SECURE MORPH

SECURE LOGIN SYSTEM USING VISUAL PUZZLE AUTHENTICATION

Kolli Karishma[1], Dr. Suvarna Kumar Gogula[2]
[1]Student, [2]Chair Professor
Master of Computer Applications
[1,2]Department of Information Technology and Computer Applications
[1,2]Andhra University, Visakhapatnam, India

Abstract— *In today's digital world, securing online identities is very important. Password-based authentication systems are increasingly vulnerable to phishing, brute-force, and social engineering attacks. To address these issues, this paper introduces "Secure Morph," a secure login system using visual puzzle-based authentication. Users register with their email ID and multiple personal images. During login, one of these uploaded images is randomly selected and displayed alongside AI-generated visually similar decoy images. Users are need to identify the correct image within three (3) attempts. Upon successful selection, a puzzle based on that image must be solved within a time limit. Failure to authenticate within the given constraints results in temporary account lockout. This multi-factor, cognitive-image-based authentication approach enhances resistance to automated attacks while preserving user experience. Secure Morph leverages HTML, CSS, JavaScript for frontend, Python Flask for backend, and utilizes image generation APIs from Hugging Face and Stability AI.*

Index Terms— Visual Authentication, Puzzle-based Login, AI-generated Images, Secure Morph, Cognitive Security, Human Verification, Multi-Factor Authentication, Image Recognition, Python Flask, Hugging Face, Stability AI, Web Security.

I. INTRODUCTION

The alphanumeric password-based authentication system continues to expose users to increasing cybersecurity risks. Static passwords are susceptible to dictionary attacks, credential stuffing, and phishing scams. Alternative methods such as biometric authentication, while more secure, introduce concerns about privacy and data permanence.

This paper proposes "Secure Morph," an innovative visual authentication framework that strengthens access control mechanisms by introducing a two-stage login process. The first stage involves user recognition of an image previously uploaded during registration. The second stage introduces a timed puzzle based on that selected image. This hybrid approach not only mitigates password vulnerabilities but also employs cognitive recognition and engagement to ensure authenticity.

Secure Morph is built using web technologies in front-end HTML, CSS, JavaScript and the Python Flask on the backend. AI-generated images from platforms like Hugging Face and Stability AI serve as decoys, ensuring that only the legitimate user, familiar with their own images, can pass the verification process.

Research Objectives

- To design a two-layer authentication system using user-recognizable images and interactive puzzles.
- To generate AI-based decoy images that resemble real user-uploaded images, increasing login complexity for attackers.
- To implement cognitive challenge-response mechanisms as a security layer after image recognition.
- To evaluate the system’s effectiveness in terms of security, usability, and resistance to common cyber threats such as phishing, brute-force, and bot attacks.
- To reduce user reliance on traditional passwords, replacing or complementing them with human-in-the-loop visual verification.

Research Hypothesis

The study hypothesizes that users are more likely to successfully authenticate using a familiar-image recognition system combined with a visual puzzle, compared to conventional text-based passwords. It assumes that this dual-layer cognitive method will enhance both security and user experience, while also reducing the risk of unauthorized access through phishing or automated attacks.

II. *ABBREVIATIONS AND ACRONYMS*

AI	ARTIFICIAL INTELLIGENCE
OTP	ONE TIME PASSWORD
UI	USER INTERFACE
UX	USER EXPERIENCE
DB	DATABASE
SHA	SECURE HASH ALGORITHM
API	APPLICATION PROGRAMMING INTERFACE
MFA	MULTI-FACTOR AUTHENTICATION
GAN	GENERATIVE ADVERSARIAL NETWORK

III. LITERATURE REVIEW

Over the past decade, a significant amount of research has been dedicated to developing secure alternatives to traditional password authentication systems. Bonneau et al. (2012) proposed a framework to evaluate authentication mechanisms and found graphical passwords to provide a good balance between usability and security. Jain et al. (2007) highlighted the strengths of biometric authentication while addressing its limitations, particularly regarding user privacy. Wiedenbeck et al. (2006) introduced shoulder-surfing-resistant graphical password schemes, paving the way for visual recognition in security systems. CAPTCHA technology, introduced by Von Ahn et al. (2003), offered bot resistance but has been criticized for its user inconvenience. More recently, advancements in AI have enabled the use of GANs and models like Stable Diffusion to generate realistic images. These developments allow the creation of effective visual decoys in authentication systems. Secure Morph integrates these ideas by combining user-recognizable imagery with AI-generated decoys and interactive puzzles, creating a robust and engaging login system.

