SafeLABS - Laboratory User Authentication & Management System

Paranawithana T.D.
Department of Computer Engineering
Faculty of Engineering
University of Sri Jayewardenepura
Nugegoda, Sri Lanka
en97601@foe.sjp.ac.lk

***Abstract* — Laboratory safety, adherence to safety protocols, and efficient management are top priorities in hazardous environments such as chemical laboratories. Traditional authentication control methods, such as ID cards and passwords, are prone to misuse and inefficiency. Furthermore, it might be challenging to ensure that workers follow safety procedures, such wearing personal protective equipment (PPE), and to manage laboratory occupancy and resources effectively. This paper presents SafeLABS, a comprehensive laboratory management system that includes authentication, safety compliance, user and resource monitoring. The system incorporates a face recognition module via the face_recognition library based on HOG (Histogram of Oriented Gradients) - based feature extraction and a pre-trained anti-spoofing module for liveness detection. A YOLOv8-based object detection model is implemented to identify whether personnel are wearing PPE protocol before granting access to hazardous areas. SafeLABS is implemented as a role-based access control web application with real-time lab occupancy status, user and resource management, and Advanced Encryption Standard (AES)-encrypted sensitive data. Experimental results demonstrate the effectiveness of the proposed system in strengthening both security and safety while making laboratory operations more efficient. The study suggests potential areas for further improvement, including the optimization of recognition accuracy and the integration of IoT-based monitoring systems.**

Keywords — Face Recognition, Laboratory Management, Object Detection, Authentication, Web Application

I. INTRODUCTION

A. Challenges in Laboratory Security and Management

Laboratories, particularly in high-risk environments such as chemical research facilities, require strict security, safety, and operational management standards to protect personnel, sensitive materials, and equipment. Traditional authentication methods including ID cards, PINs, and passwords are vulnerable to security breaches due to issues such as theft, sharing or loss. Fingerprint systems have hygiene issues. Additionally, enforcing personal protective equipment (PPE) compliance in hazardous areas is a manual process that is often prone to errors and negligence. Furthermore, laboratory occupancy tracking, user and resource management continue to be essential in maintaining efficiency and security.

B. Advancements for Secure and Efficient Laboratories

Along with the advancements of artificial intelligence and deep learning, biometric verification, automatic object detection using computer vision-based methods, and smart management systems yield promising solutions towards secure, safe, and efficient laboratory practice. Face recognition software allows a more convenient, more secure authentication option with reduced risk compared to traditional authentication control. Similarly, object detection models used in real time can be used to verify PPE compliance, ensuring compliance by staff members with safety regulations before entering restricted zones. A centralized laboratory management system also allows effective tracking of users and resources, improving overall workflow. Automatic attendance recording using biometric authentication-based systems also improves efficiency by eliminating the requirement for manual logging while maintaining proper timekeeping.

C. Overview of SafeLABS

This paper introduces SafeLABS, a comprehensive laboratory management system that integrates authentication, compliance with safety regulations, and management of users and resources. The system uses face_recognition library-based facial authentication and relies on a pre-trained model for liveness detection to prevent spoofing attempts. An object detection model based on YOLOv8 is applied to ensure PPE wearability compliance and analyze real-time CCTV feed footage to determine whether authorized users possess mandatory safety gear like coverall, gloves, and face masks. Moreover, the SafeLABS system incorporates a web-based platform offering role-based access control, real-time monitoring of lab occupancy, user and resource management, and AES-encrypted data storage for sensitive data. An automated attendance tracking system stores user arrival based on successful face verification, reducing manual tasks while improving security.

This work's main contributions are as follows.

- The development of a comprehensive laboratory management system that combines operational user and resource monitoring, safety compliance, and face recognition-based authentication.
- The implementation of a real-time face recognition module with anti-spoofing techniques to improve authentication reliability.
- The incorporation of an automated attendance recording system that seamlessly logs user entry.
- The application of an object detection model based on YOLOv8 for PPE verification in hazardous laboratory areas.

