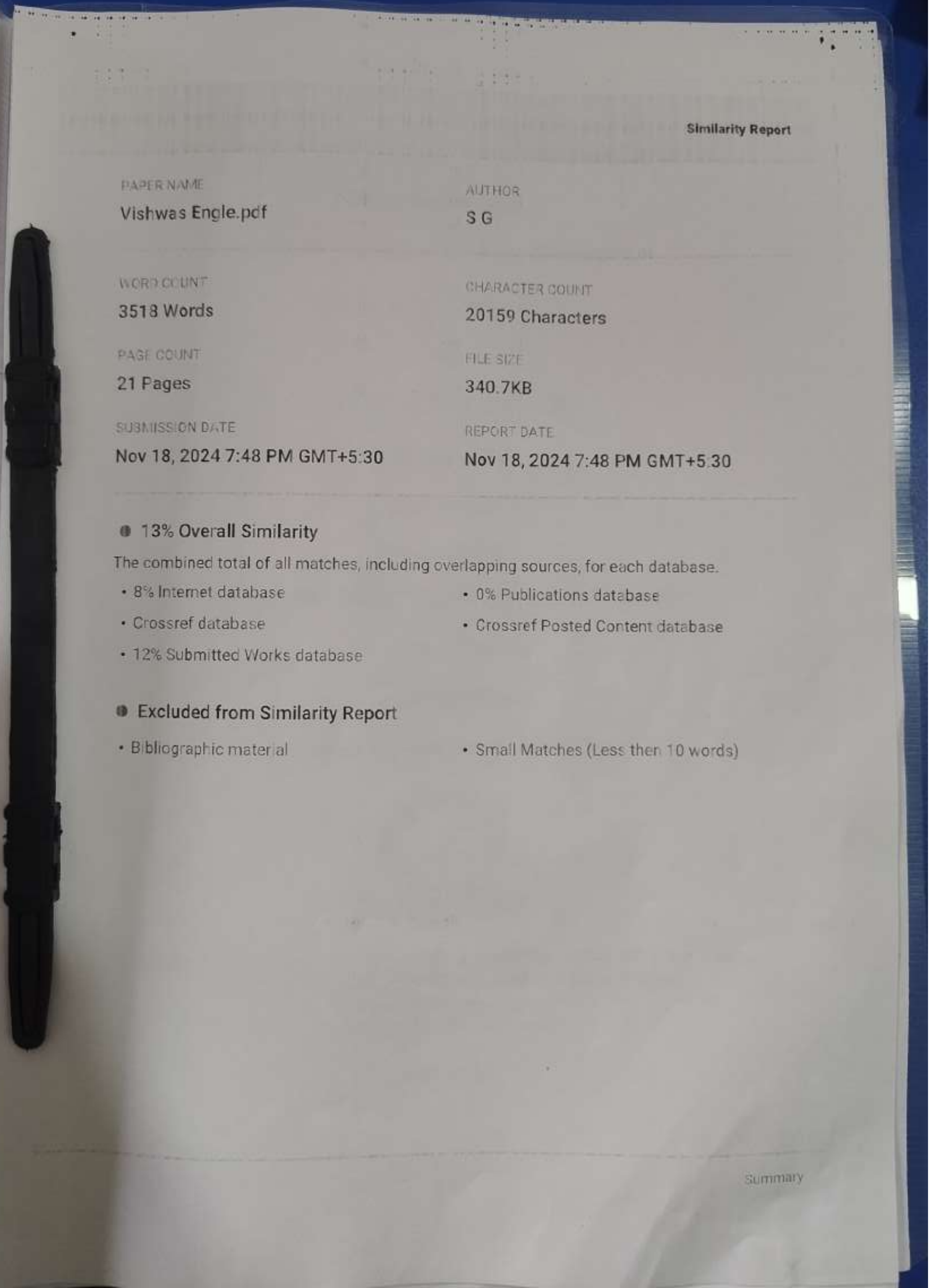


Similarity Report

PAPER NAME

Vishwas Engle.pdf

AUTHOR

S G

WORD COUNT

3518 Words

CHARACTER COUNT

20159 Characters

PAGE COUNT

21 Pages

FILE SIZE

340.7KB

SUBMISSION DATE

Nov 18, 2024 7:48 PM GMT+5:30

REPORT DATE

Nov 18, 2024 7:48 PM GMT+5:30

● 13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 8% Internet database
- 0% Publications database
- Crossref database
- Crossref Posted Content database
- 12% Submitted Works database