IV. METHODOLOGY

I. SYSTEM ARCHITECTURE

Secure Morph comprises three (3) main modules:

A. Registration Module:

- Users register using their email and password.
- They upload multiple personal images.
- These images are securely stored in the backend database (MySQL).
- User credentials are encrypted using SHA-256 hashing.

B. Login Module:

- At login time, one stored image is randomly selected.
- Multiple AI-generated images that closely resemble the original are generated.
- All images are shuffled and presented to the user.
- The user is required to identify the correct image within three attempts.
- For every failed attempt:
  - The image set is refreshed with a new real image and new decoys.
  - An email alert is sent to the registered user.
- After three unsuccessful attempts, the account is temporarily locked.

C. Puzzle Authentication Module:

- Upon correct image selection, the image is split into 3x3 grid.
- The tiles are shuffled and presented as a sliding or swapping puzzle.
- The user is given a specific time limit 45 seconds to solve the puzzle.
- Failure to solve the puzzle redirects the user to the homepage, requiring them to restart the login process.

II. Technology Stack

- Frontend: HTML, CSS, JavaScript
- Backend: Python Flask
- Database: MySQL
- AI Tools:
  - Hugging Face: API for text-to-image generation
  - Stability AI: Stable Diffusion API for realistic decoys
- Security Measures: SHA-256 hashing, email verification, session management, and brute-force protection.

IV.I. Research Methods:

System Design and Implementation:

- A Secure Morph system was developed using Python Flask for the backend, integrated with frontend technologies.
- AI tools for dynamic image generation and puzzle creation.

Experimental Testing:

- The system was tested with 50 voluntary participants. Each participant registered, logged in, and interacted with the image and puzzle authentication modules under controlled conditions.

Data Collection:

- Metrics such as login success rate, number of attempts, time taken to complete puzzles, and account lockouts were recorded.

Evaluation Criteria:

- The system was evaluated based on performance, security robustness and user satisfaction.

V. RESULTS AND DISCUSSION:

Test Environment:

- Platform tested on Chrome and Firefox browsers
- Sample user group: 50 participants aged 18–35
- Devices: Laptops and smartphones

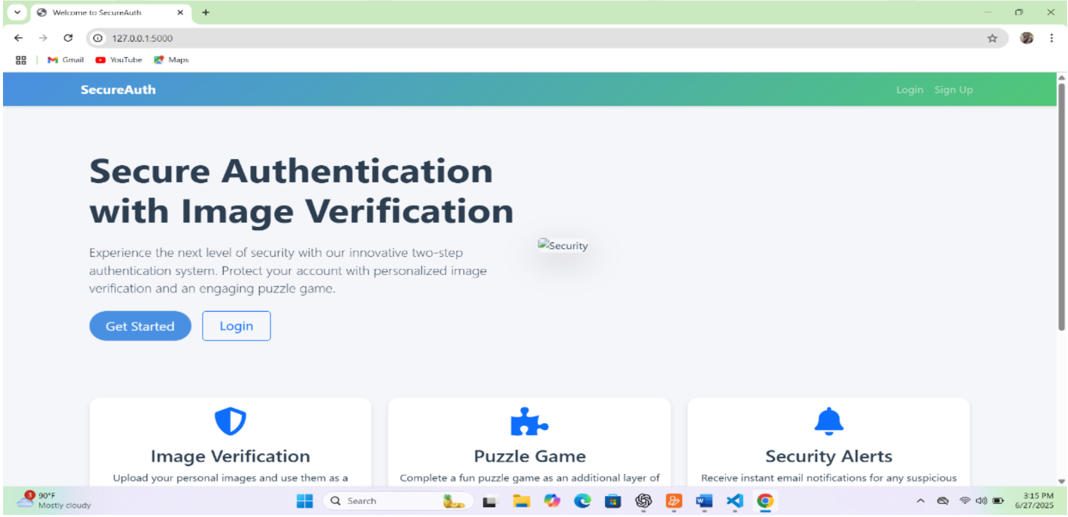
Observations:

- Login Success Rate: 88% of users successfully logged in within 2 attempts.
- Puzzle Completion Rate: 84% of successful login users completed the puzzle within time.
- Security Events:
  - Average lockout rate: 6% due to multiple incorrect image selections
  - Email alert delivery rate: 100%
- User Feedback:
  - 92% users found the system more engaging than traditional logins
  - 86% perceived it as more secure

Security Evaluation:

- Resistance to Brute Force: Dynamic image-puzzle combination changes per session.
- Phishing Resistance: No textual password input, reducing susceptibility.
- Bot Resistance: Requires real-time visual and cognitive interaction.