- A scalable web-based management system that offers real-time lab occupancy tracking, role-based access control, and user/resource management.

The remainder of this paper is structured as follows. Section II (Related Work) reviews existing research on biometric authentication, PPE detection, and laboratory management systems. Section III (Methodology) presents the methodology used in implementing SafeLABS. Section IV (Experiments and Results) discusses the experimental setup and results evaluating the effectiveness of the system. Finally, section V (Conclusion and Future Work) concludes the study and outlines future improvements for the system.

II. Related Work

A. Limitations of Traditional Authentication Methods

Traditional laboratory authentication uses physical methods, which have serious limitations. The limits of different authentication methods are discussed by Jain et al. [1], who point out that physical tokens can be misplaced, stolen, or copied. Biometric solutions have their own set of problems. According to Yampolskiy and Govindaraju [2], fingerprint systems can have usability and technical problems in certain environments, including hygienic issues. Password fatigue and cross-system reuse are two well-documented usability concerns with password-based systems, as noted by Woods and Siponen [3]. The labor-intensive and error prone nature of traditional attendance tracking systems results in administrative load and possible security vulnerabilities [4]. Kim et al. [5] explore face recognition for authentication systems, showing notable gains in accuracy over conventional approaches while reducing the associated issues.

B. Safety Compliance and PPE Detection

Safety procedures are very important in chemical laboratories and using personal protective equipment (PPE) correctly is vital in avoiding accidents. Current methods of monitoring safety compliance usually rely on subjective and inconsistent manual inspection procedures. Deep learning techniques for PPE detection in industrial settings are reviewed by Nath et al. [6], who show how convolutional neural networks can precisely recognize the use of safety equipment in real-time.

C. Laboratory Management Systems

The main focus of current laboratory information management systems is on testing workflows and sample tracking . Although the current laboratory information management systems are beneficial at managing data, Prasad and Bodhe [7] explore their implementations and discover that they frequently lack integrated security and safety compliance capabilities.

Due to the limitations of current methods, there is an obvious need for integrated systems that contain automated attendance tracking, safe authentication, comprehensive data management, and safety compliance verification. With a comprehensive strategy that includes deep learning-based face recognition with anti-spoofing features, automated attendance tracking, PPE detection, web-based management system, SafeLABS system which is explored in the following sections addresses these requirements.

III. Methodology

The SafeLABS system offers enhanced security and efficiency in chemical laboratories by combining web-based management, safety compliance verification, and deep learning-based user authentication. The system includes face recognition and liveness detection for authentication and attendance, PPE detection for access to hazardous areas, and a web application with database integration developed with a backend in model-view-controller architecture.

A. Face Recognition and automated Attendance System

The face recognition module first experimented with custom CNN models that were built from scratch and using transfer learning. However, because of problems with accuracy, scalability, and the need to retrain the model each time a new user registers, utilized the face_recognition library built on top of the Dlib library. It uses HOG to recognize faces and ResNet-34 to create 128-dimensional facial embeddings. These embeddings (numerical encodings) are saved in a pickle file upon enrollment. Live embeddings from CCTV feeds are compared to real-time verification with the help of OpenCV using Euclidean distance method. Successful matches in face encodings trigger automatic attendance logging in the database. To counter spoofing, a pre-trained model was integrated. This lightweight anti-spoofing model uses a dual-branch architecture with Fourier spectrum auxiliary supervision, differentiating real faces from fraudulent media such as photos and screens.

B. Safety Equipment Detection for Hazardous Area Access

Access to hazardous laboratory areas is controlled by object detection, which enforces PPE compliance. Using a deep learning-based object detection model, a CCTV camera at the entry to the hazardous area recognizes the necessary personal protective equipment (PPE), such as masks, gloves, and coveralls, in accordance with safety regulations. The system protects people from chemical risks by ensuring that only those wearing all required safety equipment (PPE) are allowed in.

