A PRELIMENERY REPORT ON

" Machine learning based security system for office premises "

SUBMITTED TO THE SAVITRIBAI PHULE UNIVERSITY, PUNE
IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF
BACHELOR OF ENGINEERING (COMPUTER ENGINEERING)

SUBMITTED BY

Megha Patil	Exam No. 46
Siddharth Nilakhe	Exam No. 39
Mehul ingale	Exam No. 19
E Navaneet kumar	Exam No. 11

DEPARTMENT OF COMPUTER ENGINEERING

ALL INDIA SHRI SHIVAJI MEOMRIAL SOCIETY'S
INSTITUTE OF INFORMATION TECHNOLOGY
KENNEDY ROAD, NEAR R.T.O. PUNE-411001

SAVITRIBAI PULE PUNE UNIVERSITY

2020-2021

CERTIFICATE

This is to certify that the project report entitles

"Machine learning based security system for office premises"

Submitted by

Megha Patil	Exam No. 46
Siddharth Nilakhe	Exam No. 39
Mehul ingale	Exam No. 19
E Navaneet kumar	Exam No. 11

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of **Mrs. Minal Nerkar** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degrees of **Bachelor of Engineering** (Computer Engineering).

(Mrs. Minal Nerkar)
Guide
Department of Computer Engineering

(Dr. S.N. Zaware)
Head
Department of Computer Engineering

(Dr. P.B. Mane)
Principal
AISSMS Institute of Information Technology, Pune-411001

Place: PUNE
Date:

ACKNOWLEDGMENT

It gives us immense pleasure in presenting the project report on **"Machine learning based security system for office premises"** The success and the outcome of this report required a lot of guidance. We are very grateful to our guide **Mrs. Minal Nerkar** who has provided expertise and encouragement. We thank sir who provided vision and knowledge that was very helpful throughout the research. All that we have done is only due to the great guidance. We also express our gratitude to **Dr. S.N. Zaware** Head of Computer Engineering Department, AISSMS's Institute of Information Technology, for the valuable support.

We would also like to extend our sincere thanks to Principal Dr.P.B. Mane, for his dynamic and valuable guidance throughout the project and providing the necessary facilities that helped us to complete our dissertation work.

Megha Patil
Siddharth Nilakhe
Mehul ingale
E Navaneet kumar

ABSTRACT

Safety plays a major role in today's world. User authentication, i.e., a procedure to verify the identity of the user, is essential in the digital world so as to protect the user's personal data stored online (e.g. online bank accounts) and on personal devices (e.g., smart phones, laptops) and to also enable customized services in smart spaces (e.g., adjusting room temperature etc.). Recently, traditional authentication mechanisms (e.g., passwords or fingerprints) have been repeatedly shown to be vulnerable to subversion. Researchers thus have proposed numerous new mechanisms to authenticate the users in the aforementioned scenarios. At offices and work places as well, this user authentication is of utmost importance in order to avoid any mal-practices if any as well as to maintain individual work privacy in the organization. This project aims at developing a user authentication system for offices based on their company generated login ID and passwords, One-Time-Password (OTP) generation and face recognition. The system also has features such as auto-saving data to server and auto-logout.

TABLE OF CONTENTS

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

1.1 Overview

The authentication, confidentiality and privacy of data is needed in today's world. The smart devices, like smart phones and sensing nodes, are now developing an emerging global and Internet-based information service platform called the Internet of Things (IoT). Generally, the IoT architecture is based on some existing data communication tools, which could range from RFID (Radio Frequency Identification) -tagged products to complex computational items. Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed. Direct interaction of smart devices within the immediate living space of humans intimidates new security vulnerabilities. Research has been led in developing customized tools for computer security to establish confidentiality, integrity and availability. In case of any kind of security failure, our system provides the users data fully data security and assurance of privacy. The aim is to prevention system that is adaptive and receptive to new threats and provides more control of owner on the data stored on system by restricting the access to particular user for specific file with limited rights. The idea behind it to create software that will protect the data from all kinds of attacks and maintain entire confidentiality of the data.

1.2 Motivation

Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing three tier authentications which are login credentials, face Recognition scanner and OTP. The proposed methodology provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information.

1.3 Problem Definition and Objectives

Access control is the act of providing privacy to a resource, and authentication through a single factor is no longer reliable to provide robust protection against

unauthorized access. Hence, there is a rapid growth of exploring novel multi-factor authentication methods which combine two or more authentication factors.Out of the maximum authentication methods mentioned above, combination of Login Id and password, one-time password (OTP) and face recognition have proven to be the best. Accordingly, a system is designed using these three authentication techniques that will efficiently provide/block the login access.

1.4 Project Scope and Limitations

The project is mainly developed for offices / organizations wherein the work/data of every working individual employee will be kept secured and personal so as to avoid any malpractices or misplacing of any data of the fellow colleagues. For improved security, it is always advisable to use more than one factor for authentication completion. It can also be extended for home security and cyber security systems with necessary specification changes if any. The designed project is flexible having no restrictions on use of specific device. Irrespective of any device used for login, the system will work efficiently as planned and designed.

The system may require time for writing the accurate labelling functions. Manual intervention is required for testing the model. Accuracy for multi-class labelling is comparatively less efficient.

1.5 Methodologies of Problem Solving

System is consists of a three-step secure authentication process for working employees in their respective organizations. As stated above, at first the user needs to enter the unique login Id and password combination provided to them by the company. Once that matches with the database, next step is to generate the OTP on the registered mobile number. If not, further access to login into the system will be denied. If correct generated OTP is entered into the system, the user moves second step ahead to gain access to the system. Once this is done, next comes the face recognition. With the help of webcams present with each and every system, the face in front of cam is detected. A live image is captured automatically through a webcam installed on the device, which is compared with the image stored in the database. If this image matches, user can get the access to operate that particular system.

Haar Cascade Classifier is used to implement face recognition. An additional feature of autosave and auto-logout is also included in this system. Suppose the

employee happens to leave their desk due to some reasons, the webcam will be continuously detecting and capturing the images if any. Incase an unknown face image other than that system user, is captured by the webcam, the whole work/data will be automatically saved to the company's server and the system will automatically logout, so that, the unknown user cannot make any manipulations in the users work. The autosave feature helps the user to re-continue the work form the point he/she had left it. Hence a very efficient, safe and reliable system is developed.

CHAPTER 2

LITERATURE SURVEY

1. **Effective Authentication for Restricing Unauthorized User**
   There has been a use of three tire architecture in paper "Effective Authentication For Restricing Unauthorized User", [1] for providing security to the system. Those tiers are Facial recognition, Fingerprint Scanning and OTP. All these tiers give a great strength to security of system. Incase if there is an attack on system, the measures are provided so as to not leak the important data from the system. By using AES 512 all the data is encrypted which can only be decrypted by a specific key

2. **Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey**
   The security and protection of such personal information are becoming more and more important since mobile devices are vulnerable to unauthorized access or theft. User authentication is a task of paramount importance that grants access to legitimate users at the point-of-entry and continuously through the usage session. This task is made possible with today's smartphones' embedded sensors that enable continuous and implicit user authentication by capturing behavioral biometrics and traits. In [2], Mohammed Abuhamad et al surveyed more than 140 recent behavioral biometric-based approaches for continuous user authentication, including motionbased methods, gait-based methods, keystroke dynamics-based methods, touch gesture-based methods, voice-based methods (16 studies), and multimodal-based methods. The survey provides an overview of the current state-of-the-art approaches for continuous user authentication using behavioral biometrics captured by smartphones' embedded sensors, including insights and open challenges for adoption, usability, and performance.

3. **A Multimodal Biometric User Verification System with Identical Twin using SVM**
   Biometric authentication of an individual through their own characteristics is the most common way to identify a person. In [3], a multimodal biometric user verification system with identical twin shows the fingerprint, face and lip classification model using SVM2 with kernel functions is efficient and promising. It would be seen from the results that the FRR is less than that of FAR.

4. **Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data**

Paper "Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data "[4] analyzes the performance of combining the use of on-line signature and fingerprint authentication to perform robust user authentication. Signatures are verified using the dynamic time warping (DTW) technique of string matching. The proposed minutiae-based matching algorithm, stores merely a small number of minutiae points, which greatly reduces the storage requirement with the help of phase correlation. Here, matching score level fusion is used by applying weighted sum rule for the biometric fusion process. To improve the authentication performance, deep learning classifier is proposed in this work for multi-biometrics authentication. When a biometric authentication request is submitted, the proposed authentication system uses deep learning to automatically select an appropriate matching image. In the experiment, biometric authentication was performed on healthcare in the UCI database. Multi -Biometric Authentication was used during the authentication stage.

5. **Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm**
   Presently a-days Cloud registering is rising field in light of its Performance, high accessibility, easily. Information store is principle future that cloud benefit gives to the huge association to store tremendous measure of information. Yet at the same time numerous associations are not prepared to execute distributed computing innovation since absence of security. So the principle goal of [5] is to understand the security issues and to anticipate unapproved access in distributed storage, it should be possible with the assistance of an effective validation strategy by utilizing cross breed verification calculation to give security of the information in cloud and guarantee amending code to keep up the nature of administration. In any case, solid client confirmation that confines illicit access to the administration giving servers is the foremost prerequisite for securing cloud condition

6. **On keystrokes as Continuous User Biometric Authentication**
   Authentication of a user through an ID and password is generally done at the start of a session. But the continuous authentication system observes the genuineness of the user throughout the entire session, and not at login only. In [6], Suhail Javed Quraishi and Sarabjeet Singh Bedi proposed the usage of keystroke dynamics as biometric trait for continuous user authentication

in desktop platform. Biometric Authentication involves mainly three phases named as enrollment phase, verification phase and identification phase. The identification phase marks the accessed user as an authenticated only if the input pattern matches with the profile pattern otherwise the system is logout. The proposed Continuous User Biometric Authentication (CUBA) System is based on free text input from keyboard. There is no restriction on input data during Enrolment, Verification, and Identification phase. Unsupervised One-class Support Vector Machine is used to classify the authenticated user's input from all the other inputs. This continuous authentication system can be used in many areas like in Un-proctored online examination systems, Intrusion Fraud Detection Systems, Areas where user alertness is required for entire period e.g. Controlling Air Traffic etc.