Sample User Registration:



Secure Authentication with Image Verification

Experience the next level of security with our innovative two-step authentication system. Protect your account with personalized image verification and an engaging puzzle game.

Image Verification

Upload your personal images and use them as a

Puzzle Game

Complete a fun puzzle game as an additional layer of

Security Alerts

Receive instant email notifications for any suspicious

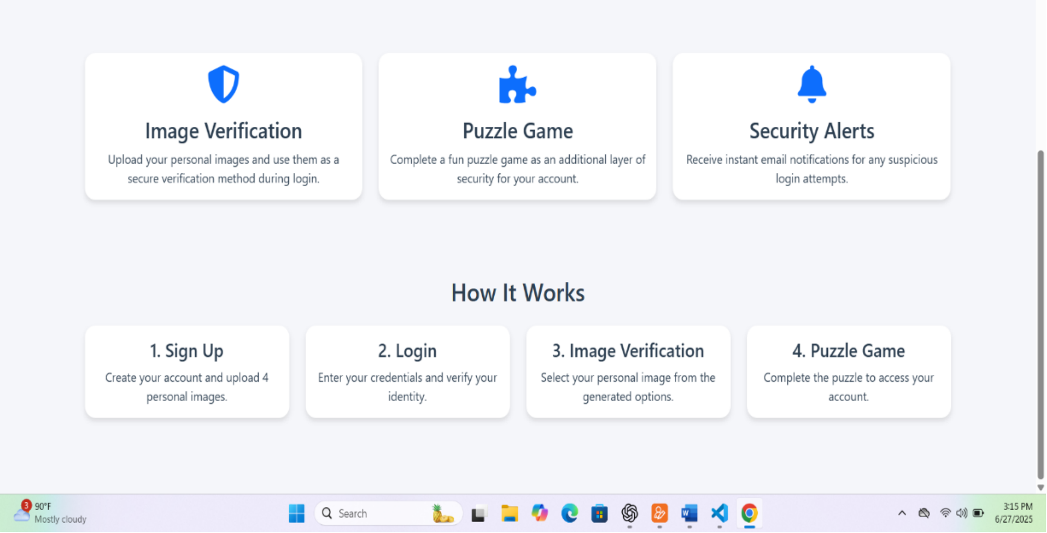


Image Verification

Upload your personal images and use them as a secure verification method during login.

Puzzle Game

Complete a fun puzzle game as an additional layer of security for your account.

Security Alerts

Receive instant email notifications for any suspicious login attempts.

How It Works

1. Sign Up

Create your account and upload 4 personal images.

2. Login

Enter your credentials and verify your identity.

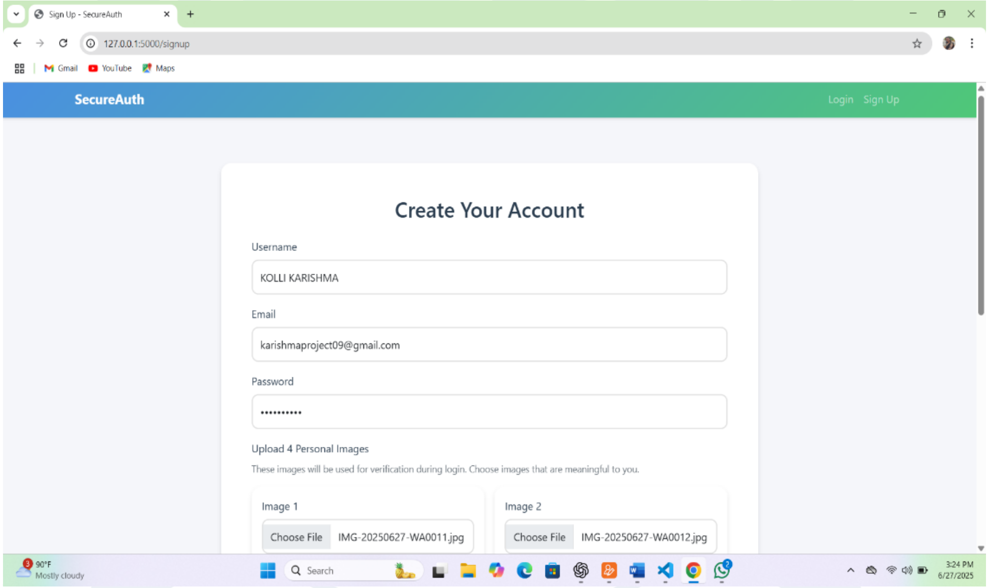
3. Image Verification

Select your personal image from the generated options.