C. Web Application and Database Integration

A scalable web application that offers a centralized platform for administration and monitoring is made for effective and comprehensive laboratory management. User management, resource management, real-time lab occupancy tracking through attendance data, an announcements section for updates in the laboratory and system, data encryption to protect sensitive data, and role-based access control (RBAC) that separates administrative and regular user roles like lab assistants, research assistants are some of the key features of SafeLABS web application. To store and retrieve data, the system connects with a relational database, guaranteeing

smooth interaction between the management and authentication components.

D. System Integration

Liveness detection (pre-trained anti-spoofing model) is integrated with face recognition at the laboratory entrance and if an authorized user enters, his/her attendance is automatically recorded to the database after the verification process. The web application incorporates with database for lab occupancy tracking according to the attendance data, managing users and resources and other functionalities. Safety equipment detection modules comes separately. Fig. 1 illustrates the system architecture.

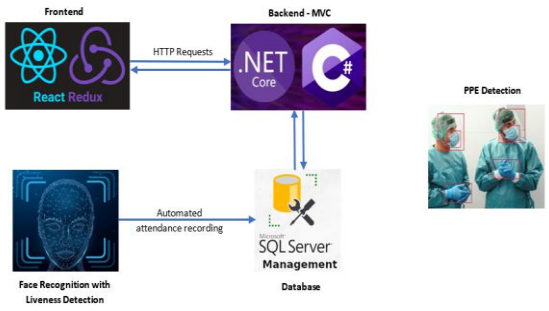

Fig. 1. System Architecture

IV. Experiments and Results

The SafeLABS system was evaluated by various experiments, focusing on face recognition accuracy with liveness detection, PPE detection performance, and web application usability. Experiments utilized custom datasets and real-time CCTV feeds.

A. Face Recognition Performance

Initial aim was to build custom Convolutional Neural Network (CNN) models from scratch for face recognition and then use transfer learning for greater performance. Different datasets were created with 100 and 500 training images belonging to 3 or 4 classes of faces in each and different preprocessing techniques were applied to them. After several attempts of building CNN models from scratch trained on those datasets were failed because of poor generalization and learning, a dataset of 700 training and 300 testing images per class (having 3 classes) was used for next experiments below. The images were extracted from high-quality video clips, preprocessed with MTCNN, and data augmentation was done.

- Custom CNN model was built and trained for 20 epochs with early stopping callback but still model was unable to generalize well. Resulting curves which are not smooth, are shown in Fig. 2.

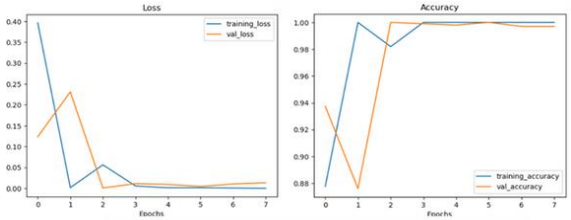

Fig. 2. Loss and Accuracy Curves for the New CNN Model

- Then a pre-trained ResNet50V2 model with feature extraction, trained for 30 epochs with augmentation and dropout, reduced training loss from 1.44 to 0.94 and validation loss from 1.35 to 0.76 (Fig. 3). Custom image recognition remained weak.

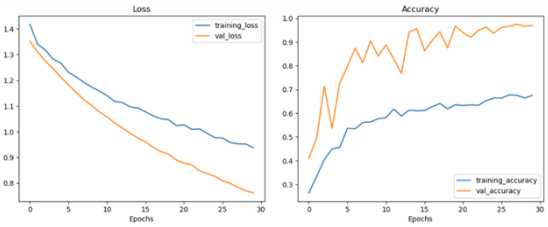

Fig. 3. Loss and Accuracy Curves for ResNet50V2 Model

- Pre-trained InceptionV3 model with feature extraction, trained for 20 epochs with augmentation, achieved 97% validation accuracy and 0.3 validation loss (Fig. 4), displaying better curves for loss and accuracy, recognizing 73.7% of 19 custom images, though retraining was needed for new users.