7. **A Robust e-Invigilation System Employing Multimodal Biometric Authentication**

   The significant growth in users of e-learning technologies and their use in courses have given rise to a major concern over protecting them from misuse; a significant concern is that of the potential for cheating or illicit assistance during online examinations. Paper "A Robust e-Invigilation System Employing Multimodal Biometric Authentication", presents the development of robust, flexible, transparent and continuous authentication mechanism for e-assessments. To monitor the exam taker and ensure that only the legitimate student is taking the exam, the system offers a continuous user identification employing multimodal biometrics; a security layer using an eye tracker to record the student's eye movement; and, speech recognition to detect inappropriate communication. The focus of [7] in particular is the development and evaluation of 3D facial authentication. An experiment has been conducted to investigate the ability of the proposed platform to detect any cheating attempts. During the experiment, participants' biometric data, eye movement, and head movements have been collected using custom software. The 3D camera also captured the session using a built-in microphone and the system recognized speech (employing a speech recognition algorithm). 51 participants participated in this experiment. The FRR of all legitimate participants was 0 and 0.0063 in 2D and 3D facial recognition modes respectively. Furthermore, three participants were tasked with a series of eight scenarios that map to typical misuse. The results of the FAR and FRR of five of these threat scenarios in both 2D and 3D mode were 0

with two cases exhibiting an FAR of 0.11 and 0.076 in the 2D mode.

8. **EFFECTIVE AUTHENTICATION FOR AVOIDING UNAUTHORIZED USER ACCESS**
   Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing two tier authentications which are Irish Recognition scanner and OTP. The proposed methodology in [8] provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources. To overcome these drawbacks, the AES 256 algorithm will be introduced after our one-time password authentication protocol. Thus the proposed system is more secured and can be provide effective authentication.

9. **Modified Role Based Access Control Model For Data Security**
   Paper "Effective Authentication for Avoiding Unauthorized User Access", presented a modified Role Based Access Control model by extending traditional role based access control in SQL (Structure Query Language) data storage. The said model evaluates and executes security policies which contain versatile access conditions against the dynamic nature of data. The goal of [9] is to devise a mechanism for a forward looking, assertive yet flexible security features to regulate access to data in the data storage that is devoid of rigid structures and consistency. This is achieved by integrating roles and authenticated fine-grained access rules and implemented through effective audit trail. The model and the rules used are presented and show that when implemented, it is capable of outperforming existing models that are role based.

10. **A SECURITY BY BIOMETRIC AUTHENTICATION**
    Paper [10] presented a state of art about biometric hand, different techniques used. Biometric is essentially used to avoid risks of password easy to find or Stoll; with as slogan save Time and Attendance. BIOMETRICS is the mea-

surement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing biometric techniques but also present detailed of representative methods within each category. Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices. Although many technologies fit in the biometric space, each works a bit differently. Relatively new on the biometric scene, face recognition devices use PC-attached cameras to record facial geometry. Once the biometric data is collected, it is encrypted and stored–locally, in the case of the desktop-only products; in a central database for the network solutions. When a user tries to log on, the software compares the incoming biometric data against the stored data.

CHAPTER 3

SOFTWARE REQUIREMENTS SPECIFICATION

3.1 Assumptions and Dependencies

Assumptions

1. It is assume perfect working conditions with min 2 GB RAM and above 1GHz speed
2. Probability chosen is the best using the loss function

. **Dependencies**
Numpy, Scikit-Learn.

3.2 Functional Requirements

3.2.1 System Feature 1

Functional requirements of the system are the functions or modules implemented in the entire system. In our system the various modules are being implemented for processing the input dataset. The input to the system is the unlabelled dataset and this dataset is being processed to generate the labelled dataset automatically.

Modular Flow Of Computations Of Functions:

1. Accepting the unlabelled dataset from the end user.
2. Preprocessing the dataset to avoid the noisy data if available.
3. Computing the scores based on the data points of the input.
4. Passing the input through the CNN layers (intermediate layer).
5. Extracting the prototype.
6. Generate a class inference graph.
7. Expect the output as the labelled dataset with accuracy measures if prominent

The system requires the functions to be written initially by the domain experts in order to have the correct results . The system is initially trained with the dataset provided and later the prediction is done for generating the similar labels.

3.3 External Interface Requirements

3.3.1 User Interfaces

1. The system will interact with the user using a GUI that would be built using php.

2. Backend manipulations will be done with the help of python.

3.4 Non Functional Requirements

3.4.1 Performance Requirements

Accuracy of the proposed system is better than the previous data programming paradigms such as snorkel model. The end user has to just feed the data once the system and the entire further process is automated. No manual intervention after training the data is demended.

3.4.2 Safety Requirements

In case of the damage to the dataset another copy of the dataset is being stored at the hard disk. The output of every module is being saved. If there is extensive damage to the system the reconstruction of the states is being done.

3.4.3 Security Requirements

The images (input data) is already being preprocessed before being manipulated by the system , this eliminates the noisy data from the input dataset leading to better accuracy. The intermediate layer of CNN is being used so that interprets close enough to the realistic human encoding techniques.

3.4.4 Software Quality Attributes

1. Correctness The correctness of the system depends on the accuracy and the probabilistic labels generated. If the labels are accurate according to the prototype then the system has achieved its correctness to the maximum level.

2. Reliability: The system is reliable because every module has its reconstruction and recoding possible multiple times.

3. **Robustness** The system is robust enough to perform preprocessing and manipulations over large datasets. Compatible with different operating systems.

4. **Maintainability** it depends on the following factors:

   (a) **readability** The dataset is readable even if not the preprocessing is being done to reduce the noise in the system.

   (b) **Extensibility** The dataset can be of variables size from kilobytes, megabytes to gigabytes. The system is capable of performing computations on small, medium and large datasets.

   (c) **Testability** Generation of the correct labels leads to the development of the correct test cases and test plans for future testing.

5. **Efficiency** Higher the GPU, CPU and the RAM processing higher is the efficiency. The efficiency also depends on the quality of the input data.

6. **Availability** The input dataset must be available in the segregated manner so that its easy to manipulate.

7. **Usability** system is easy to handle, it also navigates in expected way with minimum delays. In such case the system reacts accordingly and transverses quickly between its states.

3.5 System Requirements

3.5.1 Software Requirements(Platform Choice)

1. **Scikit-learn:** It's a machine learning open source library supporting support vector machine. Regression and clustering via clubbing similar objects together.

2. **OpenCV**

3.5.2 Hardware Requirements

1. **Disk Space:** Minimum disk space of 500 GB is expected for computations and storage means.

2. **Processor**i5 CPU @1.60 GHz 1.80 GHz, 32-bit x32 OR 64-bit x64 processor is preferable.

3. **Memory:** 4 GB RAM and above , .

4. **Display:** 1600 * 900 minimum display resolution for better display

3.6 Analysis Models: SDLC Model to be applied

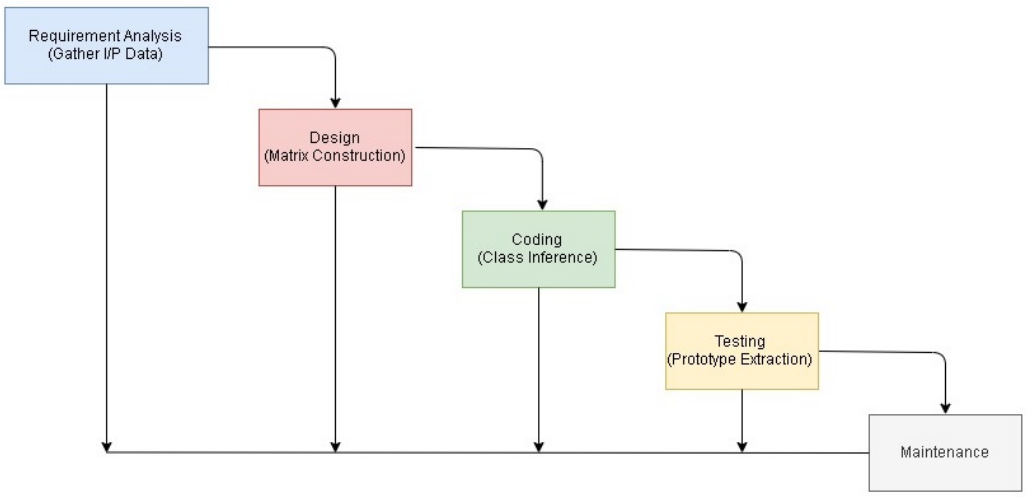


Figure 3.1: Waterfall Model

SDCL Waterfall model is being depicted by our system.

- The initial stage is requirement analysis stage here the data is being gathered which is to be provided as an input to the system.
- Second stage is the design stage where all the data is being formatted into a particular matrix. The scores are used to generate the matrix.
- Third stage is the coding stage in which the system performs its main functionality of mapping of the classes and getting the exact prototype.
- Testing is done in the fourth phase inorder to test the image with the probabilistic label.
- In the maintenance phase it's the last phase wherein the system has to depict and maintain the probabilistic labels of the respective images.

3.7 System Implementation Plan

In the system plan implementation the input is the unlabelled dataset that comprises of images, text or the tabular data. This being then given to the Chanel of the CNN inorder to produce the prototype of the image. This prototype is being then given to the system inorder to generate the matrix and further the class inference. Output then generated are the probabilistic labels to the unlabeled images.

Table 3.1: System Implementation Plan

SR NO	DURATION	ACTIVITY PERFORMED
1	July second week	Topic Finalization
2	3rd and 4th week of July	Understanding of Base Paper
3	1st and 2nd week of August	Literature Survey
4	3rd and 4th week of August	System Architecture Design Completion
5	1stand 2nd week of September	1st review Completed
6	3rd and 4th week of September	2nd review Completed
7	1st week of October	UML diagrams, State Charts and DFD's Completed
8	2nd week of October	3rd Review Completed
9	3rd and 4th week of October	Final review completed
10	November	Exam
11	December second week	Distribution of implementation modules
12	January	Project implementation in modules
13	February	Development of the entire module
14	March	Testing of the project
15	April first week	Final Report Submission

CHAPTER 4

SYSTEM DESIGN

4.1 System Architecture

A face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely. Fig 1 illustrates the system architecture of proposed system. It consists of a three-step secure authentication process for working employees in their respective organizations.

