Graphical Password using Image Segmentation

This presentation explores how graphical passwords leverage image segmentation for enhanced security. We'll examine its principles, advantages, and implementation.

Prepared By:

Sourabh Sinha [23SCSE2150018]

Saurabh Kumar [23SCSE2030726]

Tanish Tyagi [23SCSE2150023]

What is a graphical password?

Traditional Passwords

Traditional passwords rely on text-based sequences, prone to brute-force attacks and susceptibility to forgetting.

Graphical Passwords

Graphical passwords use visuals for authentication, increasing memorability and security by relying on visual pattern recognition.

How does image segmentation work?

Image Analysis

The image is analyzed to identify distinct regions based on colors, textures, and other visual characteristics.

Pixel Grouping

Similar pixels are grouped together to form segments representing different objects or areas within the image.

Grid Creation

The segmented image is divided into a grid, typically a 4x4 matrix, creating a visual puzzle for authentication.

Benefits of a graphical password

1 **Enhanced Memorability**

Visuals are easier to remember than text sequences, making it more user-friendly.

2 **Increased Security**

Graphical passwords are harder to guess or brute-force, providing stronger protection against unauthorized access.

3 **User-Friendly Interface**

Graphical passwords are intuitive and engaging, making authentication more enjoyable for users.

Step 1: User uploads an image

Image Selection

Users choose an image they find memorable and meaningful, such as a personal photo or a favorite artwork.

Step 2: Image is segmented into a 4x4 grid

1

Segmentation Process

The image is automatically segmented into 16 individual squares, preserving the original visual elements.

2

Grid Display

The 16 squares are then arranged randomly within a 4x4 grid, creating a unique visual puzzle.

Step 3: User authenticates by rearranging the segments

1

Puzzle Interaction

Users interact with the grid, dragging and dropping the segments to rearrange them in their original order.

2

Authentication

Once the segments are correctly rearranged, the system verifies the user's identity, granting access.

Securing documents with graphical passwords

1

Data Encryption

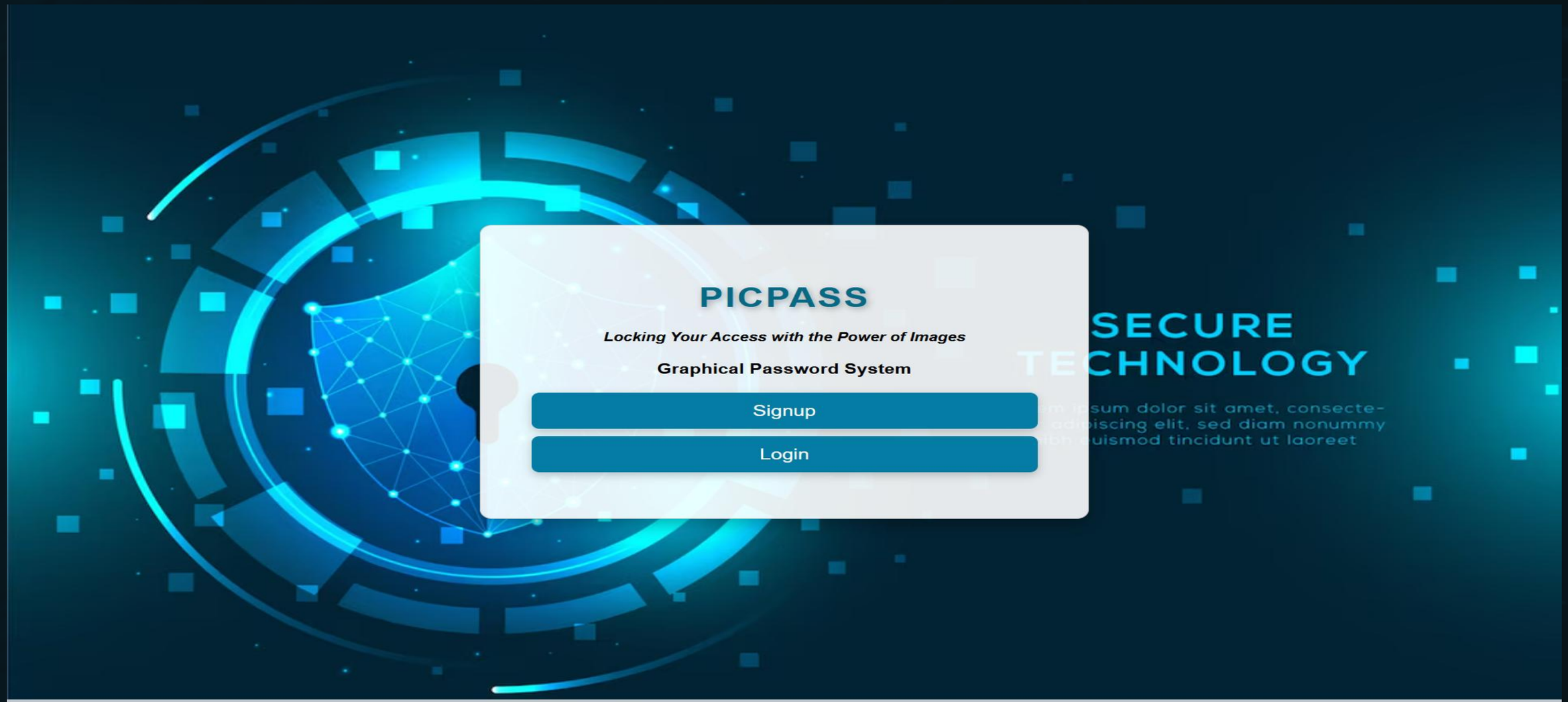
The document is encrypted using a secure algorithm, making it unreadable without proper authorization.

