Grenze International Journal of Engineering and Technology, June Issue

Integrating Zero Trust Architecture with Facial Recognition for Enhanced Security

Pappula Madhavi[1], Geethika Pallelapati[2], Ramisetty Siva Naga Lakshmi[3] and Lakkireddy Suma[4]
[1-4]Lakireddy Bali Reddy College of Engineering Mylavaram, Andhra Pradesh, India
Email: pappulamadhavi06@gmail.com, pallelapatigeethika@gmail.com, panduramisetty51@gmail.com, sumalakkireddy@gmail.com

***Abstract*— In an era where digital threats are escalating, traditional perimeter-based security frameworks cannot easily address the modern complexity of organizational needs. This project, "Integrating Zero Trust Architecture with Facial Recognition for Enhanced Security," implements a Zero Trust model boosted with facial recognition technology to ensure only authorized persons access sensitive data within an open collaborative environment. It uses the Haar Cascade and FaceNet algorithms in order to provide robust and dynamic identity verification, so allowing data sharing across a group while strictly keeping access files based on authorized facial matches. The hybrid of these Zero Trust principles with more advanced algorithms for facial recognition makes security even better by verifying user credentials but also ensuring the presence of authorized personnel for critical data interaction. The project does assuredly support in ensuring the safe and reliable maintenance of data confidentiality and integrity within collaborative organizational settings.**

***Index Terms*—Zero Trust Architecture, Facial Recognition, Haar Cascade, FaceNet, Identity Verification, Data Security, and Access Control, Collaborative Environment, Authentication, and Authorization, Confidentiality, Integrity.**

I. Introduction

As the threats become cyber, traditional models such as "Trust but Verify" have become outdated. Zero Trust Architecture assumes that by default no user or device is trustworthy and is gaining popularity due to strong access control and continuous authentication. This project propels the development of ZTA with facial recognition through Haar Cascade and FaceNet, verifying a person against templates of already registered users. The data shared is only accessible to authorized personnel, hence ensuring security, confidentiality, and integrity. By integrating Zero Trust principles with facial recognition-based authentication, this system prevents unauthorized access, even when credentials are compromised, thus offering a secure and reliable framework for managing sensitive data.

II. Literature Survey

We have studied various research papers related to our project from reputed journals and conferences such as IEEE and SCOPUS, which provided valuable insights into the technologies and algorithms required for implementation. Among these, Preetha Shivanna and Sheela Samudrala Venkatesiah (2024) proposed an approach for facial recognition that was compared with state-of-the-art methods. Their method, which integrates

Grenze ID: 01.GIJET.11.2.544

a Siamese network with biometric authentication, achieved an accuracy of 96.5%. The novelty of their research lies in the combination of these techniques to enhance security and recognition performance. Similarly, Brian C. Lovell, Abbas Bigdeli, and Sandra Mau (2022) focused on achieving real-time face recognition using embedded system technologies such as Robot Operating System (ROS), GPU acceleration, and smart algorithm design. Their system was tested in international airport trials, achieving an effective recognition rate of 91% (11/12) when identifying Persons of Interest (POIs) among thousands of passengers from multiple flights. These references provide a strong foundation for understanding how advanced facial recognition techniques and Zero Trust security models can be integrated to improve data security and identity verification in our project.

III. METHODLOGY

A. Model Representation

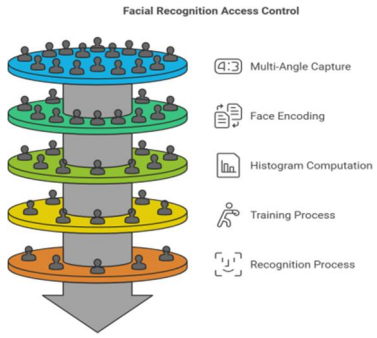

Fig. 1

Methodology describes the models that are used in our project and how they are useful while developing the project. Here are the methods used-

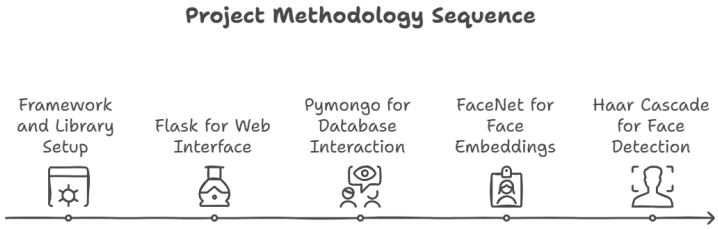

Fig. 2

B. Architecture

Framework and Library Setup

- Flask: Web application framework for handling HTTP requests and rendering HTML templates.
- Pymongo: Manages interactions with MongoDB for storing user data.
- FaceNet (Keras): Generates face embeddings for recognition.
- Haar Cascade (OpenCV): Detects faces in images for further processing.

User Registration and Management

- User details are stored in MongoDB.
- Each user captures 40 images for training.
- Session-based authentication manages logged-in users.

Photo Capture and Storage

- Users capture photos after registration.
- Each photo is sent to the server, decoded, and stored in a user-specific directory.
- The system triggers training after 40 images are collected.

Face Detection with Haar Cascade

- Haar Cascade scans images for facial patterns.

- Detected faces are cropped and prepared for embedding extraction.

Embedding Generation with FaceNet
- Faces are resized to 160x160 pixels and normalized.
- FaceNet generates embeddings (unique feature vectors) for each face.
- These embeddings are saved for future recognition.

