Synopsis on Graphical Password Authentication using Image Segmentation

- **Rebanta Mandal**, Registration No: 220953632, Roll No: 55
- **Aditya P Sajjan**, Registration No: 220953029, Roll No: 10
- **Ved Sai Srikar Abbaraju**, Registration No: 220953628, Roll No: 54
- **H Ganapathi Kamath**, Registration No: 220953667, Roll No: 62

1. System Requirements

1.1 Hardware Requirements

The successful implementation of the proposed graphical password authentication system requires a thorough understanding of the necessary system requirements, both in terms of hardware and software. These requirements ensure that the system operates efficiently and provides the desired security features while maintaining usability for end users.

1. ***Server Specifications:***
   - **Processor:** A multi-core processor (Intel i5 or equivalent) to handle multiple requests simultaneously and ensure efficient data processing.
   - **RAM:** A minimum of 8 GB of RAM to support the smooth execution of applications, particularly during peak load times.
   - **Storage:** Sufficient storage space (at least 500 GB SSD) to accommodate the database and image files, allowing for quick read and write operations.
   - **Network Interface:** A reliable network interface card (NIC) to maintain stable connectivity, ensuring swift communication between the server and client devices.
2. ***Client Specifications:***
   - **Processor:** A dual-core processor or better to facilitate smooth operation of web browsers and applications.
   - **RAM:** At least 4 GB of RAM to support multitasking and efficient browsing.
   - **Display:** A monitor capable of supporting high resolution (1920x1080 or higher) to display images and interfaces clearly.
   - **Internet Connection:** A stable internet connection with a minimum speed of 1 Mbps for optimal performance during user authentication processes.

1.2 Software Requirements

The software components required for the graphical password authentication system encompass both the operating system and application software.

1. ***Operating System:***
   - **Server OS:** Windows Server 2016 or later, which provides a robust environment for hosting the SQL Server and the web application.

- **Client OS:** Windows 10 or later for users, allowing compatibility with modern web browsers and applications.

2. ***Development Tools:***
   - **Integrated Development Environment (IDE):** Microsoft Visual Studio 2019 or later, providing comprehensive tools for application development, debugging, and testing.
   - **Database Management System:** Microsoft SQL Server 2019 or later for managing the relational database that stores user data, authentication logs, and images.

3. ***Web Technologies:***
   - **Frameworks:** .NET Framework or .NET Core for developing the server-side logic and APIs.
   - **Languages:** C# for backend programming and JavaScript/HTML/CSS for frontend development, enabling dynamic web interfaces and interactions.
   - **Image Processing Libraries:** Libraries such as System.Drawing or OpenCV for image manipulation, segmentation, and handling user-uploaded images effectively.

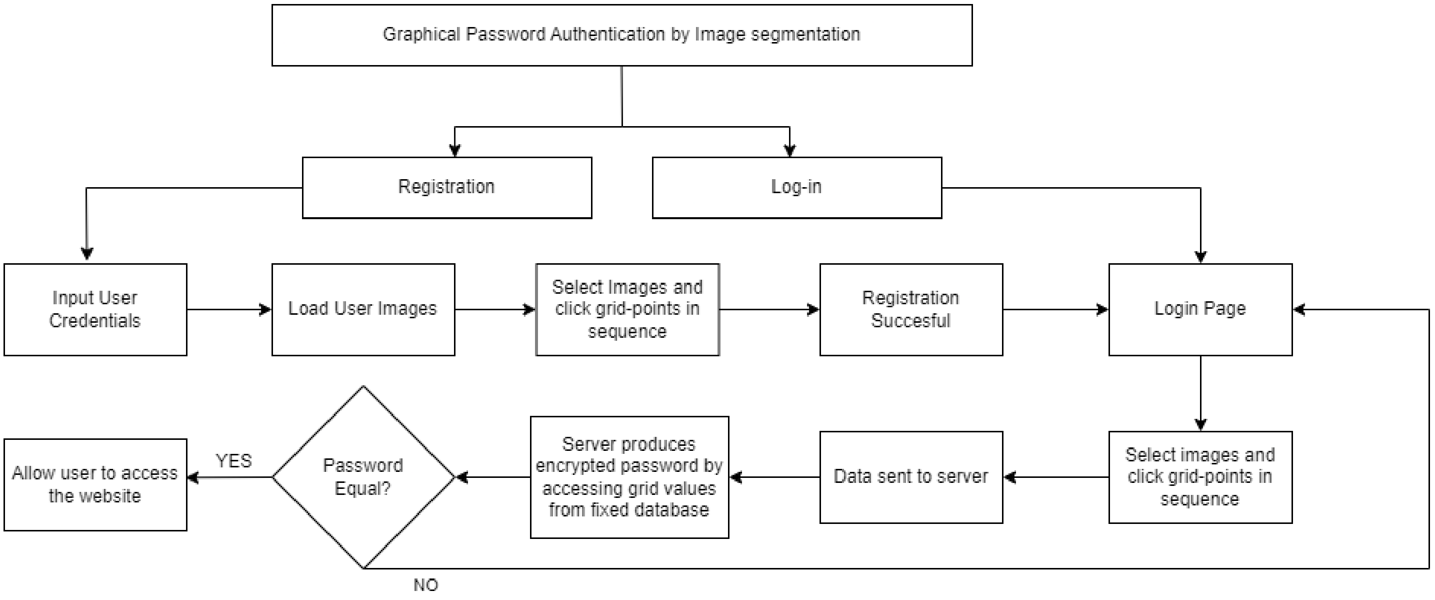
4. ***Browser Compatibility:***

   The application should support modern web browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari to ensure a wide range of accessibility for users.

2. Model Design

2.1 Initial Block Diagram

The initial block diagram of the graphical password authentication system provides a visual representation of the system's architecture. The diagram typically includes the following components:


Graphical Password Authentication by Image segmentation
Registration
Log-in
Input User Credentials
Load User Images
Select Images and click grid-points in sequence
Registration Succesful
Login Page
Select images and click grid-points in sequence
Data sent to server
Server produces encrypted password by accessing grid values from fixed database
Password Equal?
YES
Allow user to access the website
NO

2.2 Model Design Components

The model design consists of several key components that define the functionality and interaction of the system:

1. ***Image Submission:***

Users are prompted to submit an image, which will be segmented for authentication purposes. The image upload interface allows users to easily select and upload their chosen image.

2. ***Image Fragmentation and Storage:***

Upon submission, the system divides the uploaded image into a grid (e.g., 9x9) and stores the individual segments separately in the database. Each segment is assigned a unique identifier, facilitating easy retrieval during the authentication process.

3. ***Part Jumbling:***

The system presents the segmented parts to the user in a random order to enhance security. This process ensures that attackers cannot easily guess the correct sequence or arrangement of image segments.

4. ***Authentication Process:***

During authentication, users must rearrange the jumbled image segments to match their original order. The system verifies the placement of segments against stored data to confirm user identity. If the user successfully matches the original order, authentication is granted; otherwise, access is denied.

5. ***User Management:***

The system also includes user management features, allowing for user registration, password recovery options, and secure handling of user data.

Conclusion

The graphical password authentication system's model design and system requirements are critical components that contribute to its effectiveness and usability. By ensuring that the hardware and software requirements are met, and by implementing a structured model design, the system can provide secure, user-friendly authentication that capitalizes on users' ability to recognize images. The careful consideration of these elements lays a strong foundation for the successful deployment and operation of the system, addressing the growing need for robust authentication solutions in an increasingly digital world.