2

Graphical Key

The graphical password serves as the decryption key, enabling only authorized users to unlock the document.

SCREENSHOTS



Experience the future of password protection with graphical authentication and seamless file uploads.

Signup

host

••••

Choose File HD.jpg

Register

Already have an account? Login here

Go to Home

SECURE
ECHNOLOGY

ipsum dolor sit amet, consecte-
dipiscing elit, sed diam nonummy
euismod tincidunt ut laoreet

Login

host

••••

Choose File HD.jpg

Login

Don't have an account? Sign up here

Go to Home

SECURE
ECHNOLOGY

ipsum dolor sit amet, consecte-
dipiscing elit, sed diam nonummy
euismod tincidunt ut laoreet

Welcome to Your PicPass Dashboard

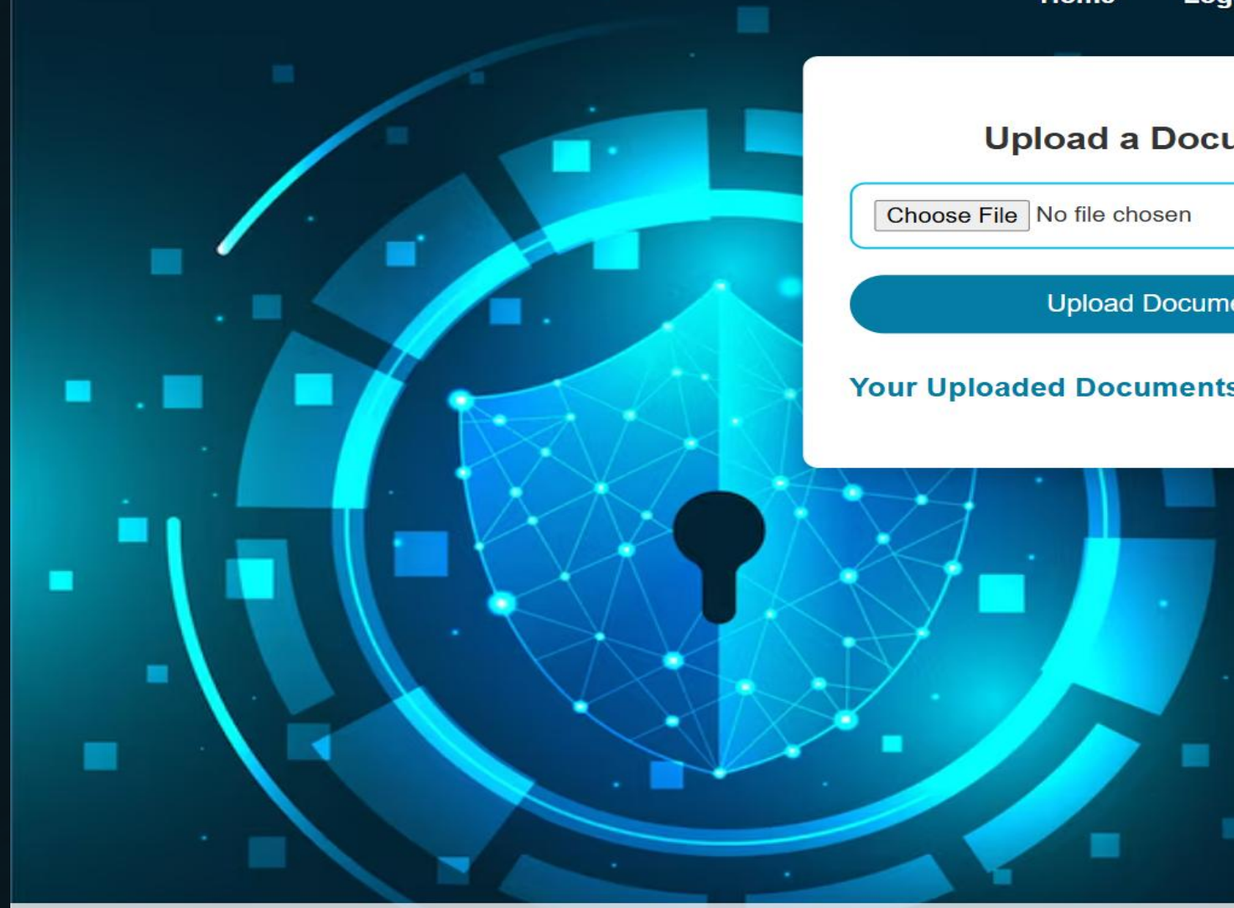
Home Logout

Upload a Document

Choose File No file chosen

Upload Document

Your Uploaded Documents



SECURE TECHNOLOGY

Lorem ipsum dolor sit amet, consecte-
tuer adipiscing elit, sed diam nonummy
nibh euismod tincidunt ut laoreet

Securely store and manage your files with ease—your personal digital locker, accessible anytime, anywhere.

