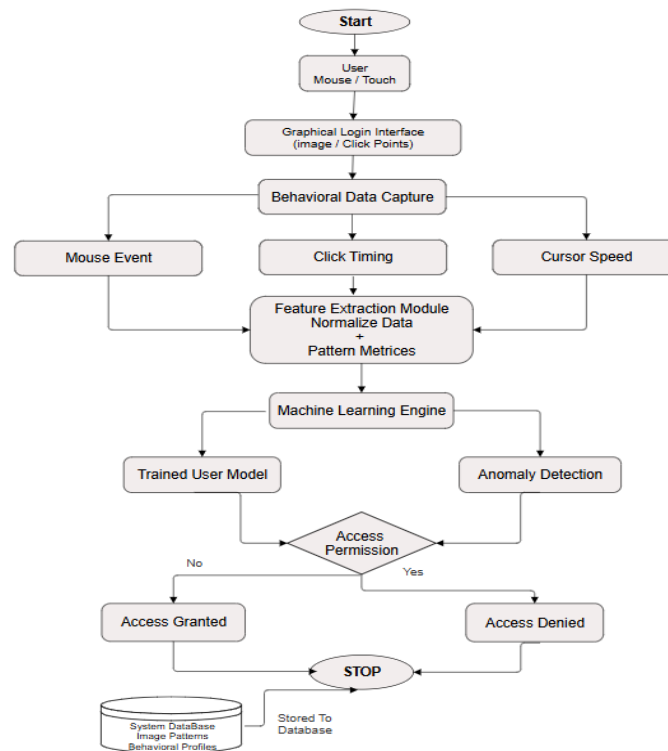
User-selected click points can exhibit predictable hotspots, creating a potential weakness in click-based graphical passwords [7], [8].

Have shown improved usability but remain vulnerable to shoulder surfing and hotspot attacks.

Recent studies have explored behavioural biometrics, including **keystroke dynamics, mouse movement analysis, and continuous behavioural authentication** [10]–[15].

However, the integration of AI-driven behavioural analysis with graphical password authentication remains comparatively less explored, particularly in real-world deployment scenarios.

## 2.2 Proposed System Architecture



### Block Diagram Flow

The proposed system consists of four main modules:

#### A. User Registration Module

- ✓ Mouse movement Path
- ✓ Click durations
- ✓ Time Interval between clicks

#### B. Graphical Login Module

- ✓ User repeats the same graphical pattern
- ✓ Behavioural data is captured again during login

#### C. Feature Extraction Module

- ✓ Extracts numerical features from mouse and click data
- ✓ Normalizes data for machine learning input

#### D. AI-Based Authentication Module

- ✓ Machine learning model compares current behaviour with stored profile

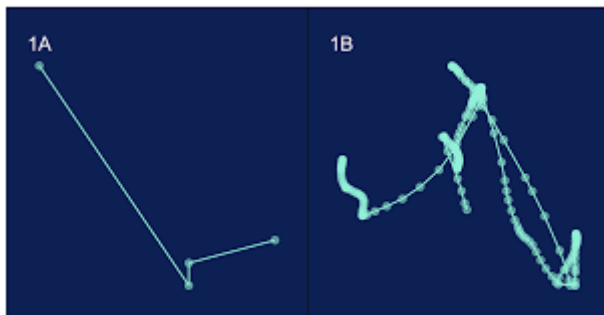
- ✓ Detects anomalies and suspicious patterns

## 2.3 Use of Graphical Passwords in AI & Machine Learning

Graphical passwords are used as a **secure authentication method** where users log in using **images, patterns, or click-points** instead of text passwords.

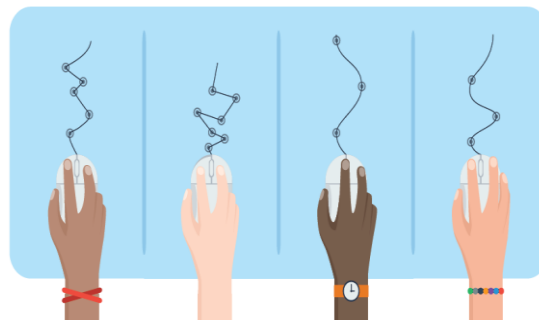
When combined with **Artificial Intelligence (AI)** and **Machine Learning (ML)**, graphical passwords become **intelligent security systems** that can:

- ✓ Verify what the user selects (image/pattern)
- ✓ Analyse how the user interacts (behaviour)
- ✓ Detect humans vs. bots automatically



1A: Automated mouse Movement

1B: Human Mouse Movement



Human Mouse Behaviour

## 2.4 Need of AI and Machine Learning in Graphical Password

Traditional graphical passwords only check **correctness**, but AI & ML add **behavioural intelligence**. But with AI and ML we can learn

- ✓ Learn normal user behaviour
- ✓ Detect abnormal or suspicious logins
- ✓ Prevent automated attacks even if the password is stolen
- ✓ Reduce reliance on CAPTCHAs and OTPs

## 2.5 Graphical Passwords and AI works together

### 2.5.1 Registration Algorithm

#### Step1: Graphical Credential Selection

The user selects the predefined graphical password images and corresponding click points.