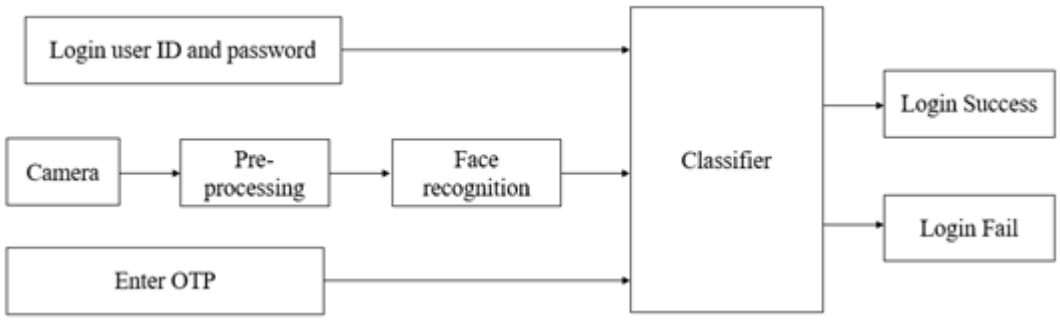


Figure 4.1: System Architecture of Proposed System

As stated above, at first the user needs to enter the unique login Id and password combination provided to them by the company. Once that matches with the database, next step is to generate the OTP on the registered mobile number. If not, further access to login into the system will be denied. If correct generated OTP is entered into the system, the user moves second step ahead to gain access to the system. Once this is done, next comes the face recognition. With the help of webcams present with each and every system, the face in front of cam is detected. A live image is captured automatically through a webcam installed on the device, which is compared with the image stored in the database. If this image matches, user can get the access to operate that particular system. Haar Cascade Classifier is used to implement face recognition. An additional feature of autosave and auto-logout is also included in this system. Suppose the employee happens to leave their desk due to some reasons, the webcam will be continuously detecting and capturing the images if any. Incase an unknown face image other than that system user, is captured by the webcam, the whole work/data will be automatically saved to the company's server and the system will automatically logout, so that, the unknown user cannot make any manipulations in the users work. The autosave feature helps the user to re-continue the work form the point

he/she had left it. Hence a very efficient, safe and reliable system is developed.

4.2 Data Flow Diagrams

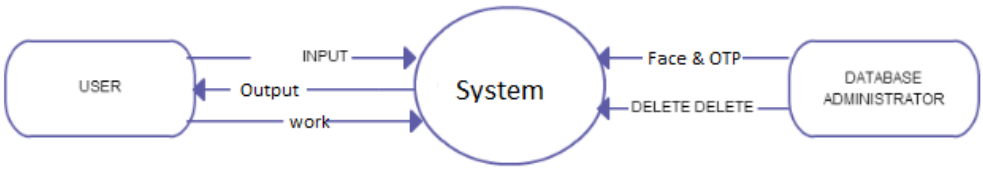


Figure 4.2: DFD Level 0

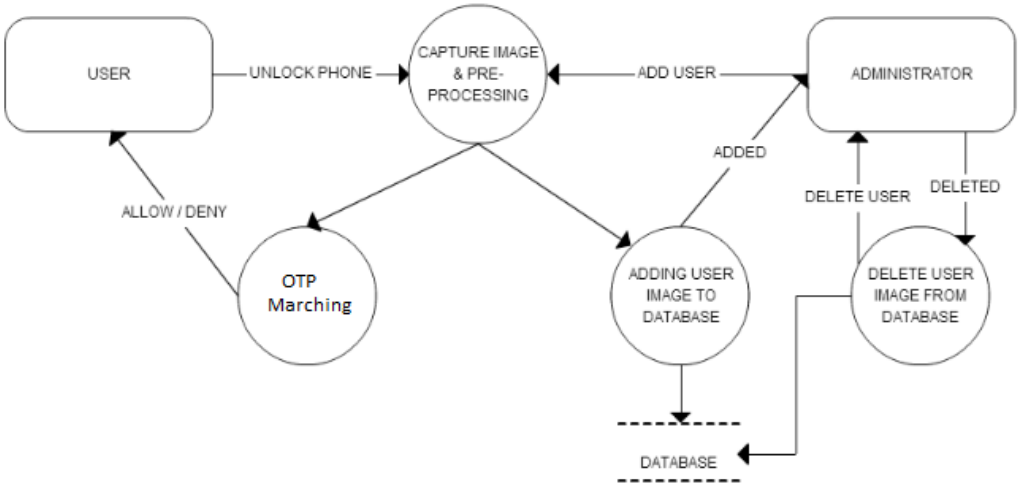


Figure 4.3: DFD Level 1

4.3 UML Diagrams

Class Diagram

The class diagram is used for representing the entire system in the classes having attributes and functionalities.

- They include the entities as the classes.
- Class contains the attributes and the functions.
- User, System and Activity are the classes representing their different variables and functions used.
- The user uses the attributes like the image, text, tabular format data.

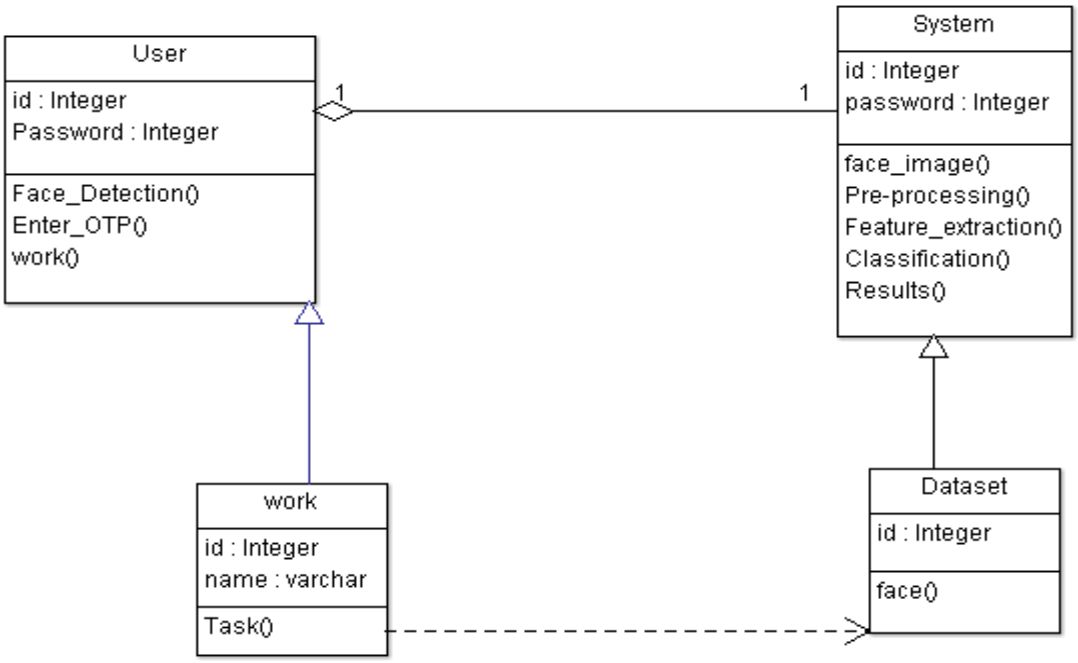


Figure 4.4: Class Diagram

- The system uses the functionalities like matrix construction() and the construction of the class inference().

Activity Diagram

- Activity Diagram is a behavioral diagram presenting the actors their functions performed.
- They also include the swim lanes and the forks and joins.
- The represent the individual lane as their entire activities and the functionality carried out by that particular actor in the respective lanes.
- Input is being provided by the user and the output is being given back to the user.

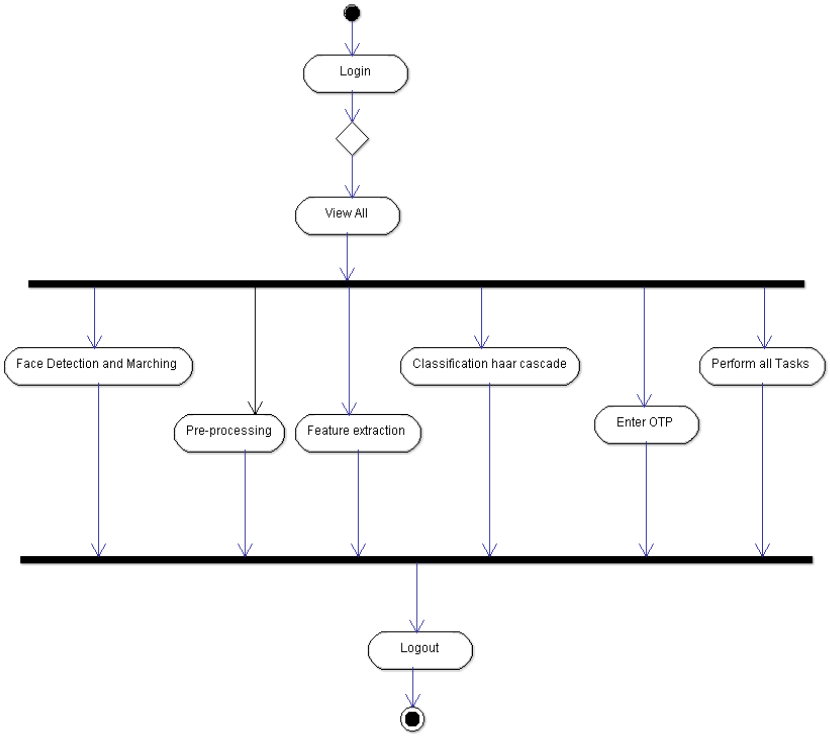


Figure 4.5: Activity Diagram

State Diagram

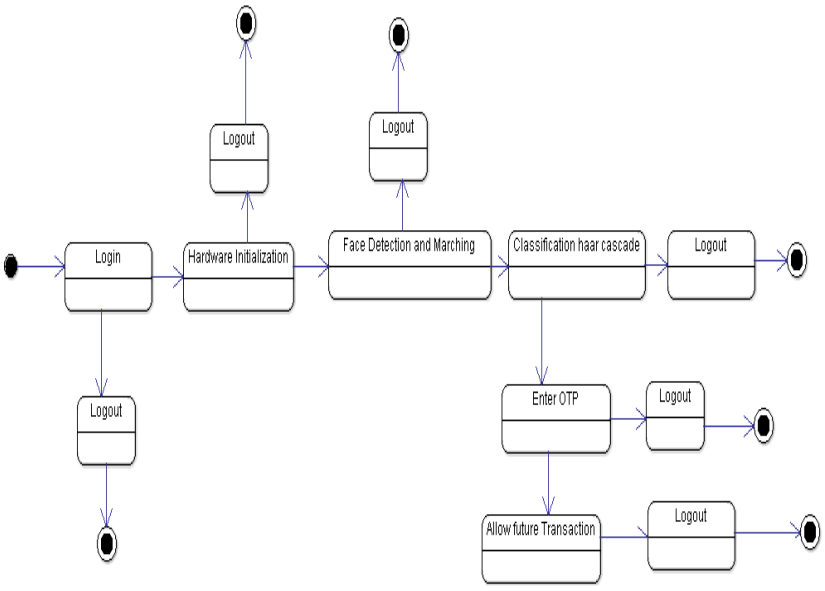


Figure 4.6: State Diagram

- Indicating the different states of the system along with inputs given conditions.