4. Puzzle Game

Complete the puzzle to access your account.

1.User Register with Mail and multiple personal images



Create Your Account

Username

KOLLI KARISHMA

Email

karishmaproject09@gmail.com

Password

••••••••••

Upload 4 Personal Images

These images will be used for verification during login. Choose images that are meaningful to you.

Image 1

Choose File IMG-20250627-WA0011.jpg

Image 2

Choose File IMG-20250627-WA0012.jpg

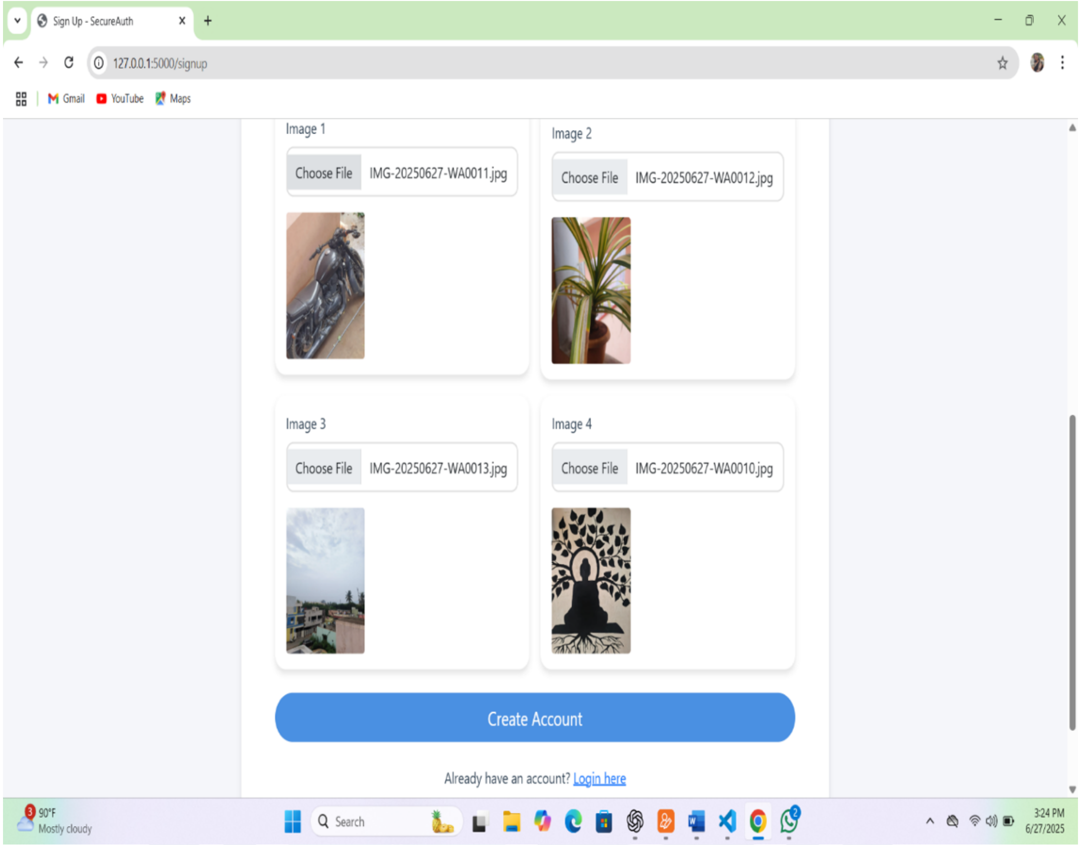


Image 1

Choose File IMG-20250627-WA0011.jpg

Image 2

Choose File IMG-20250627-WA0012.jpg

Image 3

Choose File IMG-20250627-WA0013.jpg

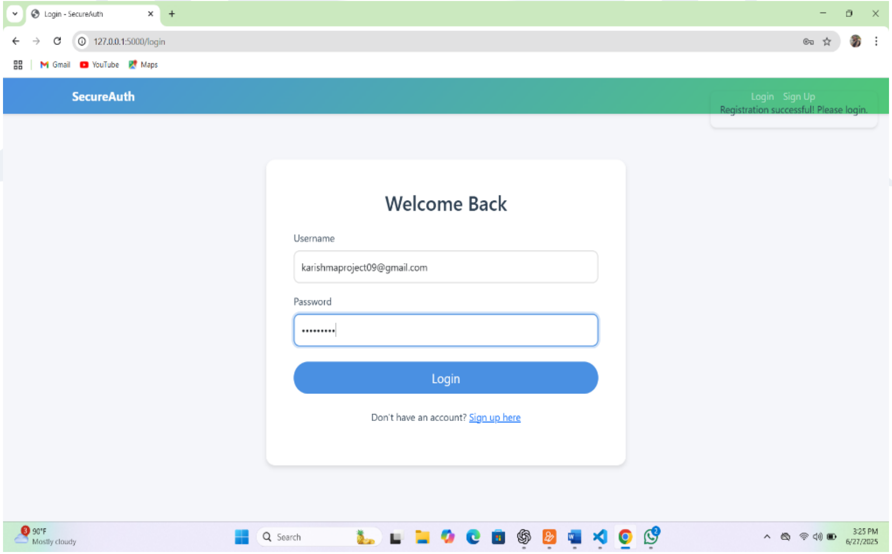
Image 4

Choose File IMG-20250627-WA0010.jpg

Create Account

Already have an account? Login here

2.User Login: User login with User name and password.