#### Step2: Behavioural Data Collection

During the authentication process, the system records user interaction parameters, including:

- Mouse movement patterns

- Click timing
- Cursor trajectory/path

### Step3: Behavioural Profile Generation

The collected interaction data are processed and provided to a trained **Machine Learning (ML) model**, which analyses the user's behavioural characteristics and generates a **user behavioural profile**.

### Step4: Process Termination

The behavioural data collection and profile-generation process is completed, and the generated behavioural profile is securely stored for subsequent authentication.

Step5: STOP

## 2.5.2 Login Algorithm

### Step 1: Graphical Password Re-authentication

The user repeats the registered graphical password by selecting the predefined images and corresponding click points.

### Step 2: Behavioural Feature Collection

The system captures the user's current behavioural interaction features, including mouse movements, click timing, cursor trajectory, and interaction sequence.

### Step 3: AI-Based Behavioural Comparison

The extracted behavioural features are provided to the trained AI/ML model and compared with the user's previously stored behavioural profile.

### Step 4: Authentication Decision

- If the current behavioural pattern sufficiently matches the stored profile, **access is granted**.
- If the behavioural pattern is identified as abnormal, **access is denied or additional verification is triggered**.

### Step 5: Process Termination

The authentication process is completed and the decision is recorded for security monitoring.

Step 6: STOP

## 2.5.3 AI driven Graphical Password Authentication

### Step 1: Initialization

Initialize the graphical password authentication and behavioural analysis system.

### Step 2: Graphical Password Registration

The user registers a graphical password by selecting predefined images and corresponding click points.

### Step 3: Behavioural Data Acquisition

The system captures the user's behavioural interaction features, including mouse movements, cursor trajectory, click timing, and interaction sequence.

## Step 4: Machine Learning Model Training

The collected behavioural features are processed and used to train a machine learning model for generating the user's behavioural profile.

## Step 5: Login Attempt

The registered user initiates the authentication process by entering the graphical password.

## Step 6: Real-Time Behavioural Analysis

During login, the system captures and extracts the user's real-time behavioural features.

## Step 7: Behavioural Verification and Access Granting

The AI/ML model compares the current behavioural pattern with the stored behavioural profile. If the behaviour satisfies the defined similarity criteria, **access is granted**.

## Step 8: Anomaly Detection and Response

if the observed behaviour deviates from the stored behavioural profile, the authentication attempt is classified as anomalous. **Access is denied and a security alert is triggered**.

## Step 9: Termination

terminate the authentication session and securely record the authentication outcome.

## Step 10: STOP

## 3. Results

### 3.1 Role of Machine Learning in the System

| ML Model         | Purpose                               |
|------------------|---------------------------------------|
| Random Forest    | Detect abnormal login patterns        |
| SVM              | Separate genuine users from attackers |
| Neural Networks  | Learn complex behaviour               |
| Isolation Forest | Identify anomalies                    |

Using ML continuously **improves accuracy** with more login data.

### 3.2 Real world Application of AI –Based Graphical Password Authentication

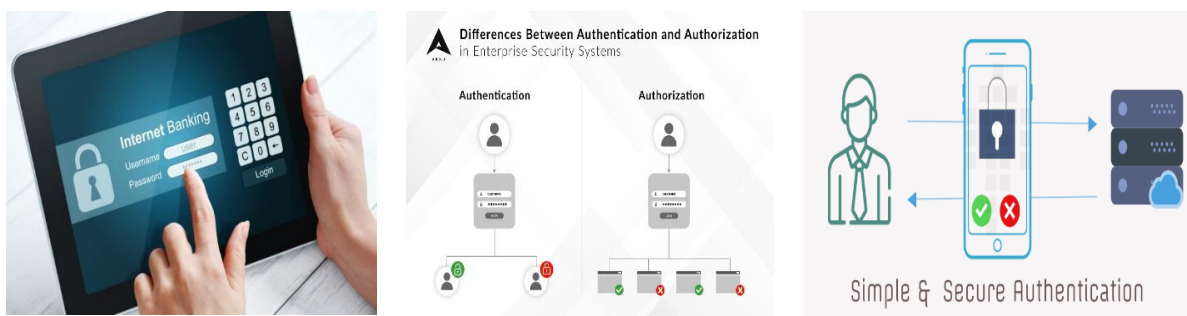


Fig: Real-world application of Graphical password authentication

- A. Banking and Finance Services
  - ✓ Secure net banking logins
  - ✓ Prevent phishing and credential stuffing
- B. Mobile Applications
  - ✓ Touch-based graphical authentication
  - ✓ Gesture behaviour analysis
- C. Corporate & Enterprise System
  - ✓ Employee authentication
  - ✓ Insider threat prevention
- D. E-learning and online Exams
  - ✓ Verifies student identity
  - ✓ Prevents impersonation
- E. Healthcare Systems
  - ✓ Protects patient records
  - ✓ HIPAA-compliant secure access