- Input is the unlabelled dataset to the initial state.
- Output of the system is the probabilistic label.
- The system is in the on state after the input data is given to the matrix construction phase.
- The input for every state is the output of the previous state .
- The system is ideal only when the input data is accepted by the system after that the system is on state.

Sequence Diagram

- **Actors**
    1. User
    2. System
    3. Activity
- Different roles played by the different actors are been specified separately in their individual lanes.
- Each actor has number of timelines for the activity (Function) to be preformed.

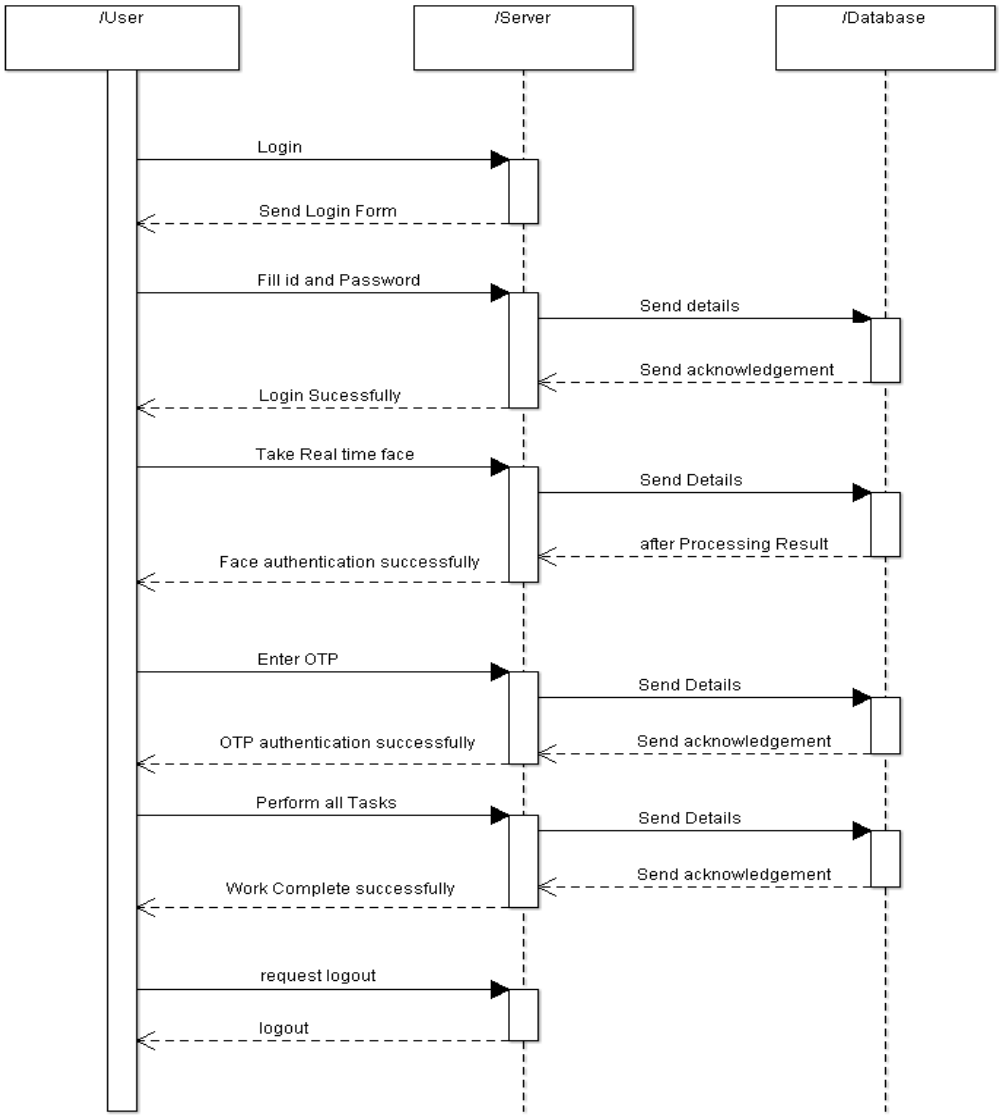


Figure 4.7: Sequence Diagram

Use case Diagram

Use Case diagram is used for representing the problem statement that is the actors in it, their functionality in an behavioral manner. They are useful when the system is to be in the programmatic execution.

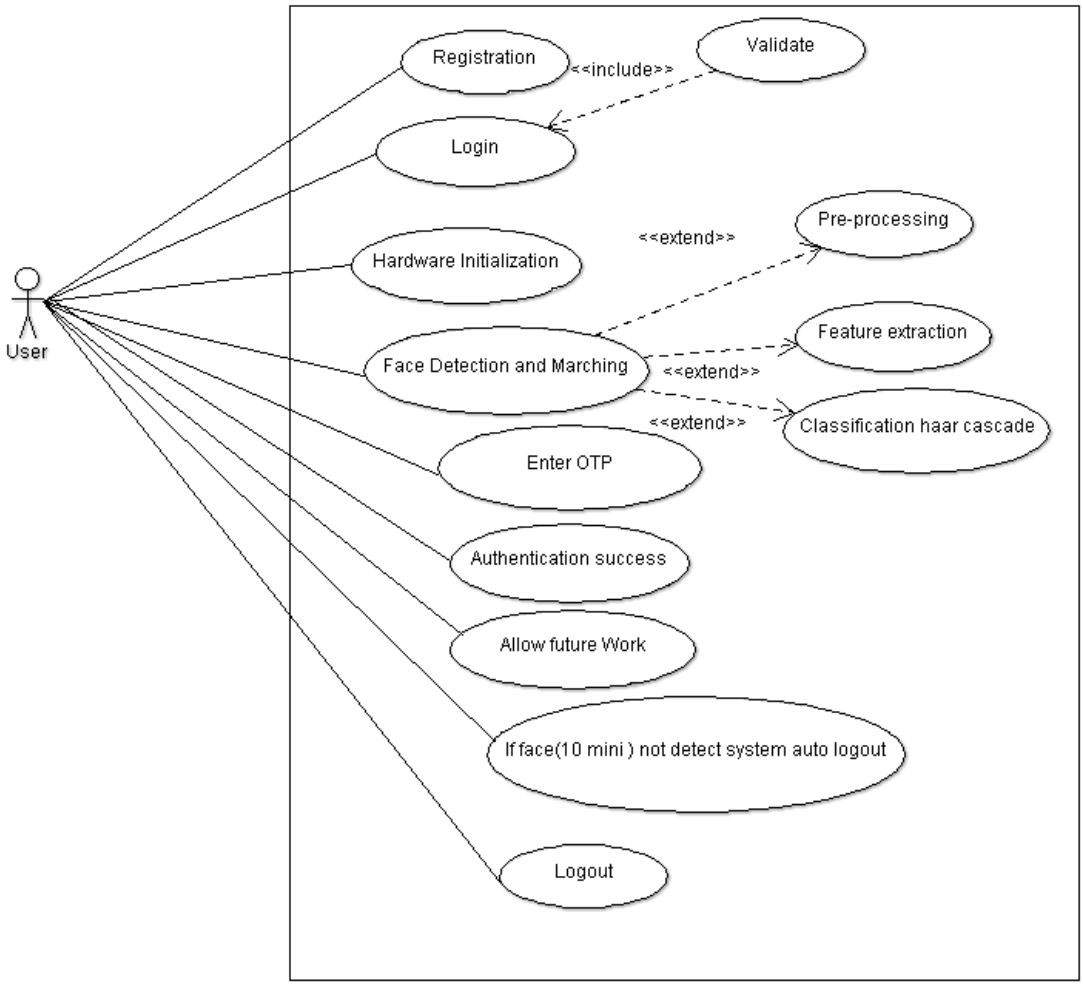


Figure 4.8: Use Case Diagram

CHAPTER 5

PROJECT PLAN

5.1 Project Estimate

Waterfall model is being used for the project estimation. It depicts the step wise execution of the entire project.

5.1.1 Reconciled Estimates

Cost Estimate :

Not Applicable. We are using free framework.

Time Estimate:

Approximately eight months.

5.1.2 Project Resources

Windows System, Djano framework, Python, High Speed Internet Connectivity, 4GB RAM, 2.93 GHZ CPU Speed.

5.2 Risk Management

In the overall procedure of our system involves the process of extracting the best prototype from the given image dataset, selecting the features for best estimations and then assigning the images to their respective class using probabilistic labels. The time and space complexity is within the polynomial time. The procedure in every stage will be NP-Complete. As our system will assign every image to either of the class we wall into NP-Complete category of problems.

5.2.1 Risk Identification

The various risks that are identified are :

1. Need of continuous internet while running the system as it is being executed on Colab.
2. Availability of featured dataset.

5.2.2 Risk Analysis

The risks are being analyzed taking into consideration the requirements for execution. The analysis include the need of internet for the project to run on the platform. The dataset being an important aspect is being taken into consideration for risk analysis because the entire computations are done on this input dataset.

5.2.3 Overview of Risk Mitigation, Monitoring, Management

Table 5.1: Risk 1 Mitigation, Monitoring, Management

Risk ID	1
Risk Description	Internet Availability
Category	Requirements
Probability	Less
Impact	High
Response	Mitigation
Strategy	Wi-Fi, LAN, Router
Risk Status	Identified

Table 5.2: Risk 2 Mitigation, Monitoring, Management

Risk ID	2
Risk Description	Need of Featured Dataset
Category	Requirements
Probability	Medium
Impact	High
Response	Mitigation
Strategy	Dataset Pre-processing
Risk Status	Identified

5.3 Project Schedule

5.3.1 Project Task Set

Major aspects of the project:

- Task 1: Correctness
- Task 2: Availability
- Task 3: Integrity

5.3.2 Timeline Chart

Table 5.3: System Implementation Plan

SR NO	DURATION	ACTIVITY PERFORMED
1	July second week	Topic Finalization
2	3rd and 4th week of July	Understanding of Base Paper
3	1st and 2nd week of August	Literature Survey
4	3rd and 4th week of August	System Architecture Design Completion
5	1stand 2nd week of September	1st review Completed
6	3rd and 4th week of September	2nd review Completed
7	1st week of October	UML diagrams, State Charts and DFD's Completed
8	2nd week of October	3rd Review Completed
9	3rd and 4th week of October	Final review completed
10	November	Exam
11	December second week	Distribution of implementation modules
12	January	Project implementation in modules
13	February	Development of the entire module
14	March	Testing of the project
15	April first week	Final Report Submission

5.4 Team Organization

Team consists of four members. Proper planning mechanism is used and roles are analyzed and defined.

