

FACIAL AUTHENTICATION SYSTEMS PROJECT

By Wala Marzouki

Third deliverable



MY FACIAL AUTHENTICATION WEB APP

TABLE OF CONTENTS

- Scope: The Solution Overview and Objectives
- System architecture
- Users and Roles
- Workflows
- Review



THE SOLUTION OVERVIEW AND OBJECTIVES

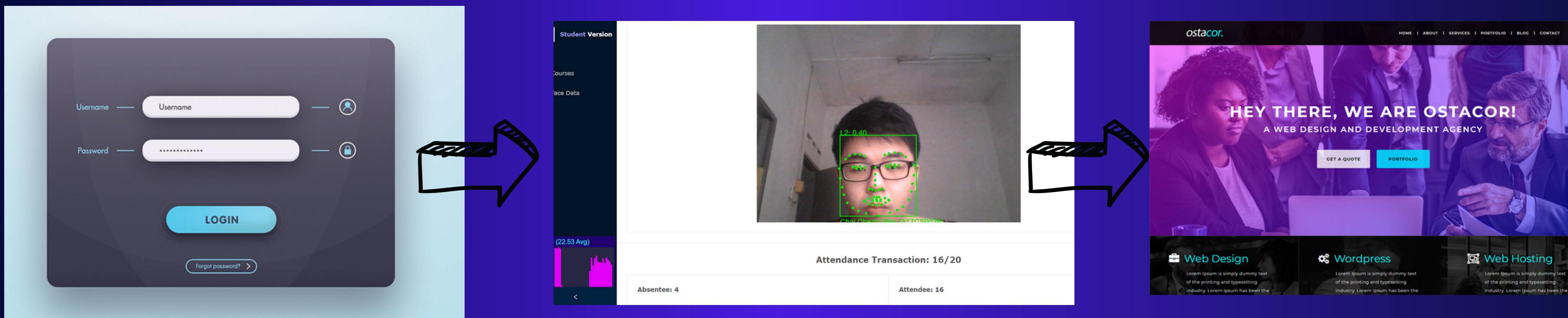
In the rapidly changing digital world of today, ensuring the authenticity of users engaging in online interactions is paramount. Traditional authentication techniques frequently fall short in providing the necessary level of security and convenience. This problem is addressed by our Facial Authentication Web App, which provides a quick, easy, and highly secure authentication procedure.

Our primary objectives center around enhancing access control to sensitive company information and revolutionizing secure online communication. Through the utilization of advanced facial recognition technology, we empower enterprises to safeguard their digital assets and uphold the integrity of their online communication channels. By providing a reliable system for authenticating users, whether they are managers accessing critical company data or CEOs conducting virtual meetings with global teams, our technology significantly reduces the risk of unauthorized access and potential security breaches.

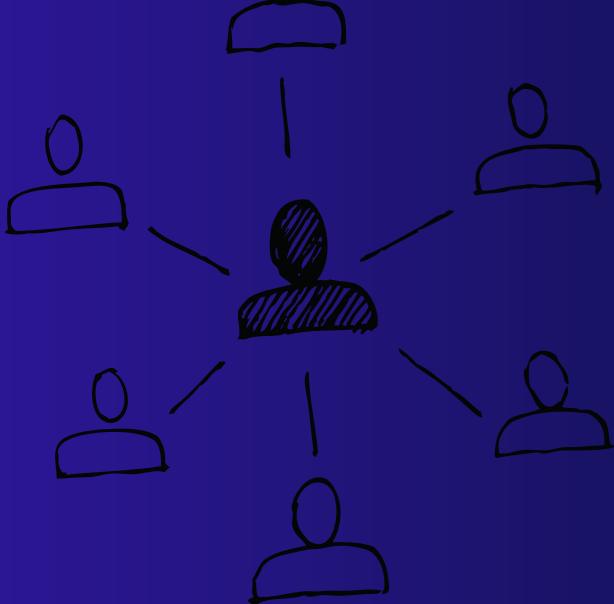


SYSTEM ARCHITECTURE

we have three interconnected components that collectively ensure a seamless and secure user experience: the login interface, the authentication interface, and the website interface. The login interface serves as the entry point for users, where they provide their credentials to access the system. Once authenticated, users are seamlessly directed to the authentication interface, where their facial features are meticulously compared with reference images of authorized individuals. Upon successful authentication, users gain entry to the website interface, which serves as the central hub for accessing critical data and links for online meetings.