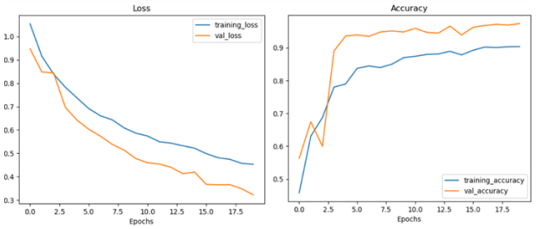

Fig. 1. Loss and Accuracy Curves for InceptionV3 Model

There were issues with these trained models including overfitting, lack of generalization and need for re-training the model when a new user registration happens. So, the solution was using a pre-trained face encoding generator model that do not require re-training the model. Below Fig. 5 shows comparison of considered pre-trained face encoding generator models.

Feature	face_recognition (dlib)	FaceNet	VGGFace	ArcFace
Accuracy (on LFW)	~97-99%	~99.63%	~97-98%	~99.83%
Speed	Fast with HOG Moderate with CNN	Moderate	Moderate	Slower
Architecture	ResNet-34	Inception - ResNet	VGG-16 / VGG-19	ResNet-50 / ResNet-100
Model Size	Small to Moderate	Moderate	Large	Large
Use Cases	Face recognition and verification, embedded applications	Face verification, clustering, embeddings generation	Face verification and classification	Face verification, high-accuracy face matching
Embedding Dimension	128	512	4096	512
Ease of Integration	High, easy with Python API	Moderate	Moderate to complex	Complex
Scalability	High, works with relational databases	Medium (best with specialized vector DBs)	Low	Low

Fig. 5. Comparison Between Face Encoding Generation Models

The face_recognition library built on top of Dlib library which contains HOG model for face detection and ResNet-34 model for 128-dimensional embeddings generation was used because of high accuracy, scalability, and ease of use. When a new user registers, face encodings were generated for his/her several face images and stored. Then in authentication process, live face's encodings needed to be compared with stored encodings using Euclidean distance method with the aid of OpenCV.

To enhance security, the MiniFASNetV2 model from Silent-Face-Anti-Spoofing [source: GitHub/minivision-ai] was integrated for anti-spoofing (liveness detection). This lightweight model uses a dual-branch architecture with Fourier spectrum supervision to distinguish real faces from fake media such as photos and screens, achieving 97.8% TPR and 1e-5 FPR in its APK tests. Its integration is critical to prevent spoofing attacks, ensuring reliable authentication in operational settings. When a person is at the entrance of the laboratory, and he/she passes both liveness detection and face verification, the attendance is automatically recorded into the database. Below figures (Fig. 6 to Fig. 8) show the results of testing the face recognition module with anti-spoofing integration.

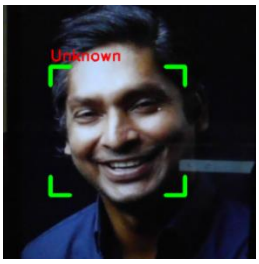

Fig. 6. Detecting an Unauthorized User (Before Integrating Liveness Detection)

Fig. 7. Detecting a Spoofing Attempt

Fig. 8. Granting Access for an Authorized User

B. PPE Detection Performance

After downloading the CPPE-5 dataset from https://huggingface.co, a custom script was used to convert it from COCO to YOLO format. Coverall, Face_Shield, Gloves, Goggles, and Mask are the five PPE classes for which the dataset was annotated. The dataset was divided into 700 training images and 329 validation images. The 640x640 pixel images were scaled, and the YOLO format (center coordinates, width, height) was applied to the bounding boxes. Using the Adam optimizer, the YOLOv8 nano model (yolov8n.pt) was trained on the dataset for 50 epochs with a batch size of 16. Although there are some misclassifications such as 0.33 of actual Face_Shields predicted as background, the normalized confusion matrix shown in Fig. 9 shows high true positive rates for Coverall (0.96), Face_Shield (0.94), Gloves (0.74), Goggles (0.81), and Mask (0.88). A test image for safety equipment (PPE) detection is shown in Fig. 10.

