Software Requirements Specification

1. **Introduction**1.1 Purpose:Establish secure lab access through multi-factor authentication.

1.2 Document conventions:Define standards for documentation within the project.

1.3 Intended audience:Developers, security personnel, stakeholders.

1.4 Additional information:

<https://github.com/ujwalanadella/codeclause_task1_Facedetection>

1.5 Contact information/SRS team members:Member 1:

Name & roll no: - Nadella Ujwala – AP21110010682

E-mail: - [ujwala\_nadella@srmap.edu.in](mailto:ujwala_nadella@srmap.edu.in)

Member 2:

Name & roll no: - Lakkimsetty Sanjana-AP21110010685

E-mail: - [sanjana\_l@srmap.edu.in](mailto:sanjana_l@srmap.edu.in)

Member 3:

Name & roll no: - Jayyavarapu Yaswanth SriRam – AP21110010686

E-mail: - [yaswanthsriram\_j@srmap.edu.in](mailto:yaswanthsriram_j@srmap.edu.in)

Member 4:

Name & roll no: - Jetti Prasanna Kumar – AP21110010687

E-Mail: - [prasannakumar\_j@srmap.edu.in](mailto:prasannakumar_j@srmap.edu.in)

* 1. References:<https://github.com/minivision-ai/Silent-Face-Anti-Spoofing>

1. **Overall Description**

2.1 Product perspective:The proposed secure lab access system is designed to integrate with the organization's current infrastructure, particularly user authentication and access control systems. The relationship with existing systems is as follows:Authentication Systems:Our system will interface with the organization's existing authentication systems, such as LDAP (Lightweight Directory Access Protocol) or Active Directory, to validate user credentials and ensure consistency in user authentication processes.

Access Control Systems:Integration with the organization's access control systems is essential for enforcing security policies and permissions. Our system will communicate with existing access control systems to grant or deny access based on authentication outcomes.

Database Systems:Our system will interact with the organization's database systems to maintain user profiles and access logs. This interaction involves storing and retrieving user information, access permissions, and access history for auditing purposes.

Network Infrastructure:The secure lab access system requires network connectivity to communicate with existing systems. It will utilize standard network protocols and interfaces to establish connections with servers hosting authentication, access control, and database services.

2.2 Product functions:

1) Utilizing a camera or facial recognition technology, the system scans the user's face. Facial features are then compared against a database of authorized users for authentication, allowing access to the secure lab environment.

2)Upon user interaction, the system prompts the user to draw a specific pattern. The drawn pattern is then verified against the predefined pattern for authentication.

2.3 User classes and characteristics: 1)Employees: Authorized personnel affiliated with the organization, requiring regular access to the lab. 2)Visitors: Guests or temporary visitors requiring temporary access to the lab, with limited permissions and shorter-term access needs.

2.4 Operating environment:The system operates within a controlled laboratory environment, characterized by restricted access, controlled lighting conditions, and minimal external interference.

2.5 User environment:Users interact with the system via dedicated touchscreen interfaces or facial recognition devices located at lab entry points, ensuring seamless and intuitive access.

2.6 Design/implementation constraints:1)The system must comply with data privacy regulations (e.g., GDPR, HIPAA), imposing restrictions on data collection, storage, and processing.

2)Hardware limitations, such as processing power and memory, may influence the design and implementation of real-time face recognition algorithms, requiring optimization for efficient operation.

2.7 Assumptions and dependencies: Assumptions:

1)Users possess the necessary technical proficiency to interact with the system effectively.

2)The availability of stable internet connectivity for system updates and data synchronization.

Dependencies:

1)Integration with existing authentication systems (e.g., LDAP, Active Directory) for user credential validation.

2)Availability of compatible hardware meeting system requirements.

1. **External Interface Requirements**

3.1 User interfaces:

1)Face Recognition Interface:

The system utilizes a camera or facial recognition device to capture and analyze the user's facial features for identification and authentication

2)Pattern Drawing Interface:

Users interact with the system via a touchscreen or input device to draw a predefined pattern for authentication.

3.2 Hardware interfaces:

1) Cameras or facial recognition devices capable of capturing high-resolution images for face recognition interface.

2) Sufficient processing power and memory resources to support real-time pattern verification and facial recognition algorithms.

3) Touchscreen devices or input devices for pattern drawing interface.

3.3 Software interfaces:

1)Face Recognition Module: Performs facial recognition to authenticate users based on captured facial features.

2)Pattern Confirmation Module: Responsible for verifying the drawn pattern against the predefined pattern.

3)Database Management System (DBMS): Stores user profiles, access permissions, and access logs.

4)User Interface (UI): Facilitates user interactions for pattern drawing and displays authentication outcomes.

5)Integration Interfaces: Allow communication between software components, including APIs, protocols, and data formats, ensuring seamless interaction and data exchange.

3.4 Communication protocols and interfaces: 1)HTTP/HTTPS

2)TCP/IP

3)APIs

4) Standardized Data Formats (e.g., JSON, XML)

**4. System Requirements**

4.1 Face Recognition: 1)Description and Priority:Face recognition is crucial for accurate user identification, leveraging deep learning to ensure reliable authentication. Its priority lies in providing a robust and efficient means of access control, enhancing security within the lab environment.

2)Action/result:The system captures and analyzes facial features, comparing them against stored templates. The expected result is successful identification of authorized users, granting access upon recognition, or denying access to unauthorized individuals.

3) Functional requirements:Functional requirements include integration with deep learning algorithms for facial feature extraction and matching, real-time image processing capabilities, secure storage of facial templates, and logging of recognition events, ensuring accurate and efficient user authentication.

4.2 Pattern Confirmation: 1) Description and Priority:Pattern confirmation provides an additional layer of security, enhancing the authentication process alongside face recognition. It ensures that only authorized users with knowledge of the predefined pattern can access the lab environment, prioritizing security and access control. 2) Action/result:Upon user interaction, the system prompts for pattern drawing. The expected result is successful verification of the drawn pattern against the predefined pattern, granting access if the patterns match or denying access otherwise.

3) Functional requirements:Functional requirements include a user interface for pattern drawing, an algorithm for pattern verification, storage and retrieval of predefined patterns, and logging of authentication events for auditing purposes, ensuring a seamless and secure authentication process.

**5. Other Nonfunctional Requirements**

5.1 Performance requirements:The system should achieve real-time processing of face recognition and pattern confirmation, providing seamless access within milliseconds.

5.2 Safety requirements:The system must ensure user privacy and data security, adhering to relevant regulations and implementing encryption protocols.

5.3 Security requirements:Implementation of multi-factor authentication, encryption protocols, and access controls to safeguard against unauthorized access and data breaches.

5.4 Software quality attributes:The system should exhibit high reliability through robust error-handling mechanisms and maintainability through modular design and documentation.

5.5 Project documentation:Comprehensive documentation covering system architecture, user manuals, and API documentation to facilitate understanding and future development.

5.6 User documentation:Clear and intuitive user guides with step-by-step instructions for face recognition interactions and pattern drawing, ensuring ease of use for all users.

**6.Other Requirements**

Appendix A: This appendix serves as a placeholder for any additional documentation that may be required in the future. Its content will be determined as the project progresses, allowing flexibility to include supplementary materials as needed.

Appendix B: This appendix serves as a placeholder for any additional documentation that may be required in the future.