5.4.1 Team Structure

Table 5.4: Team Structure

SR No.	Member Name	Responsibility
1	Megha Patil	Developer , Project analysis
2	Siddharth Nilakhe	Developer , Requirement gathering
3	Mehul ingale	Developer , Project Design
4	E Navaneet kumar	Developer , Testing

5.4.2 Management Reporting and Communication

Well organized plans were been made and completed accordingly within time. Progress reporting was been updated and completed. Communication as per requirements were being done effectively.

CHAPTER 6

PROJECT IMPLEMENTATION

6.1 Overview of Project Modules

6.1.1 Face recognition

Face recognition is a method of identifying or verifying the identity of an individual using their face. We have used Haar Cascade algorithm to recognize face.

6.1.2 Credentials Matching

Credentials (Loin Id and Password) are matched by comparing input Credentials with that of already stored in database

6.2 Tools and Technologies Used

6.2.1 Python

Python is a general purpose programming language started by Guido van Rossum, which became very popular in short time mainly because of its simplicity and code readability. It enables the programmer to express his ideas in fewer lines of code without reducing any readability. Compared to other languages like C/C++, Python is slower. But another important feature of Python is that it can be easily extended with C/C++. This feature helps us to write computationally intensive codes in C/C++ and create a Python wrapper for it so that we can use these wrappers as Python modules. This gives us two advantages: first, our code is as fast as original C/C++ code (since it is the actual C++ code working in background) and second, it is very easy to code in Python. This is how OpenCV-Python works, it is a Python wrapper around original C++ implementation. And the support of Numpy makes the task more easier. Numpy is a highly optimized library for numerical operations. It gives a MATLAB-style syntax. All the OpenCV array structures are converted to-and-from Numpy arrays. So whatever operations you can do in Numpy, you can combine it with OpenCV, which increases number of weapons in your arsenal. Besides that, several other libraries like SciPy, Matplotlib which supports Numpy can be used with this.

6.2.2 MySQL

MySQL is the most popular Open Source Relational SQL Database Management System. MySQL is one of the best RDBMS being used for developing various web-based software applications. MySQL is developed, marketed and supported

by MySQL AB, which is a Swedish company. A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds.
Other kinds of data stores can also be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those type of systems.

6.2.3 OpenCV

OpenCV was started at Intel in 1999 by Gary Bradsky and the first release came out in 2000. Vadim Pisarevsky joined Gary Bradsky to manage Intel's Russian software OpenCV team. In 2005, OpenCV was used on Stanley, the vehicle who won 2005 DARPA Grand Challenge. Later its active development continued under the support of Willow Garage, with Gary Bradsky and Vadim Pisarevsky leading the project. Right now, OpenCV supports a lot of algorithms related to Computer Vision and Machine Learning and it is expanding day-by-day. Currently OpenCV supports a wide variety of programming languages like C++, Python, Java etc and is available on different platforms including Windows, Linux, OS X, Android, iOS etc. Also, interfaces based on CUDA and OpenCL are also under active development for high-speed GPU operations. OpenCV-Python is the Python API of OpenCV. It combines the best qualities of OpenCV C++ API and Python language.

6.3 Algorithm Details

6.3.1 Haar Cascade Algorithm

Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video and based on the concept of features proposed by Paul Viola and Michael Jones in their paper "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001.It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images and used to detect objects in other images. The algorithm has four stages:

1. Haar Feature Selection
2. Creating Integral Images
3. Adaboost Training

4. Cascading Classifiers

Haar Feature Selection: A Haar feature considers adjacent rectangular regions at a specific location in a detection window, sums up the pixel intensities in each region and calculates the difference between these sums.
Creating Integral Images: Integral Images are used to make feature selection super fast. Among all these features we calculated, most of them are irrelevant. Therefore at this stage irrevelent images and background is deleted.
Adaboost Training: Selection of best feature among hundreds and thousands of features is accomplished using a concept called Adaboost which both selects the best features and trains the classifiers that use them. This algorithm constructs a "strong" classifier as a linear combination of weighted simple "weak" classifiers.

The process is as follows.

- During the detection phase, a window of the target size is moved over the input image, and for each subsection of the image and Haar features are calculated.
- This difference is then compared to a learned threshold that separates non-objects from objects.
- Because each Haar feature is only a "weak classifier" (its detection quality is slightly better than random guessing) a large number of Haar features are necessary to describe an object with sufficient accuracy and are therefore organized into cascade classifiers to form a strong classifier.

The cascade classifier consists of a collection of stages, where

- Each stage is an ensemble of weak learners. They are classifiers called decision stumps.
- Each stage is trained using a technique called boosting. Boosting provides the ability to train a highly accurate classifier by taking a weighted average of the decisions made by the weak learners.
- Each stage of the classifier labels the region defined by the current location of the sliding window as either positive or negative.
- Positive indicates that an object was found and negative indicates no objects were found.

  - If the label is negative, the classification of this region is complete, and the detector slides the window to the next location.
  - If the label is positive, the classifier passes the region to the next stage. The detector reports an object found at the current window location when the final stage classifies the region as positive.

- The stages are designed to reject negative samples as fast as possible. The assumption is that the vast majority of windows do not contain the object of interest. Conversely, true positives are rare and worth taking the time to verify.
  - A true positive occurs when a positive sample is correctly classified.
  - A false positive occurs when a negative sample is mistakenly classified as positive.
  - A false negative occurs when a positive sample is mistakenly classified as negative.

- To work well, each stage in the cascade must have a low false negative rate. If a stage incorrectly labels an object as negative, the classification stops, and you cannot correct the mistake.

CHAPTER 7

SOFTWARE TESTING

Software Testing is the process of executing every functionality and procedure of the program or application with the intent to find the errors or bugs. Testing is performed to investigate the entire project from every aspect. It deals with the motto to make the model more robust and accurate. The results make the developer aware of the issues that the program might go through in the future. Software testing is important to understand the future risks.

7.1 Type of Testing

7.1.1 Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. Unit tests ensurethat each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.
Process

- Creates a file log for each function, where each line contains the functions parameters, every time the function is ran.
- Reports the time it took to run the function.
  - Test fixture: A test fixture is used as a baseline for running tests to ensure that there is a fixed environment in which tests are run so that results are repeatable.
    Examples:
    * Creating temporary databases.
    * Starting a server process.
  - Test case: A test case is a set of conditions which is used to determine whether a system under test works correctly.
  - Test suite: Test suite is a collection of test cases that are used to test a software program to show that it has some specified set of behaviours by executing the aggregated tests together.
  - Test runner: A test runner is a component which set up the execution of tests and provides the outcome to the user.

A unit test is a method that instantiates a small portion of our application and verifies its behavior independently from other parts. A typical unit test contains

3 phases: First, it initializes a small piece of an application it wants to test (also known as the system under test, or SUT), then it applies some stimulus to the systemunder test (usually by calling a method on it), and finally, it observes the resultingbehavior.
If the observed behavior is consistent with the expectations, the unit test passes, otherwise, it fails, indicating that there is a problem somewhere in the system under test. These three unit test phases are also known as Arrange, Act and Assert, or simply AAA.

7.1.2 Integration Testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration testing is specifically aimed at exposing the problems that arise from the Combination of components. Integration tests are the class of tests that verify that multiple moving pieces and gears inside the clock work well together. Where unit tests investigate the gears, integration tests look at the position of the hands to determine if the clock can tell time correctly. They look at the system as a whole or at its subsystems. Integration tests typically function at a higher level conceptually than unit tests. Thus, writing integration tests also happens at a higher level.
Because they deal with gluing code together, there are typically fewer integration tests in a test suite than there are unit tests. However, integration tests are no less important. Integration tests are essential for having adequate testing. They encompass all of the cases that you cannot hit through plain unit testing. Sometimes, especially in probabilistic or stochastic codes, the precise behavior of an integration test cannot be determined beforehand. That is OK. In these situations it is acceptable for integration tests to verify average or aggregate behavior rather than exact values. Sometimes you can mitigate nondeterminism by saving seed values to a random number generator, but this is not always going to be possible. It is better to havean imperfect integration test than no integration test at all.

7.1.3 Regression Testing

Regression testing is a type of software testing that ensures that previously developed and tested software still performs the same way after it is changed or interfaced with other software. Changes may include software enhancements, patches,

configuration changes, etc. Regression tests assume that the past is correct. They are great for letting developers know when and how a code base has changed. They are not great for letting anyone know why the change occurred. The change between what a code produces now and what it computed before is called a regression. Regression tests are qualitatively different from both unit and integration tests. Rather than assuming that the test author knows what the expected result should be, regression tests look to the past for the expected behavior. The expected result is taken as what was previously computed for the same inputs.

7.1.4 Alpha Testing

Alpha testing is a type of acceptance testing; performed to identify all possible issues/bugs before releasing the product to everyday users or public. The focus of this testing is to simulate real users by using black box and white box techniques. The aim is to carry out the tasks that a typical user might perform. Alpha testing is carried out in a lab environment and usually the testers are internal employees of the organization. To put it as simple as possible, this kind of testing is called alpha only because it is done early on, near the end of the development of the software, and before Beta Testing.

7.1.5 Beta Testing

- Beta Testing of a product is performed by "real users" of the software application in a "real environment" and can be considered as a form of external User Acceptance Testing.
- Beta version of the software is released to a limited number of end-users of the product to obtain feedback on the product quality. Beta testing reduces product failure risks and provides increased quality of the product through customer validation.
- It is the final test before shipping a product to the customers. Direct feedback from customers is a major advantage of Beta Testing. This testing helps to tests the product in real time environment.