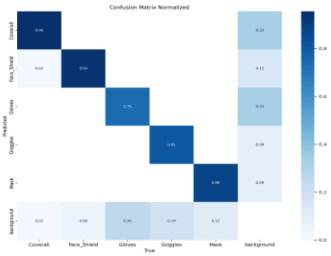

Fig. 9. Resulted Confusion Matrix

Fig. 10. Custom Test Image for PPE Detection

C. Web Application Usability

The web application was implemented using React-Redux for a responsive frontend and C# with .NET Core framework for backend APIs, following the Model-View-Controller (MVC) architecture. The database was maintained in Microsoft SQL Server Management Studio (MSSQL), and its tables including User, Attendance, Resource, ResourceType, Announcement, and ImageId were linked by foreign keys as necessary. Fig. 11 shows the database schema.

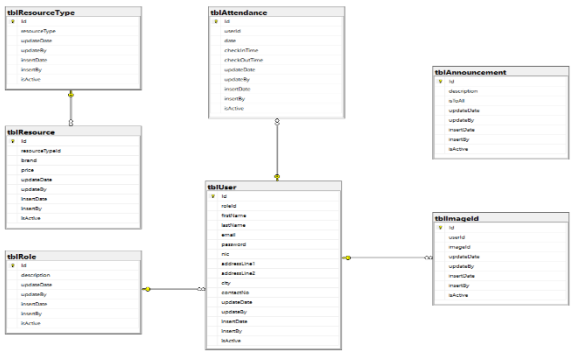

Fig. 11. Database Diagram

All core features of the web application including user and resource management, lab occupancy viewing, announcements section were implemented successfully with Insert, Update, Retrieve capabilities. Role-Based Access Control (RBAC) ensured Admins could manage users, announcements and resources, while other normal user roles such as Lab Assistants and Research Assistants had read-only access for certain operations. The Advanced Encryption Standard (AES) with a 256-bit key secured passwords and connection strings, with no breaches detected. Error handling in forms was implemented via client-side validation and

backend checks, reducing submission errors. User Interface screenshots (Fig. 12 to Fig. 24) demonstrate the intuitive interface of the web application.