Recognition Process
- Haar Cascade detects faces in uploaded images.
- FaceNet generates embeddings and compares them with stored data using Euclidean distance.
- Color histograms are used for additional matching accuracy.
- If similarity is within the threshold, the face is recognized; otherwise, labeled as "unknown".

Recognition Endpoint and Validation
- Users upload an image for recognition.
- If recognized, they access the homepage; otherwise, they are logged out.

Logging
- Logs track all processes for debugging and transparency.
- Errors in image processing, file handling, or model training are logged and handled efficiently.

IV. Dataset Information

A. Dataset and Preprocessing

The dataset consists of real-time images captured during user registration. Each user provides 40 images taken from multiple angles, including front, left, right, top, and bottom views, ensuring a comprehensive dataset for facial recognition. These images are preprocessed using Haar Cascade for face detection and FaceNet for feature extraction, making the system robust against variations in pose and lighting conditions.

B. Methodology - Data Collection

To improve recognition accuracy, the system captures real-time facial images from users in all directions during the registration phase. This includes images from frontal, side (left and right), and tilted (top and bottom) views to ensure that the model learns a diverse set of facial features. These images are stored in MongoDB and later used for authentication, enhancing the accuracy and reliability of the Zero Trust-based security model.

V. Results

Fig 3.Web Interface

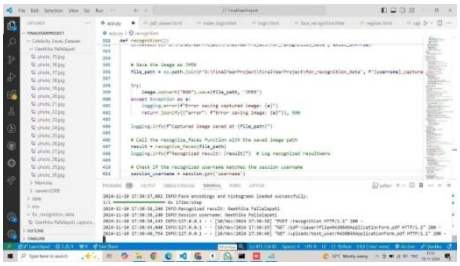

Fig 4.Face Encoding

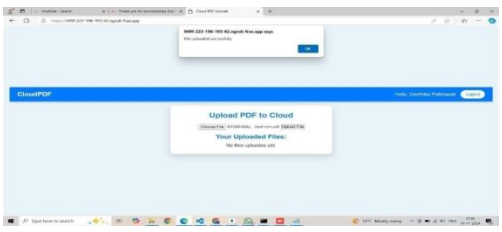

Fig 5. File Transferring

Fig 6. Recognition Process

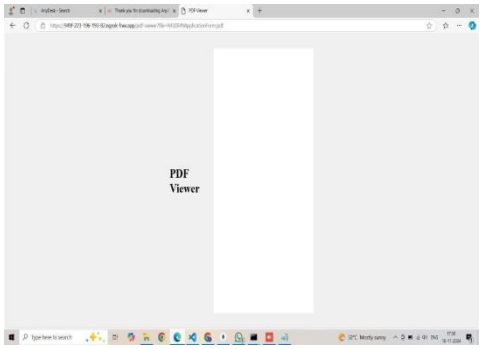

Fig 7.Training Process

Fig 8.Output Page

VI. CONCLUSION

This project enhances secure file access within an organization by using face recognition as a biometric login method, alongside username and email, instead of passwords. This approach ensures that sensitive files are accessible only to authorized personnel, significantly strengthening security. The face recognition feature provides a user-friendly, hands-free authentication process, reducing the risk of unauthorized access while streamlining login. By replacing traditional passwords with face recognition, the system offers both convenience and enhanced security, making it ideal for protecting confidential data in an organizational setting.

This project integrates a multi-factor authentication system that combines username, email, and face recognition to prevent unauthorized access. By eliminating passwords, it mitigates common security risks like password theft or reuse. Face recognition not only adds a reliable layer of security but also improves user experience with a seamless login process. This innovative solution highlights the potential of biometrics in secure applications, especially where data confidentiality is crucial. Overall, the system sets a new standard for secure, efficient access control in organizational environments.

REFERENCES

[1] Lake, B., Salakhutdinov, R., Gross, J., Tenenbaum, J. (2011). One shot learning of simple visual concepts. In Proceedings of the Annual Meeting of the Cognitive Science Society, 33(33): 2568-2573.

[2] Li, F.F., Fergus, R., Perona, P. (2006). One-shot learning of object categories. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(4): 594-611. https://doi.org/10.1109/TPAMI.2006.79

[3] Palatucci, M., Pomerleau, D., Hinton, G.E., Mitchell, T.M. (2009). Zero-shot learning with semantic output codes. Advances in Neural Information Processing Systems, 22.

[4] Bromley, J., Guyon, I., LeCun, Y., Säckinger, E., Shah, R. (1993). Signature verification using a "Siamese" time delay neural network. Advances in Neural Information Processing Systems, 6.

[5] Koch, G., Zemel, R., Salakhutdinov, R. (2015). Siamese neural networks for one-shot image recognition. ICML Deep Learning Workshop, 2(1).

[6] Taigman, Y., Yang, M., Ranzato, M.A., Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Columbus, OH, USA. pp. https://doi.org/10.1109/CVPR.2014.220 1701-1708.

[7] Bengio, Y. (2009). Learning deep architectures for AI.Foundations and trends®in Machine Learning,2(1):1 127. http://doi.org/10.1561/2200000006

[8] Krizhevsky, A., Sutskever, I., Hinton, G.E. (2017). ImageNet classification with deep convolutional neural networks. Communications of the ACM, 60(6): 84-90. https://doi.org/10.1145/3065386