USERS AND ROLES



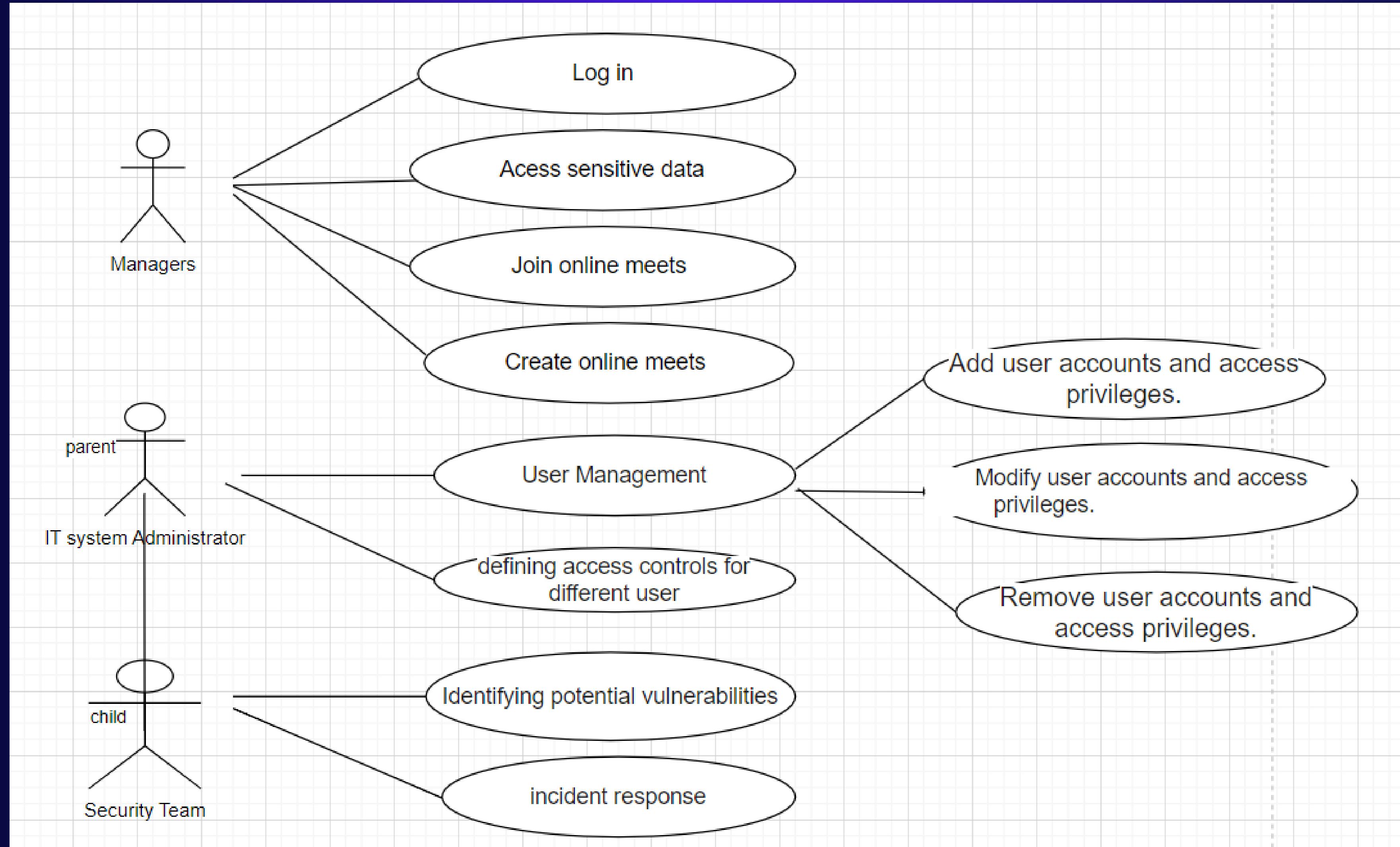
Users in our system represent a wide range of positions, each with specific duties and access levels based on the requirements of their respective organizations.

- **At the forefront are Managers**, responsible for operational supervision and making decisions in their areas of expertise. They use the system to retrieve important corporate data that is necessary for their managerial duties and to organize or take part in online meetings.
- **IT System administrators**, With their unique control over user management and system configurations, act as the protectors of system integrity. They ensure comprehensive control over user management, system configurations, and database updates for access privileges so a smooth run of operations in a secure way.

Together these roles form a cohesive ecosystem which ensure efficient collaboration and safeguarding organizational assets through the utilization of our facial authentication system.