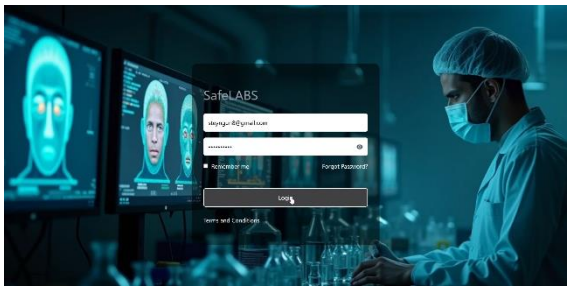

Fig. 12. Logging Page

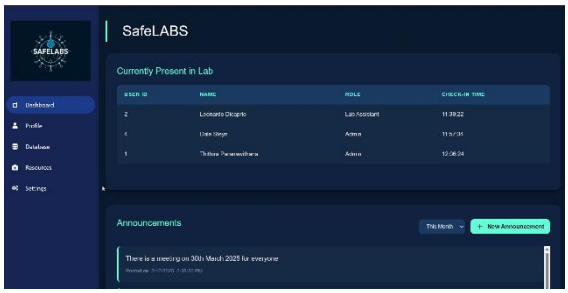

Fig. 13. Dashboard Page for Admin User

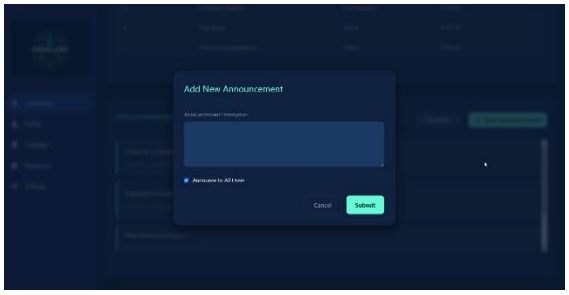

Fig. 14. Insert Announcement Window

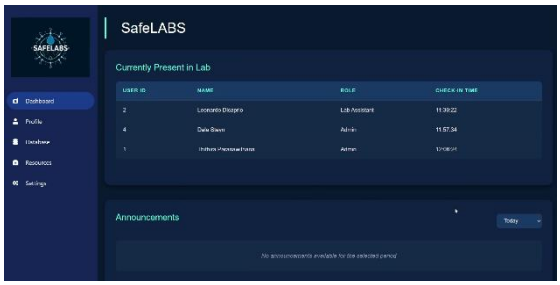

Fig. 15. Dashboard Page for Other Roles

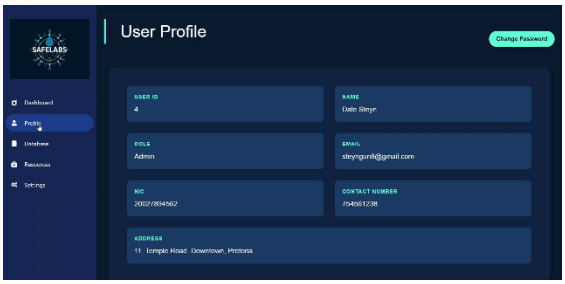

Fig. 16. Profile Page for All Users

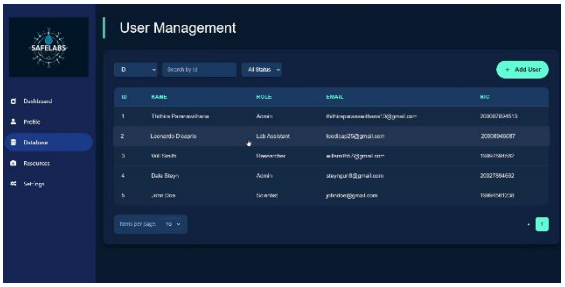

Fig. 17. User Database Page for Admin User

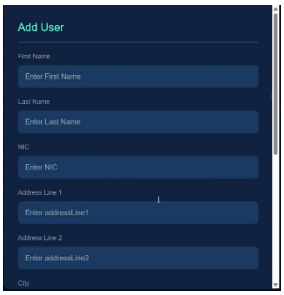

Fig. 18. Add User Window

Fig. 19. Update User Option

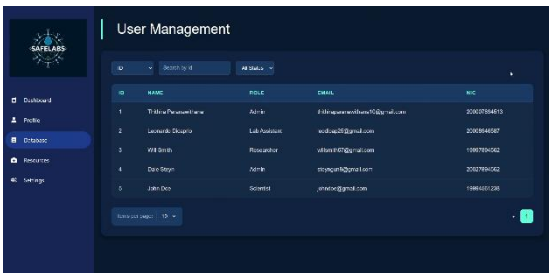

Fig. 20. User Database Page for Other Roles

Fig. 21. Resource Page for Admin User

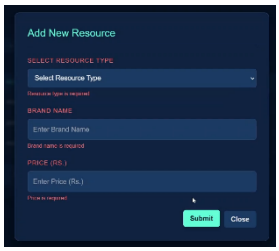

Fig. 22. Add New Resource

Fig. 23. Update Resource Option

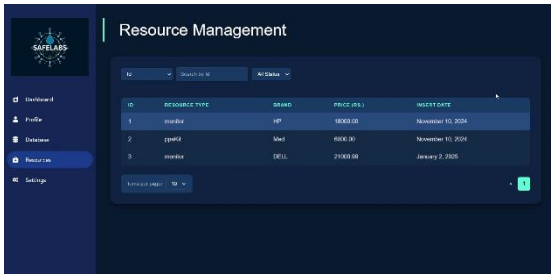

Fig. 24. Resource Page for Other Roles

V. Conclusion and Future Work

SafeLABS offers a comprehensive laboratory management system and efficiently automates laboratory authentication and safety compliance by integrating face recognition with liveness detection and a PPE detection model. This ensures secure access and adherence to safety protocols, even in the presence of challenges such as maintaining face recognition accuracy under changing lighting conditions, achieving a balance between security and user experience, managing complexity in the implementation of role-based access control, and seamlessly integrating multiple technologies. Comprehensive laboratory management is made possible by a web application, which supports scalability across many environments and allows for user management, resource tracking, real-time occupancy monitoring, and announcements.