● Excluded from Similarity Report

- Bibliographic material
- Small Matches (Less then 10 words)

Summary

Three level password security system using python

Minor Project Report

Submitted for the partial fulfilment of the degree of

Bachelor of Technology

In

Internet Of Things (IO)

Submitted By

Vishwas Engle

0901IO221076

UNDER THE SUPERVISION AND GUIDANCE OF

Dr. Aditya Dubey

Assistant Professor

Department of Centre of Internet Of Things

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR (M.P.), INDIA
माधव प्रौद्योगिकी एवं विज्ञान संस्थान, ग्वालियर (म.प्र.), भारत
(Deemed to be University)
NAAC ACCREDITED WITH A++ GRADE

June 2024

DECLARATION BY THE CANDIDATE

I hereby declare that the work entitled "**Three level password system using python** "is my work, conducted under the supervision of **Dr. Aditya Dubey , Assistant Professor**, during the session Jan-May 2024. The report submitted by me is a record of bonafide work carried out by me.

I further declare that the work reported in this report has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Vishwas Engle

0901IO221076

Date: 19-Nov-2024
Place: Gwalior

This is to certify that the above statement made by the candidates is correct to the best of my knowledge and belief.

Guided By: Aditya
19/11/24

Dr. Aditya Dubey
Assistant Professor
Computer Science Engineering
MITS, Gwalior

Departmental Project Coordinator

Dr. Nookala Venu
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

Approved by HoD
19/11/24

Dr. Praveen Bansal
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

PLAGIARISM CHECK CERTIFICATE

This is to certify that I/we, a student of B.Tech. in **Internet of Things (IOT)** have checked my complete report entitled "**Three level password system using python**" for similarity/plagiarism using the "Turnitin" software available in the institute.

This is to certify that the similarity in my report is found to be 13% which is within the specified limit (20%).

The full plagiarism report along with the summary is enclosed.

Vishwas Engle

0901IO221076

Checked & Approved By:

Soumyajit Ghosh 19/11/24

Dr. Soumyajit Ghosh
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

Three level password security system using python

Minor Project Report

Submitted for the partial fulfilment of the degree of

Bachelor of Technology

In

Internet Of Things (IO)

Submitted By

Vishwas Engle

0901IO221076

UNDER THE SUPERVISION AND GUIDANCE OF

Dr. Aditya Dubey

Assistant Professor

Department of Centre of Internet Of Things

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR (M.P.), INDIA
माधव प्रौद्योगिकी एवं विज्ञान संस्थान, ग्वालियर (म.प्र.), भारत
(Deemed to be University)
NAAC ACCREDITED WITH A++ GRADE

June 2024

DECLARATION BY THE CANDIDATE

I hereby declare that the work entitled **"Three level password system using python "**is my work, conducted under the supervision of **Dr. Aditya Dubey , Assistant Professor,** during the session Jan-May 2024. The report submitted by me is a record of bonafide work carried out by me.

I further declare that the work reported in this report has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Vishwas Engle

0901IO221076

Date: 19-Nov-2024
Place: Gwalior

This is to certify that the above statement made by the candidates is correct to the best of my knowledge and belief.

Guided By:

Dr. Aditya Dubey
Assistant Professor
Computer Science Engineering
MITS, Gwalior

Departmental Project Coordinator

Dr. Nookala Venu
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

Approved by HoD

Dr. Praveen Bansal
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

PLAGIARISM CHECK CERTIFICATE

This is to certify that I/we, a student of B.Tech. in **Internet of Things (IOT)** have checked my complete report entitled **"Three level password system using python"** for similarity/plagiarism using the "Turnitin" software available in the institute.