7.2 Test cases and Test Results

Table 7.1: Test Result

No.	Functionality	Procedure	Expected output	Actual output	Result
1	Checking Login button functionality	1. enter username and password 2. press login button	Login should be successful	Login is successful	pass
2	Checking Login button functionality	1. enter wrong username and password 2. press login button	Login should not be successful	Login is unsuccessful	pass
3	Authenticating Face	1. Capture face of known person 2.Click on face matching button	System should displayed person's name	Webpage displays person's name	Pass

CHAPTER 8

RESULTS

8.1 Screenshots

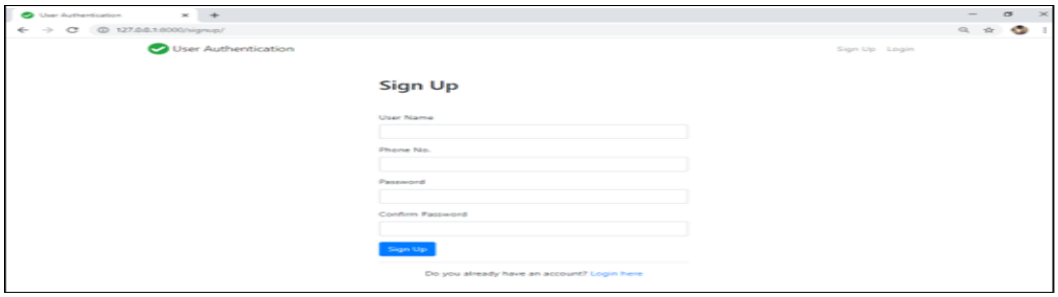


Figure 8.1: Output 1

Figure 8.2: Output 2

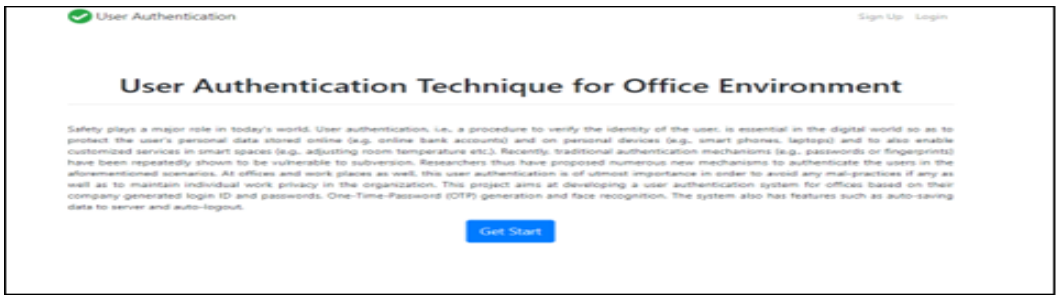


Figure 8.3: Output 3

Figure 8.4: Output 4

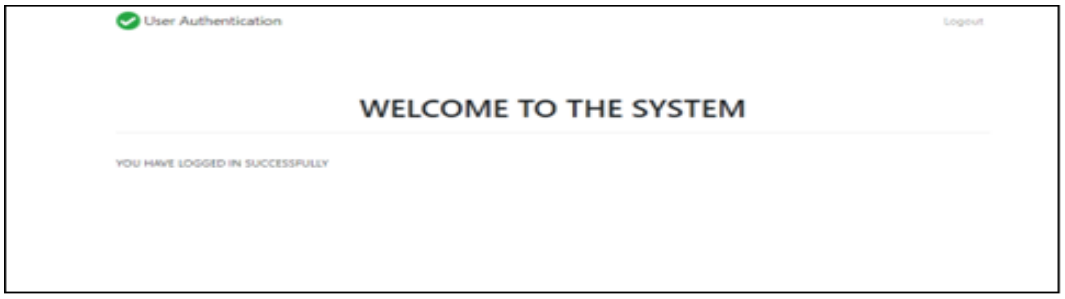


Figure 8.5: Output 5

CHAPTER 9

CONCLUSIONS AND FUTURE WORK

9.1 Conclusion

There has been a use of three tier architecture for providing the authentication and security to the system. Those tiers are login credentials, face recognition and OTP. All these tiers give a great strength for not only providing the authentication but also secure the data in the system. The proposed approach provides more control over the data that stored in the system and restricting the access to specific user for specific file with less privilege and for less time period on the basis of secret key using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is guaranteed twice by providing encrypting using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to get illegal access to restricted resources.

9.2 Future work

1. In order to overcome the drawbacks of proposed system if anyone tries to hack the data, the authorized user will get a notification and through an email or message and the authorized user can crash the hard disk. In order to recover it back through particular system software might be needed.

2. There can also be changes in the phases of the tool and use anything else as per the convenience of the user. Our system will be compatible with many other types of scanners as well as sensors.

3. The same system can be developed in such a way that it can run on multiple operating systems. For now the system used is windows, later it can even be made compatible with mac as well as Linux for user's convenience.

9.3 Applications

1. Can be used in security sector.

2. It can be used for securing IoT based smart services like smart home, smart grid etc.

APPENDIX A

The system would perform the following satisfiability tests to detect the following as NP Hard or NP Complete.

1. When the input data is being fed to the system the entire data must be fed to the system be it of the small size or medium size data. It is an NP Complete problem.

2. Image to be compared is available in the training dataset. It is an NP Hard problem because the image is sometimes not exactly available in the dataset .

3. The construction of the matrix is an NP Complete problem.

4. Construction of the class inference is an NP Complete problem.

5. Possibility of finding the exact prototype of the image is and NP Complete problem because even if the exact match is not found at least the best prototype is being matched.

6. Assignment of the appropriate probabilistic label is an NP Complete problem.

APPENDIX B

URKUND

Urkund Analysis Result

Analysed Document: 8-BE-sem-2-Report--1-final.pdf (D107337774)
Submitted: 6/1/2021 12:45:00 PM
Submitted By: aissmsioit.library@aissmsioit.org
Significance: 9 %

Sources included in the report:

SWMAIF_REPORT.pdf (D58343254)
Finalreport(depression detection).pdf (D78845920)
PROJ_2k19_1 New.pdf (D61131993)
report.pdf (D78870867)
Athira_Hari_10520152_Dissertation.pdf (D103048292)
http://www.ijaresm.com/uploaded_files/document_file/Jubed_AhmedLq8R.pdf
http://203.201.63.46:8080/jspui/bitstream/123456789/1400/17/Smart%20Surveillance%20System%20By%20Amrit%20Sinha%2C%20Ankur%20Singh%20and%20Manas%20Kashyap%20USN%201CR14CS011%2C%201CR14CS015%20and%201CR14CS076.pdf
https://kola.opus.hbz-nrw.de/files/2039/Thesis_Nabil_Finalized.pdf

Instances where selected sources appear:

28

APPENDIX C
Paper Publication and Certificates

IMPLEMENTATION PAPER ON MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES

Megha Patil, Mehul Ingale, Navaneet Kumar, Siddharth Nilakhe, Mrs.MINAL NERKAR

Department of Computer Engineering, AISSMS IOIT, Pune, India.

Abstract: Safety plays a major role in today's world. User authentication, i.e., a procedure to verify the identity of the user, is essential in the digital world so as to protect the user's personal data stored online (e.g. online bank accounts) and on personal devices (e.g., smart phones, laptops) and to also enable customized services in smart spaces (e.g., adjusting room temperature etc.). Recently, traditional authentication mechanisms (e.g., passwords or fingerprints) have been repeatedly shown to be vulnerable to subversion. Researchers thus have proposed numerous new mechanisms to authenticate the users in the aforementioned scenarios. At offices and work places as well, this user authentication is of utmost importance in order to avoid any mal-practices if any as well as to maintain individual work privacy in the organization. This project aims at developing a user authentication system for offices based on their company generated login ID and passwords, One-Time-Password (OTP) generation and face recognition. The system also has features such as auto-saving data to server and auto-logout.

Keywords: AutoSaved, Auto-logout, Face recognition, Login ID and passwords credentials, One-Time-Password (OTP).

I. INTRODUCTION

Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing three tier authentications which are login credentials, face Recognition scanner and OTP. The proposed methodology provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources.

The authentication, confidentiality and privacy of data is needed in today's world. The smart devices, like smart phones and sensing nodes, are now developing an emerging global and Internet-based information service platform called the Internet of Things (IoT). Generally, the IoT architecture is based on some existing data communication tools, which could range from RFID (Radio Frequency Identification) -tagged products to complex computational items. Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed. Direct interaction of smart devices within the immediate living space of humans intimidates new security vulnerabilities. Research has been led in developing customized tools for computer security to establish confidentiality, integrity and availability. In case of any kind of security failure, our system provides the users data fully data security and assurance of privacy. The aim is to prevention system that is adaptive and receptive to new threats and provides more control of owner on the data stored on system by restricting the access to particular user for specific file with limited rights. The idea behind it to create software that will protect the data from all kinds of attacks and maintain entire confidentiality of the data.

II. LITERATURE REVIEW

There has been a use of three tire architecture in paper "Effective Authentication For Restricing Unauthorized User", [1] for providing security to the system. Those tiers are Facial recognition, Fingerprint Scanning and OTP. All these tiers give a great strength to security of system. Incase if

there is an attack on system, the measures are provided so as to not leak the important data from the system. By using AES 512 all the data is encrypted which can only be decrypted by a specific key.

The security and protection of such personal information are becoming more and more important since mobile devices are vulnerable to unauthorized access or theft. User authentication is a task of paramount importance that grants access to legitimate users at the point-of-entry and continuously through the usage session. This task is made possible with today's smartphones' embedded sensors that enable continuous and implicit user authentication by capturing behavioral biometrics and traits. In [2], Mohammed Abuhamad et al surveyed more than 140 recent behavioral biometric-based approaches for continuous user authentication, including motionbased methods, gait-based methods, keystroke dynamics-based methods, touch gesturebased methods, voice-based methods (16 studies), and multimodal-based methods. The survey provides an overview of the current state-of-the-art approaches for continuous user authentication using behavioral biometrics captured by smartphones' embedded sensors, including insights and open challenges for adoption, usability, and performance.

Biometric authentication of an individual through their own characteristics is the most common way to identify a person. In [3], a multimodal biometric user verification system with identical twin shows the fingerprint, face and lip classification model using SVM2 with kernel functions is efficient and promising. It would be seen from the results that the FRR is less than that of FAR.

Paper "Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data "[4] analyzes the performance of combining the use of on-line signature and fingerprint authentication to perform robust user authentication. Signatures are verified using the dynamic time warping (DTW) technique of string matching. The proposed minutiae-based matching algorithm, stores merely a small number of minutiae points, which greatly reduces the storage requirement with the help of phase correlation. Here, matching score level fusion is used by applying weighted sum rule for the biometric fusion process. To improve the authentication performance, deep learning classifier is proposed in this work for multi-biometrics authentication. When a biometric authentication request is submitted, the proposed authentication system uses deep learning to automatically select an appropriate matching image. In the experiment, biometric authentication was performed on healthcare in the UCI database. Multi -Biometric Authentication was used during the authentication stage.