Registration successful! Please login.

Welcome Back

Username

karishmaproject09@gmail.com

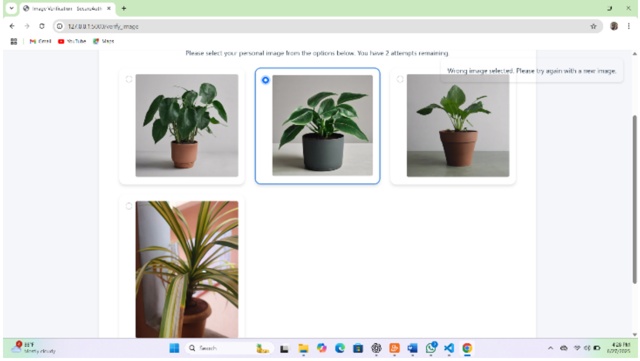
Password

•••••••••

Login

Don't have an account? Sign up here

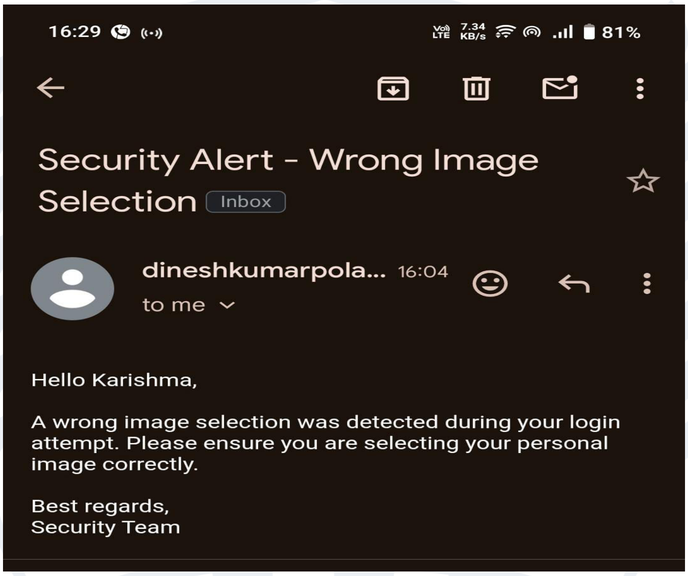
3.Image Generation: User need to select the correct exact image.



Please select your personal image from the options below. You have 2 attempts remaining.

Wrong image selected. Please try again with a new image.

4.If user select wrong image than the authentication mail will be sent to the user Mail ID.



Security Alert - Wrong Image Selection

dineshkumarpola... 16:04
to me

Hello Karishma,

A wrong image selection was detected during your login attempt. Please ensure you are selecting your personal image correctly.