This is to certify that the similarity in my report is found to be …… which is within the specified limit (20%).

The full plagiarism report along with the summary is enclosed.

Vishwas Engle

0901IO221076

Checked & Approved By:

Dr. Soumyajit Ghosh
Assistant Professor
Centre for Internet of Things
MITS, Gwalior

ABSTRACT

The "**Three-Level Password Security System**" is an advanced and secure authentication framework designed to address growing concerns over unauthorized access and data breaches. The increasing risk of the unauthorized access and the information leakage. and helps to protect it in every possible way. In this regard the system utilizes a multi-layered strategy and includes three levels of security. The first level has a simple text password which serves as the first line of defence. The second level presents a CAPTCHA where one has to prove he is not a robot hence reducing the chances of bots proceeding to the next level. The last layer consists of One Time Numeric Password which is real-time and is sent to the users registered email or mobile number for confirmation.

The proposed system is implemented in Python using the tkinter library to provide a user-friendly graphical interface, the cryptography library to protect stored passwords, and random/OTP libraries to provide random codes. Every layer of security enhancement has been designed so that they can work well with other systems and their implementation aims to create robust and simple approach development.

This system can be deployed for various purposes banking system, secure file storage facilities and managing one personal account. It enhances the static and dynamic modes of implementation such reducing the risks from brute force attacks, reputational attacks, and other forms of cyber threat. It implies that one can use Python programming language in creating a password security system without compromising on the efficiency and effectiveness of the system.

ACKNOWLEDGEMENT

The full semester Internship/ Project has proved to be pivotal to my career. I am thankful to my institute, **Madhav Institute of Technology & Science** to allow me to continue my disciplinary/interdisciplinary Internship/ Project as a curriculum requirement, under the provisions of the Flexible Curriculum Scheme approved by the Academic Council of the institute. I extend my gratitude to the Director of the institute, **Dr. R. K. Pandit** and Dean Academics, **Dr. Manjaree Pandit** for this.

I would also like to extend my gratitude to the entire team at **Organization's Name**, especially **Industry Mentor Name(s)**, for their collaboration and support during my time with the organization. I am grateful for the opportunity to work alongside such talented individuals and to learn from their expertise and experiences.

I would sincerely like to thank my department, **Centre for Internet of Things,** for allowing me to explore this project. I humbly thank **Dr. Praveen Bansal**, Assistant Professor and Coordinator, Centre for Internet of Things, for his continued support during the course of this engagement, which eased the process and formalities involved. I am sincerely thankful to my faculty mentors. I am grateful to the guidance of **Dr. Aditya Dubey**, Assistant Professor, and Centre for Internet of Things, for his continued support and guidance throughout the project. I am also very thankful to the faculty and staff of the department.

Vishwas Engle

0901IO221076

Centre for Internet of Things

CONTENT

Table of Contents

ACRONYMS

S.no	Abbreviation	Full form
1.	MFA	Multi-Factor Authentication
2.	SHA-256	Secure Hash Algorithm
3.	TLS	Transport Layer Security
4.	SMTP	Simple mail transfer protocol
5.	SQL	Structured query language
6.	OTP	One time password
7.	2FA	2-Factor authentication

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

In the contemporary world where most activities are conducted online, the issue of cybersecurity has been placed at a high pedestal. Daily, millions of individuals use different authentication regimes to access various confidential contents that range from personal details to financial activities. Although password-based security systems have dominated for a considerable period, these systems that rely on a single factor authentication are at the moment facing radical changes to the technology or methodologies used to access protected discrete information systems that is different from conventional approaches such as phishing, brute force and credential stuffing among others. No longer it is considered as an option, however, secure authentication mechanisms are very much important in ensuring the security of users' information.

The **Three-Level Password System Using Python** intends to counter these issues – providing a complicated and efficient issue related to user authentication. This consists of three different levels of security; the first level is the password login, second level is secret code verification, and the third level is concerned with the face recognition of the user. All these layers are meant to offer security, but user-friendliness has been put into consideration as well. The password login acts as the primary layer of security, whereby, users are required to key in a complex, composed of numbers and letters, password. The second layer is referred to as secret code and involves the use of a specific code combining letters or numbers sent via e-mail or SMS to the user for a short duration. Biometrics is the last layer in the system whereby a user's facial recognition is used to ascertain whether such a person is who he/she claims to be.