Presently a-days Cloud registering is rising field in light of its Performance, high accessibility, easily. Information store is principle future that cloud benefit gives to the huge association to store tremendous measure of information. Yet at the same time numerous associations are not prepared to execute distributed computing innovation since absence of security. So the principle goal of [5] is to understand the security issues and to anticipate unapproved access in distributed storage, it should be possible with the assistance of an effective validation strategy by utilizing cross breed verification calculation to give security of the information in cloud and guarantee amending code to keep up the nature of administration. In any case, solid client confirmation that confines illicit access to the administration giving servers is the foremost prerequisite for securing cloud condition

Authentication of a user through an ID and password is generally done at the start of a session. But the continuous authentication system observes the genuineness of the user throughout the entire session, and not at login only. In [6], Suhail Javed Quraishi and Sarabjeet Singh Bedi proposed the usage of keystroke dynamics as biometric trait for continuous user authentication in desktop platform. Biometric Authentication involves mainly three phases named as enrollment phase, verification phase and identification phase. The identification phase marks the accessed user as an authenticated only if the input pattern matches with the profile pattern otherwise the system is logout. The proposed Continuous User Biometric Authentication (CUBA) System is based on free text input from keyboard. There is no restriction on input data during Enrolment, Verification, and Identification phase. Unsupervised One-class Support Vector Machine is used to classify the authenticated user's input from all the other inputs. This continuous authentication system can be used in many areas like in Un-proctored online examination systems, Intrusion & Fraud Detection Systems, Areas where user alertness is required for entire period e.g. Controlling Air Traffic etc

The significant growth in users of e-learning technologies and their use in courses have given rise to a major concern over protecting them from misuse; a significant concern is that of the potential for cheating or illicit assistance during online examinations. Paper "A Robust e-Invigilation System Employing Multimodal Biometric Authentication", presents the development of robust, flexible, transparent and continuous authentication mechanism for e-assessments. To monitor the exam taker and ensure that only the legitimate student is taking the exam, the system offers a continuous user identification employing multimodal biometrics; a security layer using an eye tracker to record the student's eye movement; and, speech recognition to detect inappropriate communication. The focus of [7] in particular is the development and evaluation of 3D facial authentication. An experiment has been conducted to investigate the ability of the proposed platform to detect any cheating attempts. During the experiment, participants' biometric data, eye movement, and head movements have been collected using custom software. The 3D camera also captured the session using a built-in microphone and the system recognized speech (employing a speech recognition algorithm). 51 participants participated in this experiment. The FRR of all legitimate participants was 0 and 0.0063 in 2D and 3D facial recognition modes respectively. Furthermore, three participants were tasked with a series of eight scenarios that map to typical misuse. The results of the FAR and FRR of five of these threat scenarios in both 2D and 3D mode were 0 with two cases exhibiting an FAR of 0.11 and 0.076 in the 2D mode.

Currently systems are protected using many firewalls, IDS and security software. The existing system can be easily compromised by any tool used by attacker. The aim of system is to provide effective authentication from unauthorized users by providing two tier authentications which are Irish Recognition scanner and OTP. The proposed methodology in [8] provides more control over data stored in system by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key authentication using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is fully guaranteed by not only encrypting the data using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources. To overcome these drawbacks, the AES 256 algorithm will be introduced after our one-time password authentication protocol. Thus the proposed system is more secured and can be provide effective authentication.

Paper "Effective Authentication for Avoiding Unauthorized User Access", presented a modified Role Based Access Control model by extending traditional role based access control in SQL (Structure Query Language) data storage. The said model evaluates and executes security policies which contain versatile access conditions against the dynamic nature of data. The goal of [9] is to devise a mechanism for a forward looking, assertive yet flexible security features to regulate access to data in the data storage that is devoid of rigid structures and consistency. This is achieved by integrating roles and authenticated fine-grained access rules and implemented through effective audit trail. The model and the rules used are presented and show that when implemented, it is capable of outperforming existing models that are role based.

Paper [10] presented a state of art about biometric hand, different techniques used. Biometric is essentially used to avoid risks of password easy to find or Stoll; with as slogan save Time and Attendance. BIOMETRICS is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing biometric techniques but also present detailed of representative methods within each category. Biometrics is a rapidly evolving technology which is being widely used in forensics such as criminal identification and prison security, and has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be

used during transactions conducted via telephone and internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry devices. Although many technologies fit in the biometric space, each works a bit differently. Relatively new on the biometric scene, face recognition devices use PC-attached cameras to record facial geometry. Once the biometric data is collected, it is encrypted and stored--locally, in the case of the desktop-only products; in a central database for the network solutions. When a user tries to log on, the software compares the incoming biometric data against the stored data.

III. PROPOSED SYSTEM

A face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely. Fig 1 illustrates the system architecture of proposed system. It consists of a three-step secure authentication process for working employees in their respective organizations.

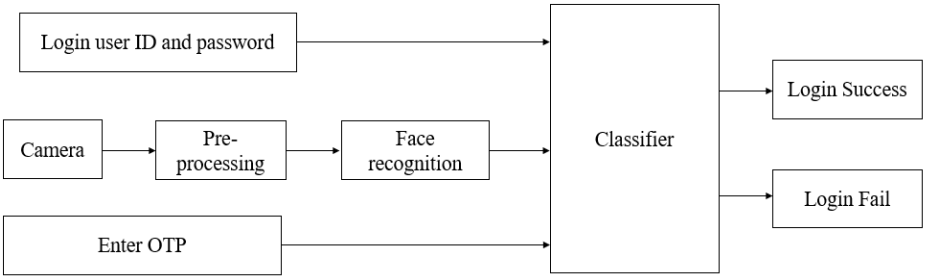


Fig 1: System Architecture of Proposed System

As stated above, at first the user needs to enter the unique login Id and password combination provided to them by the company. Once that matches with the database, next step is to generate the OTP on the registered mobile number. If not, further access to login into the system will be denied. If correct generated OTP is entered into the system, the user moves second step ahead to gain access to the system. Once this is done, next comes the face recognition. With the help of webcams present with each and every system, the face in front of cam is detected. A live image is captured automatically through a webcam installed on the device, which is compared with the image stored in the database. If this image matches, user can get the access to operate that particular system. Haar Cascade Classifier is used to implement face recognition. An additional feature of autosave and auto-logout is also included in this system. Suppose the employee happens to leave their desk due to some reasons, the webcam will be continuously detecting and capturing the images if any. Incase an unknown face image other than that system user, is captured by the webcam, the whole work/data will be automatically saved to the company's server and the system will automatically logout, so that, the unknown user cannot make any manipulations in the users work. The autosave feature helps the user to re-continue the work form the point he/she had left it. Hence a very efficient, safe and reliable system is developed.

IV. RESULTS

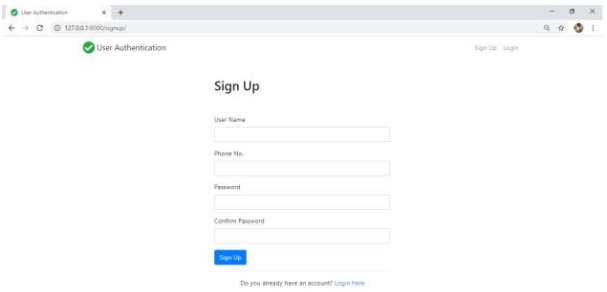


Fig. 2 sign_up_page

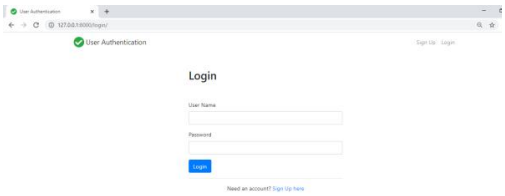


Fig. 3. Login Pages

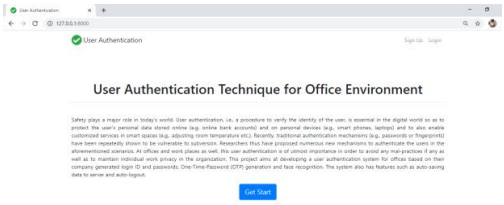


Fig. 4 Home

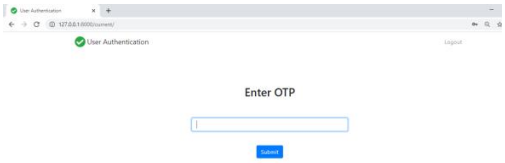


Fig. 5. Enter OTP

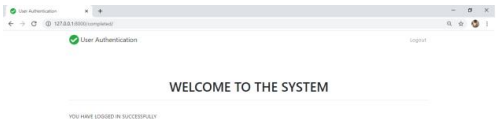


Fig. 6 FINAL_PAGE

V. CONCLUSION

There has been a use of three tier architecture for providing the authentication and security to the system. Those tiers are login credentials, face recognition and OTP. All these tiers give a great strength for not only providing the authentication but also secure the data in the system. The proposed approach provides more control over the data that stored in the system and restricting the access to specific user for specific file with less privilege and for less time period on the basis of secret key using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is guaranteed twice by providing encrypting using secret key but also to the access permission and limited file information. Especially, the purpose of the one-time password is to make it more difficult to get illegal access to restricted resources.

- In order to overcome the drawbacks of proposed system if anyone tries to hack the data, the authorized user will get a notification and through an email or message and the authorized user can crash the hard disk. In order to recover it back through particular system software might be needed.
- There can also be changes in the phases of the tool and use anything else as per the convenience of the user. Our system will be compatible with many other types of scanners as well as sensors.
- The same system can be developed in such a way that it can run on multiple operating systems. For now the system used is windows, later it can even be made compatible with mac as well as Linux for user's convenience.