## 4. Discussion

### 4.1 Human vs. Bot Detection

| Feature        | Human         | Bot      |
|----------------|---------------|----------|
| Mouse Movement | Natural curve | Straight |
| Click Timing   | Random        | Fixed    |
| Cursor Speed   | Variable      | Constant |
| Mistakes       | Minor Errors  | Perfect  |

AI models easily detects Bots based on these patterns.

### Security Analysis

| Attack Type             | Resistance                |
|-------------------------|---------------------------|
| Brout Force Attack      | Highly Resistance         |
| Shoulder Surfing Attack | Medium to High Resistance |
| Bot Attacks             | Highly Resistance         |
| Replay Attacks          | Highly Resistance         |
| Phishing Attack         | Medium Resistance         |

### 4.2 Real World Application

- ✓ Online Banking Systems
- ✓ E-learning platforms
- ✓ Healthcare Portals
- ✓ Corporate Login Systems
- ✓ Cloud Based Applications

### 4.3 Advantages in real world Implementations.

- ✓ No need to remember complex passwords
- ✓ Key logging and Brute force attack resistant.
- ✓ Low cost software.
- ✓ Scalable across platforms.
- ✓ No special hardware required
- ✓ Improved security
- ✓ User-friendly authentication

#### **4.4 Limitations in real-world use**

- ✓ Requires behavioural data for training
- ✓ Image hotspot attacks need mitigation
- ✓ Accessibility issues for visually impaired users
- ✓ Slight increase in computation cost
- ✓ Behavioural changes over time may affect accuracy
- ✓ Initial training data required

#### **4.5 Importance in today's world**

With increasing:

- ✓ Cyber attacks
- ✓ Boat based Hacking
- ✓ Credential theft

AI-powered graphical passwords offer a next-generation authentication solution that is secure, usable, and intelligent.

#### **5. Conclusion**

The proposed AI-based graphical password authentication framework enhances traditional graphical authentication by integrating user behavioural analysis with machine learning. The system captures features such as mouse movements, cursor trajectories, click timing, and interaction patterns to generate a behavioural profile. During login, the user's real-time behaviour is compared with the stored profile to identify legitimate and anomalous users. This additional behavioural layer can strengthen protection against unauthorized access. Future work will focus on evaluating machine learning techniques, optimizing behavioural features, and assessing the framework using security, accuracy, usability, and performance metrics.

#### **References**

1. Jermyn, A. Mayer, F. Monroe, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proc. 8th USENIX Security Symposium, Washington, DC, USA, 1999, pp. 1–14.
2. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys, vol. 44, no. 4, Art. no. 19, pp. 1–41, 2012, doi: 10.1145/2333112.2333114.
3. Jain et al., "Biometric Authentication Systems," Springer, 2007.

4. Bishop, C. M., Pattern Recognition and Machine Learning, Springer.
5. R. Biddle et al., “Graphical Passwords: Learning from the First Twelve Years,” ACM Computing Surveys, 2012.
6. <https://www.geeksforgeeks.org/blogs/graphical-password-authentication/>
7. <https://livesession.io/blog/mouse-movement-tracking-free-full-guide-tools-and-techniques>
8. M. Arun Prakash; T.R. Gokul - Network security-overcome password hacking through graphical password authentication - 2011 National Conference on Innovations in Emerging Technology
9. S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points,” in Computer Security – ESORICS 2007, Springer, 2007, pp. 359–374.
10. S. Khan, C. Devlen, M. Manno, and D. Hou, “Mouse Dynamics Behavioral Biometrics: A Survey,” ACM Computing Surveys, vol. 56, no. 6, Art. no. 154, pp. 1–33, 2024, doi: 10.1145/3640311.
11. P. H. Pisani and A. C. Lorena, “A systematic review on keystroke dynamics,” Journal of the Brazilian Computer Society, vol. 19, pp. 573–587, 2013
12. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, and J. Fierrez, “TypeNet: Deep learning keystroke biometrics,” IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 57–70, 2022.
13. M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, “Sensor-Based Continuous Authentication of Smartphones’ Users Using Behavioral Biometrics: A Contemporary Survey,” IEEE Internet of Things Journal, 2020, doi: 10.1109/JIOT.2020.3020076.
14. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, and J. Fierrez, “TypeNet: Deep Learning Keystroke Biometrics,” IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 57–70, 2022.
15. P. H. Pisani and A. C. Lorena, “A Systematic Review on Keystroke Dynamics,” Journal of the Brazilian Computer Society, vol. 19, pp. 573–587, 2013.