Future improvements will concentrate on enhancing robustness and capabilities of SafeLABS system. Remote monitoring will be made possible by integrating IoT and cloud services, and user accessibility can be improved by creating a mobile application. Advanced data encryption techniques will better safeguard sensitive information, and adopting stronger anti-spoofing techniques will further increase security against fake authentication attempts. Furthermore, expanding the project's scope to include different environments, like industrial or educational institutions, would increase its applicability and guarantee that SafeLABS continues to be an effective and scalable solution for managing not just laboratories but also any other institutional environment.

References

[1] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Information Security,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, Jun. 2006, doi: https://doi.org/10.1109/tifs.2006.873653.

[2] R. V. Yampolskiy and V. Govindaraju, “Behavioural biometrics: a survey and classification,” International Journal of Biometrics, vol. 1, no. 1, p. 81, 2008, doi: https://doi.org/10.1504/ijbm.2008.018665.

[3] N. Woods and M. Siponen, “Too many passwords? How understanding our memory can increase password memorability,” International Journal of Human-Computer Studies, vol. 111, pp. 36–48, Mar. 2018, doi: https://doi.org/10.1016/j.ijhcs.2017.11.002.

[4] U. Jain, Mrunmayee Shirodkar, V. Sinha, and Bhushan Nemade, “Automated Attendance Management System using Face Recognition,” International Conference & Workshop on Emerging Trends in Technology, no. 2, pp. 23–28, May 2015.

[5] Y. Kim, J. Na, S. Yoon, and J. Yi, “Masked fake face detection using radiance measurements,” Journal of the Optical Society of America A, vol. 26, no. 4, p. 760, Mar. 2009, doi: https://doi.org/10.1364/josaa.26.000760.

[6] N. D. Nath, A. H. Behzadan, and S. G. Paal, “Deep learning for site safety: Real-time detection of personal protective equipment,” Automation in Construction, vol. 112, p. 103085, Apr. 2020, doi: https://doi.org/10.1016/j.autcon.2020.103085.

[7] P. J. Prasad and G. L. Bodhe, “Trends in laboratory information management system,” Chemometrics and Intelligent Laboratory Systems, vol. 118, pp. 187–192, Aug. 2012, doi: https://doi.org/10.1016/j.chemolab.2012.07.001.

[8] Q. CAI, “Face recognition algorithm based on supervised neighborhood preserving embedding,” Journal of Computer Applications, vol. 29, no. 12, pp. 3349–3351, Mar. 2010, doi: https://doi.org/10.3724/sp.j.1087.2009.03349.

[9] J. Hugging Face, “Hugging Face – On a mission to solve NLP, one commit at a time.,” huggingface.co, 2024. https://huggingface.co/

[10] Kaggle, “Kaggle: Your home for data science,” Kaggle.com, 2024. https://www.kaggle.com/

[11] TensorFlow, “API Documentation | TensorFlow Core v2.4.1,” TensorFlow. https://www.tensorflow.org/api_docs

[12] Mohamad Alansari, Oussama Abdul Hay, S. Javed, Abdulhadi Shoufan, Yahya Zweiri, and Naoufel Werghi, “GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations,” IEEE Access, vol. 11, pp. 35429 35446, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3266068.

[13] L. Blanger and A. R. Panisson, “A Face Recognition Library using Convolutional Neural Networks,” International Journal of Engineering Research and Science, vol. 3, no. 8, pp. 84–92, Aug. 2017, doi: https://doi.org/10.25125/engineering-journal-ijoer-aug-2017-25.

[14] A. Geitgey, “Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning,” Medium, Jul. 24, 2016. https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78

[15] computervisioneng, “Silent-Face-Anti-Spoofing/README_EN.md at master · computervisioneng/Silent-Face-Anti-Spoofing,” GitHub, 2022. https://github.com/computervisioneng/Silent-Face-Anti-Spoofing/blob/master/README_EN.md