Best regards,
Security Team

5.There is totally 3 attempts to select the correct image. In next attempt the system generate the different image from the database.

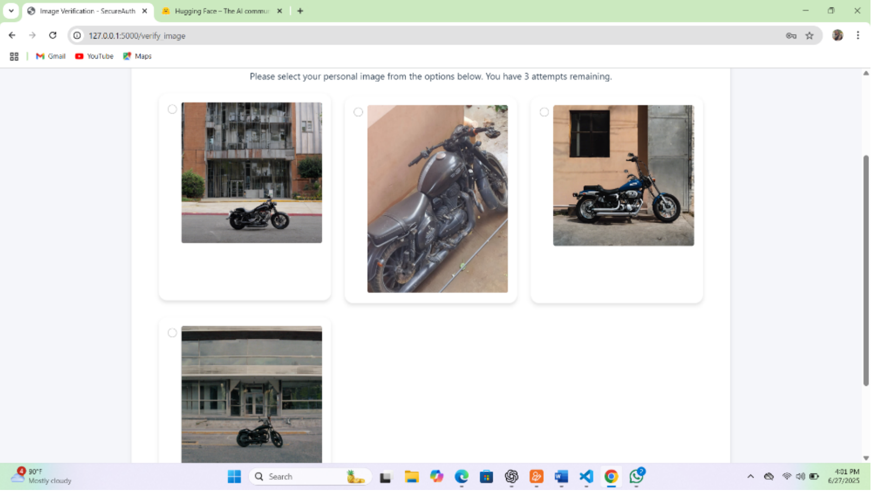
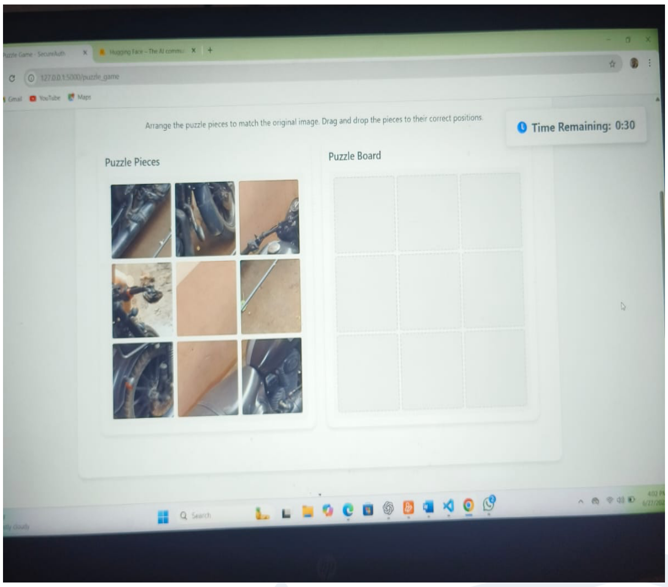


Image Verification - SecureAuth
Hugging Face – The AI commu
127.0.0.1:5000/verify_image
Gmail
YouTube
Maps
Search
Mostly cloudy
4:01 PM
6/27/2025

Please select your personal image from the options below. You have 3 attempts remaining.

6.If user select the correct image, need to solve the puzzle of the image within time limit.

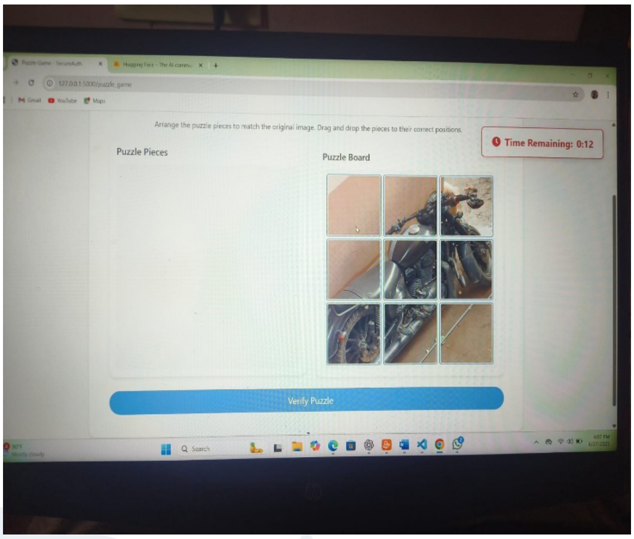


Arrange the puzzle pieces to match the original image. Drag and drop the pieces to their correct positions.