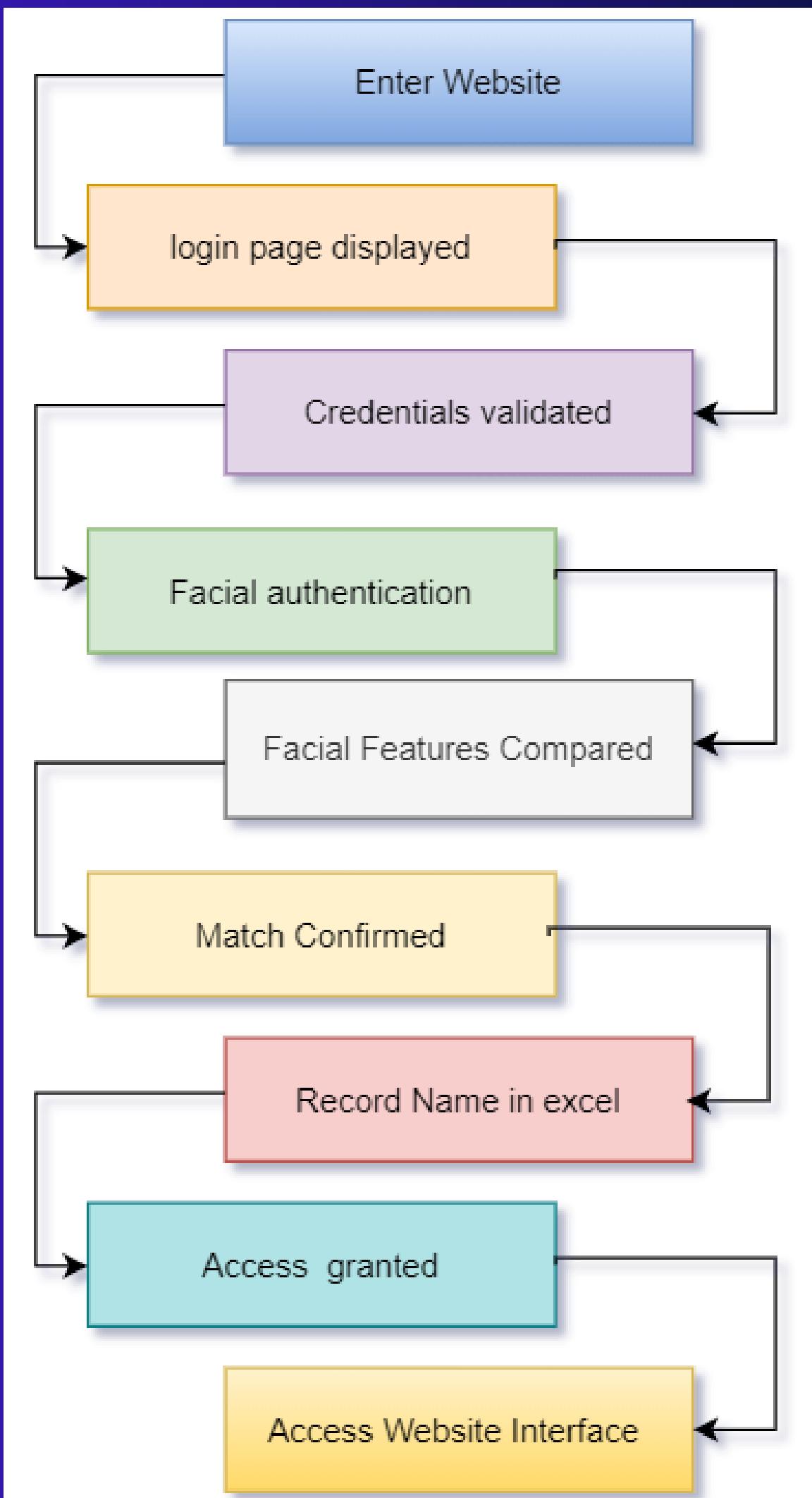
- **The security Team** specialists in threat assessment, data security, and incident response, find possible weak points in the system, put security measures in place to reduce risks, make sure user data (like face scans) is stored securely, and develop incident response plans to deal with any security lapses or problems. This team is essential to maintaining the strength of our system's security protocols.





WORKFLOWS

In our website's operation, users commence by logging in upon entering the platform, utilizing their credentials stored within our registered database. Once successfully logged in, users are seamlessly directed to the facial authentication web page. Here, our system meticulously compares the user's facial features with those of authorized managers stored within our database. This comparison involves computing histograms for both the reference image and the region of interest (ROI) containing the detected face. Utilizing the correlation method, the system measures the similarity between these histograms. If the similarity exceeds a predefined threshold, the individual is authenticated, means there is a match and access is granted so, the individual's name is recorded in an Excel sheet for tracking purposes. Following authentication, users gain access to our website's interface, which houses crucial data and links for facilitating online meetings.



REVIEW

In conclusion, the Facial Authentication Web App represents a significant tool in ensuring secure online communication and access control to sensitive company information. By leveraging facial recognition technology, the system provides a robust authentication mechanism that enhances security, usability, and scalability while maintaining user convenience. Throughout this document, we have explored the high-level design of the system, including its various components, workflows, and user roles.

THANK YOU!