IOT BASED SMART SECURITY SOLUTION FOR UNIQUE AUTHENTICATION

Mili (RA1911004010072), Samarpan (RA1911004010074), Matura (RA1911004010113)

Project Guide : Mrs. A. Bhavani

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur

Introduction

There exist many kinds of smart home lock systems such as keypad lock systems where a code is punched in and access is provided if the code is correct, or the voice recognition lock system, there still is scope to potentially enhance these security solutions. Having two factor authentication ensures a better approach to providing a smarter solution for user authentication. The aim of this project is to develop a model that includes fingerprint and face recognition for authentication purposes.

Problem Statement

Real-world worries about the safety of material assets. However, the existing models have issues such as forgotten pin, carrying a physical device which could be lost. Our two factor authentication system irradiates the need to carry any physical chip, thus reducing chances of human error.

Objective

- To create a database and system for user registration and implement a hardware setup to capture face and fingerprint image of the guest.
- To implement a software system to match the captured details with existing details of the user.
- To write and test machine learning and deep learning models to check which performs best for the dataset.

Realistic Constraints

- The user has to be within 12 to 24 inches from the camera module for best capturing of the image.
- The surrounding has to be fairly lit.
- The finger from where the fingerprint is supposed to be taken has to be dry and the environment should preferably be damp free

Methodology

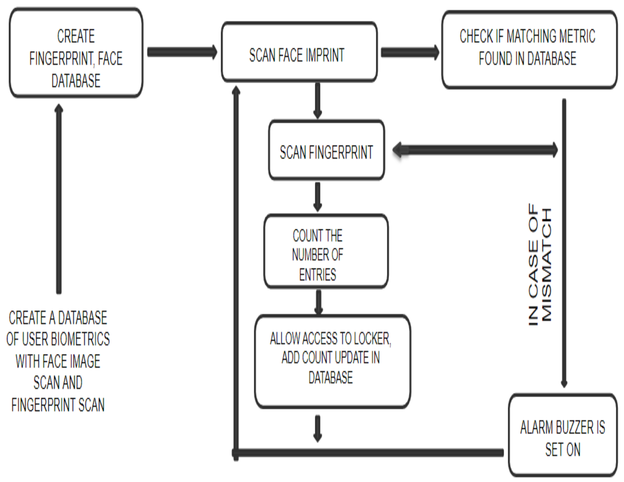
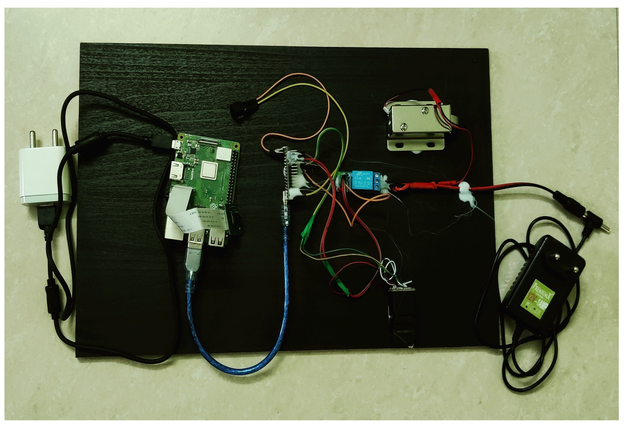


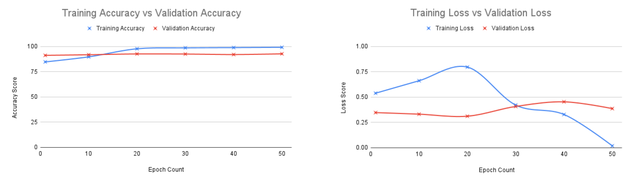
Fig. 1: Proposed Workflow

Hardware Setup

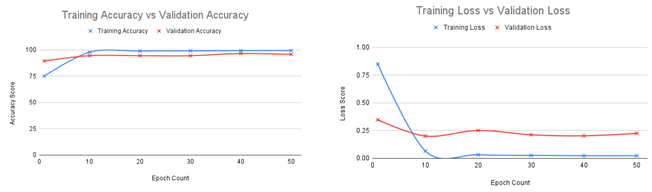


Results

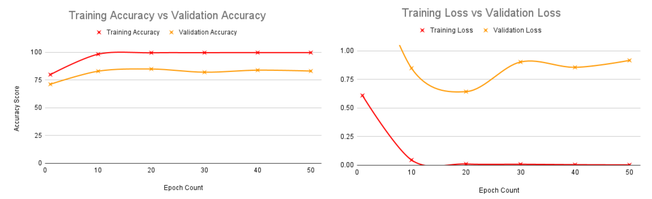
Loss and Accuracy comparison for Inception Neural Network V1



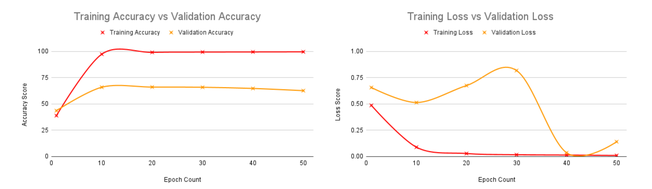
Loss and Accuracy comparison for Inception Neural Network V2



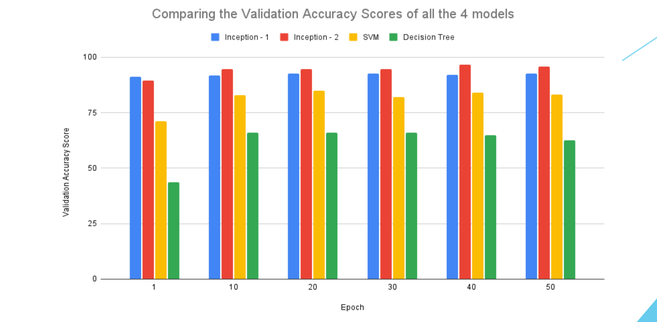
Loss and Accuracy comparison for SVM



Loss and Accuracy comparison for Decision Tree



Comparing validation accuracy of all 4 models



Conclusion

The expected output is after the face image of the user is taken as an input, if it matches with the database, then the fingerprint will be sensed and if a match is found, the lock will be unlocked. If not then the buzzer would go off. The efficiency and the accuracy of the machine learning and deep learning model is also tested

References

• W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

• K. Umamaheswari and P. Mahitha, "Smart security system for door access based on unique authentication," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1474-1477, doi: 10.1109/I-SMAC52330.2021.9640855.

Conference /Journal Publication

The research paper is being presented after being accepted by the **ICREACT 2023** - the International Conference on Research in Electronics Engineering and Communication Techniques, that was held on 3rd of May, 2023.