© 2025 PicPass. All rights reserved.

Privacy Policy | Terms of Service

BY Saurabh & Sourabh

Welcome to Your PicPass Dashboard

Home Logout

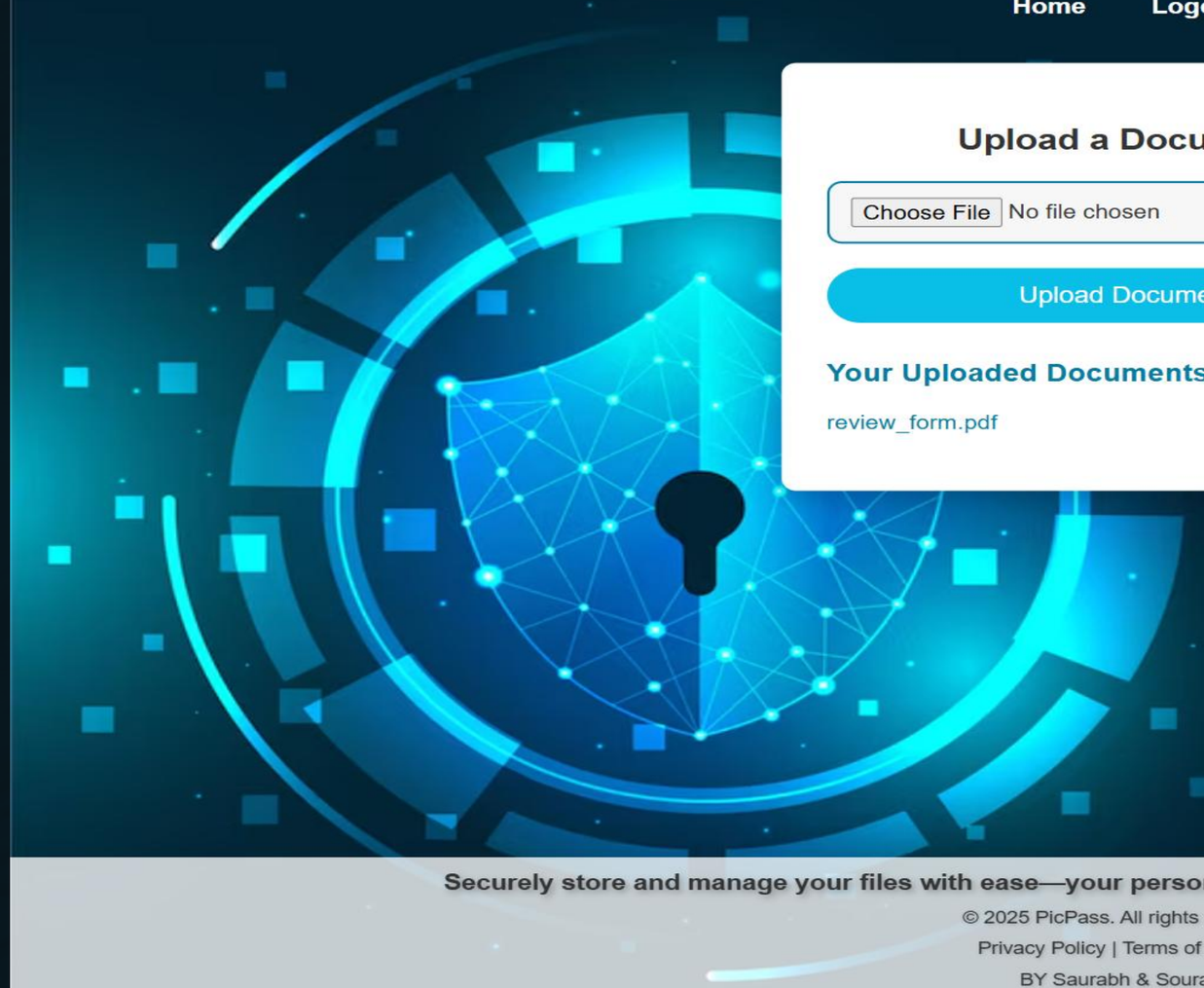
Upload a Document

Choose File No file chosen

Upload Document

Your Uploaded Documents

review_form.pdf



SECURE TECHNOLOGY

Lorem ipsum dolor sit amet, consecte-
tuer adipiscing elit, sed diam nonummy
nibh euismod tincidunt ut laoreet

Securely store and manage your files with ease—your personal digital locker, accessible anytime, anywhere.

© 2025 PicPass. All rights reserved.

Privacy Policy | Terms of Service

BY Saurabh & Sourabh