REFERENCES

[1] Patil, A., Rana, D., Vichare, S., & Raut, C. (2018). Effective Authentication for Restricing Unauthorized User. 2018 International Conference on Smart City and Emerging Technology (ICSCET). doi:10.1109/icscet.2018.8537323

[2] IEEE INTERNET OF THINGS JOURNAL 1 Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen arXiv:2001.08578v2 [cs.CR] 10 May 2020

[3] A Multimodal Biometric User Verification System with Identical Twin using SVM 2

B.Lakshmi priya, M.Pushpa Rani International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020

[4] Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data Dr. Gandhimathi Amirthalingam1 , Harrin Thangavel Volume 8, No.4, July – August 2019 International Journal of Advanced Trends in Computer Science and Engineering

[5] Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm S. Naveen Kumar1*, K. Nirmala2 International Journal of Engineering & Technology, 7 (1.1) (2018) 607-611 International Journal of Engineering & Technology

[6] On keystrokes as Continuous User Biometric Authentication Suhail Javed Quraishi, Sarabjeet Singh Bedi International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019

[7] A Robust e-Invigilation System Employing Multimodal Biometric Authentication Salam S. Ketab, Nathan L. Clarke, and Paul S. Dowland International Journal of Information and Education Technology, Vol. 7, No. 11, November 2017

[8] EFFECTIVE AUTHENTICATION FOR AVOIDING UNAUTHORIZED USER ACCESS Ms. Chaitali A.Raut International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 04, Issue 07; July - 2018 [ISSN: 2455-1457]

[9] INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 7, ISSUE 11, NOVEMBER 2018 ISSN 2277-8616 182 IJSTR©2018 www.ijstr.org Modified Role Based Access Control Model For Data Security Bukohwo Michael Esiefarienrhe, Abubakar Hashimu Ekka

[10] A SECURITY BY BIOMETRIC AUTHENTICATION Gurudatt Kulkarni1 , Ruchira Chandorkar2 , Nikita Chavan International Journal of Computer Science and Engineering Research and Development (IJCSERD), ISSN 2248- 9363 (Print), ISSN 2248-9371 (Online) Volume 2, Number 1, July-December (2012)

The International Journal of Analytical and Experimental Modal analysis

An UGC-CARE Approved Group - II Journal

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 0886-9367 / web : http://ijaema.com / e-mail: submitijaema@gmail.com

Certificate of Publication

This is to certify that the paper entitled

"IMPLEMENTATION PAPER ON MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES"

Authored by :

Megha Patil

From

AISSMS IOIT, Pune, India

Has been published in

IJAEMA JOURNAL, VOLUME XIII, ISSUE V, MAY- 2021

Michal A. Olszewski Editor-In-Chief
IJAEMA JOURNAL

6.3 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

http://ijaema.com/

The International Journal of Analytical and Experimental Modal analysis

An UGC-CARE Approved Group - II Journal

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 0886-9367 / web : http://ijaema.com / e-mail: submitijaema@gmail.com

Certificate of Publication

This is to certify that the paper entitled

"IMPLEMENTATION PAPER ON MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES"

Authored by :

Siddharth Nilakhe

From

AISSMS IOIT, Pune, India

Has been published in

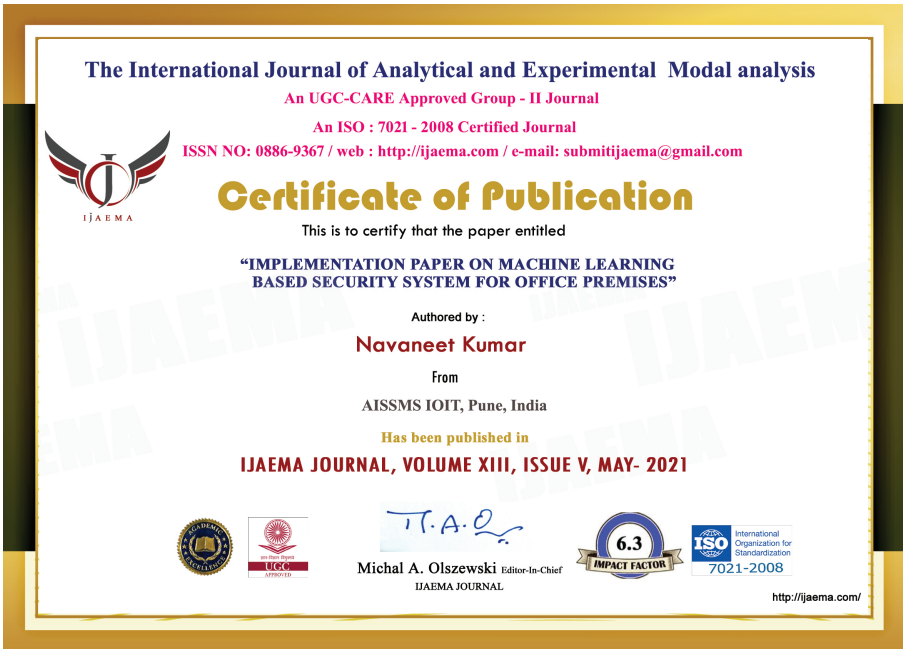
IJAEMA JOURNAL, VOLUME XIII, ISSUE V, MAY- 2021

Michal A. Olszewski Editor-In-Chief
IJAEMA JOURNAL

6.3 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

http://ijaema.com/



The International Journal of Analytical and Experimental Modal analysis

An UGC-CARE Approved Group - II Journal

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 0886-9367 / web : http://ijaema.com / e-mail: submitijaema@gmail.com

Certificate of Publication

This is to certify that the paper entitled

"IMPLEMENTATION PAPER ON MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES"

Authored by :

Navaneet Kumar

From

AISSMS IOIT, Pune, India

Has been published in

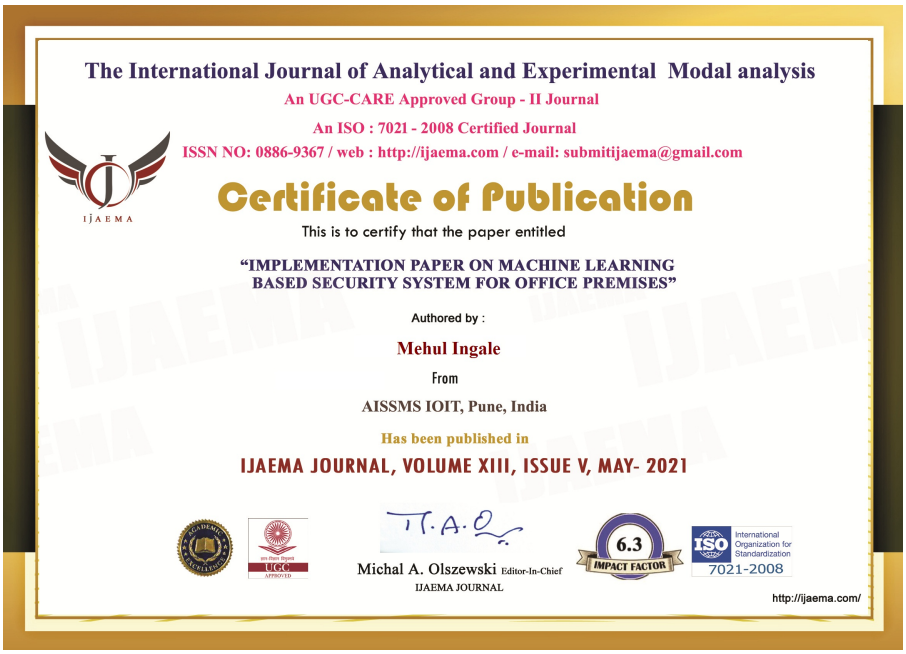
IJAEMA JOURNAL, VOLUME XIII, ISSUE V, MAY- 2021

Michal A. Olszewski Editor-In-Chief
IJAEMA JOURNAL

6.3 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

http://ijaema.com/



The International Journal of Analytical and Experimental Modal analysis

An UGC-CARE Approved Group - II Journal

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 0886-9367 / web : http://ijaema.com / e-mail: submitijaema@gmail.com

Certificate of Publication

This is to certify that the paper entitled

"IMPLEMENTATION PAPER ON MACHINE LEARNING BASED SECURITY SYSTEM FOR OFFICE PREMISES"

Authored by :

Mehul Ingale

From

AISSMS IOIT, Pune, India

Has been published in

IJAEMA JOURNAL, VOLUME XIII, ISSUE V, MAY- 2021

Michal A. Olszewski Editor-In-Chief
IJAEMA JOURNAL

6.3 IMPACT FACTOR

ISO International Organization for Standardization 7021-2008

http://ijaema.com/

AISSMS
INSTITUTE OF INFORMATION TECHNOLOGY
ADDING VALUE TO ENGINEERING

Department of Computer Engineering

Self-Evaluation

Name of the Project	Machine Learning Based Security System for Office Premises
Name of the student	E Navaneet Kumar
Name of the student	Mehul Ingale
Name of the student	Siddharth Nilakhe
Name of the student	Megha Patil

File of literature Survey	Design	Implementation	Task and Result	Attendance on project Day	Work according to plan Activity	Managing of log book	Project Presentation or Participation	Project exhibition participation	Award Prize if any
(5)	(20)	(20)	(20)	(5)	(10)	(5)	(5)	(5)	(5)
5	20	20	20	4	10	4	5	0	0

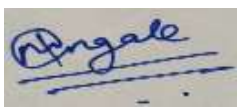
Observations and comments of Guide:

Signature of Guide

Name of Student **Signature of student**

1. **E Navaneet Kumar**

2. **Mehul Ingale**



3. **Siddharth Nilakhe** 

4. **Megha Patil** 

References

[1] Patil, A., Rana, D., Vichare, S., Raut, C. (2018). Effective Authentication for Restricing Unauthorized User. 2018 International Conference on Smart City and Emerging Technology (ICSCET). doi:10.1109/icscet.2018.8537323

[2] IEEE INTERNET OF THINGS JOURNAL 1 Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen arXiv:2001.08578v2 [cs.CR] 10 May 2020

[3] A Multimodal Biometric User Verification System with Identical Twin using SVM 2 B.Lakshmi priya, M.Pushpa Rani International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020

[4] Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data Dr. Gandhimathi Amirthalingam1 , Harrin Thangavel Volume 8, No.4, July – August 2019 International Journal of Advanced Trends in Computer Science and Engineering

[5] Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm S. Naveen Kumar1*, K. Nirmala2 International Journal of Engineering Technology, 7 (1.1) (2018) 607-611 International Journal of Engineering Technology

[6] On keystrokes as Continuous User Biometric Authentication Suhail Javed Quraishi, Sarabjeet Singh Bedi International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019

[7] A Robust e-Invigilation System Employing Multimodal Biometric Authentication Salam S. Ketab, Nathan L. Clarke, and Paul S. Dowland International Journal of Information and Education Technology, Vol. 7, No. 11, November 2017

[8] EFFECTIVE AUTHENTICATION FOR AVOIDING UNAUTHORIZED USER ACCESS Ms. Chaitali A.Raut International Journal of Recent Trends

in Engineering Research (IJRTER) Volume 04, Issue 07; July - 2018 [ISSN: 2455-1457]

[9] INTERNATIONAL JOURNAL OF SCIENTIFIC TECHNOLOGY RESEARCH VOLUME 7, ISSUE 11, NOVEMBER 2018 ISSN 2277-8616 182 IJSTR©2018 www.ijstr.org Modified Role Based Access Control Model For Data Security Bukohwo Michael Esiefarienrhe, Abubakar Hashimu Ekka

[10] Gurudatt Kulkarni, Ruchira Chandorkar, Nikita Chavan, "A SECURITY BY BIOMETRIC AUTHENTICATION" International Journal of Computer Science and Engineering Research and Development (IJCSERD), ISSN 2248-9363 (Print), ISSN 2248-9371 (Online) Volume 2, Number 1, July-December (2012)