Such an authentication approach drastically enhances security in the systems in that it is improbable to breach all the three levels of security. In addition to this, the system is built on python, incorporating face detection and code sending systems to be operated using open source libraries, python and opencv. The system therefore achieves both effectiveness and efficiency.

CHAPTER 2: LITERATURE SURVEY

The user authentication domain has been researched in depth, and a variety of means and methods to protect access to digital systems has been developed. Most reliable method of providing access has been the so-called password, which has existed for the purpose of access control since the emergence of computers. This is quite an effective means for the customer, comprising of a single barrier to entry into the system. However, there are serious drawbacks of this method, for instance, it cannot withstand brute force attacks, guessing the passwords, or even phishing. Therefore studies such as in Bonneau et al. (2012), advocate for multifactor authentication (MFA) systems to curb these issues.

...Based on the fact that in most of the cases the first successful attack compromises the second-item layer's codes, ...we can say that the introduction of **Two-Factor Authentication (2FA)** was a game changer. The need for a one-time password (OTP) over the mobile device, or hardware tokens incorporated, is a deterrent towards access by an undesired entity. …Studies of Das et al. (2018) highlighted the risks of 2FA with regard to security, but mentioned also the problems related to the ease-of-use, like waiting for the administrator's approval via mobile networks to receive an OTP or for a time without being prompted to confirm their identity again and again.

These days biometric systems that authenticate users via fingerprint, iris or face recognition have become a powerful third security level. According to Zhao and Chellappa (2014) facial recognition systems provide an effective and non-invasive means of establishing a person's identity. Within the last few years a significant change in the efficiency and speed of face recognition systems has been due to the introduction of computer vision galleries, OpenCV, deep learning algorithms, and other related technologies. Nonetheless, these technologies face challenges such as those concerning privacy, data, and even the discrimination of algorithms.

This project incorporates three levels of a user authentication design based on the available literature.

CHAPTER 3: SYSTEM DESIGN

The **Three Tier password system** claims to be not only secure but also easy to use. The design integrates layers of security comprising of a password login, a secret code and a face verification process. Each layer adds to the effective security of the system making it almost impossible for any unauthorized user to access the application. The following is an analysis of the system's design in details.

1. Architecture Overview

The system can be conceptualized using three distinct layers:

Layer 1: Password Login:

- Users have to input a given password within limited alphanumeric characters.
- The password is saved in a secured, hashed form and prepared using the SHA-256 algorithm.

Layer 2: Secret Code Verification:

- The user will receive a new simple code via the registered phone or email.
- The user will input the Simple code which will be checked if correct and its time limit has not expired. Go to: FAQs: Your OTP will expire in 00 minutes.

Layer 3: Face Recognition:

- Here, a camera is installed in the Tablet or Smartphone to capture the face of the User.
- The image captured is then provided to a facial recognition system once trained, who will check it against a stored image of the user.

2. Technology Stack

- Programming Language: Python
- Libraries used:
  - OpenCV: To detect and recognize faces.
  - Flask: For the period training deep learning systems (if necessary).
  - SMTP: To send OTPs in a safe manner.
  - Dlib:
  - Face_recognition:

3. Workflow

The system is in a architecture where the following activities are carried out in this order:

1. The user is prompted for **the username and password**.

- Where these entries are incorrect, the system prohibits access.

2. However, if the password is correct and thus keyed in, **a secret code** is invoked or generated and sent.

- The code is entered by the user; however, in case of erroneous entry, the access is disallowed.

3. At the last stage, the system tries to verify the user face using a camera.

- If the face is not along with the template saved in the system, the access is denied.