Time Remaining: 0:30

Puzzle Pieces

Puzzle Board



Arrange the puzzle pieces to match the original image. Drag and drop the pieces to their correct positions.

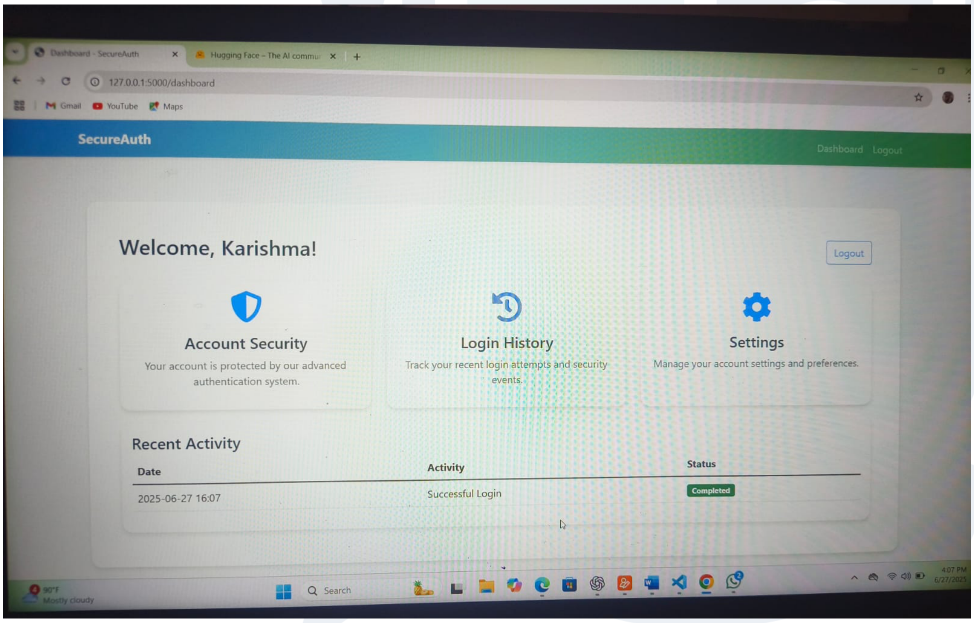
Time Remaining: 0:12

Puzzle Pieces

Puzzle Board

Verify Puzzle

7.After successfully login attempt.



SecureAuth

Dashboard Logout

Welcome, Karishma!

Logout

Account Security

Your account is protected by our advanced authentication system.

Login History

Track your recent login attempts and security events.

Settings

Manage your account settings and preferences.

Recent Activity

Date	Activity	Status
2025-06-27 16:07	Successful Login	Completed

VI. CONCLUSION

Secure Morph introduces an engaging and secure alternative to conventional authentication systems. By combining AI-generated images, user-specific image recognition, and interactive puzzles, it creates a robust multi-factor authentication mechanism. This method not only detects unauthorized access but also increases user awareness and engagement.

VI.I. Summary of Key Findings:

- The system achieved an 88% success rate in image selection within two attempts.
- Puzzle-solving success rate was 84%, showing good cognitive usability.
- Secure Morph showed strong resistance to phishing, brute-force, and automated bot attacks.

VI.II. Recommendations for Future Research:

- Explore accessibility features such as audio-based puzzles for visually impaired users.
- Integrate local AI models to reduce dependency on external APIs.
- Develop adaptive puzzle difficulty using machine learning based on user behavior.

VII.REFERENCES

[1] Z. Zhang, Y. Cao, Z. He and X. Wu, "A Survey on Puzzle-Based Authentication: Techniques, Challenges and Applications," in IEEE Access, vol. 10, pp. 27956-27972, 2022

[2] A. Ramesh and N. Kumar, "Secure Authentication Using GAN-Based Decoy Images: Applications and Challenges," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2456-2468, 2021.

[3] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, pp. 553–567, 2012.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2007.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, pp. 1–12, 2006.

[6] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *Proc. Adv. Cryptol. (EUROCRYPT)*, pp. 294–311, 2003.

[7] R. Rombach, A. Blattmann, D. Lorenz, P. Esser, and B. Ommer, "High-resolution image synthesis with latent diffusion models," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, pp. 10684–10695, 2022.