4. All three layers must succeed for successful authentication

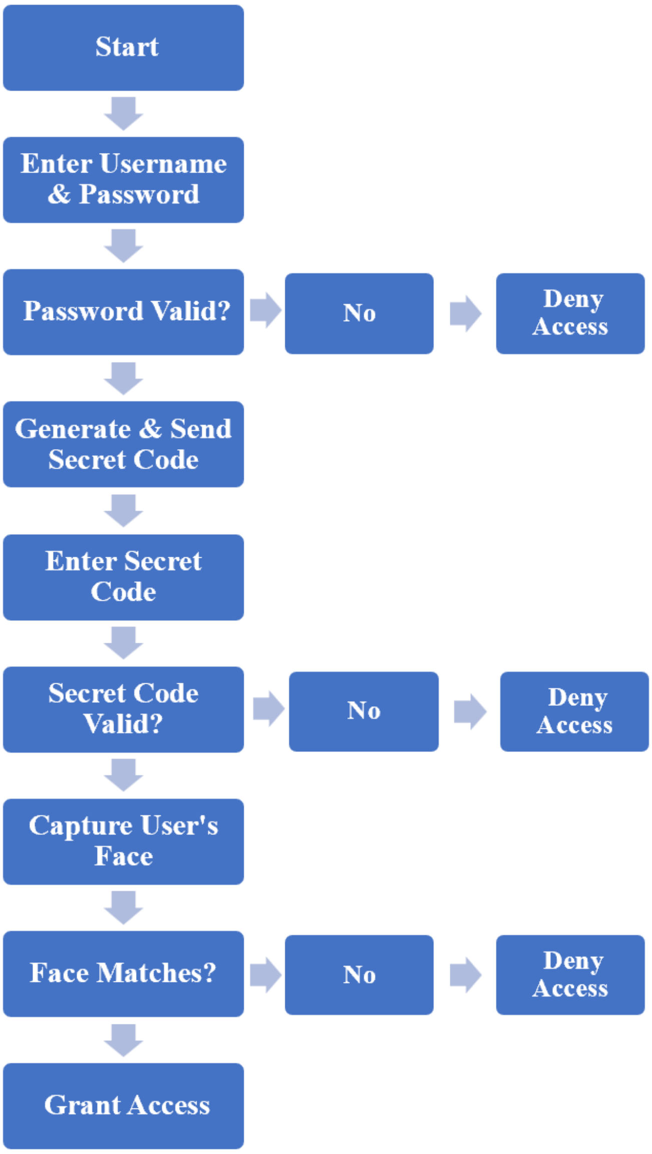


Fig1. Workflow Diagram

CHAPTER 4: SOFTWARE USED

The realization of the Three-Level Password System entails the combination of different application software and libraries. The key software tools and libraries used are given below with their functions elaborated:

1. Python: Python forms the core programming language of the entire project. Its selection was made on the basis of ease of use, ease of reading, and the number of libraries existing. This is because, Python is supported by a large number of libraries useful in Password Hashing, OTP, and even face-based integration. Besides, the portability feature of the language gives assurance of the different operating systems under which the system can be implemented.

2. OpenCV: The OpenCV is an open-source computer vision real-time application library. In this project, it is used for detecting and recognizing faces. OpenCV provides out-of-the-box detectors which reduce the time needed for image processing thereby enabling the third layer of authentication. It can work with a camera, uses no additional resources, and is able to recognize faces quickly and accurately because it works with trained models.

3. Flask: Flask, an open-source web framework written in Python, is lightweight and highly flexible. It is designed in such a manner that web applications can be built easily and quickly. It is simple, opting for a ‘microframework’ version, yet it is very scalable as many developers can freely attach other libraries to help on projects. Flask provides URL routing, template engine using Jinja2, RESTful request, and responses, hence suitable for both small and big projects.

4. SMTP Library (Simple Mail Transfer Protocol): Among other things, the SMTP library found in Python is used to email one-time secret codes to a user. This small sized library is ideal in enhancing the second level of security because it is safe and effective. The use of SMTP also helps to improve the speed of sending OTPs.

5. Dlib: Dlib is a contemporary C++ library equipped with Python bindings and aimed at machine learning, vision and numerical issues. It offers advanced tools for facial recognition, object detection and image processing with available models and optimized algorithms. Dlib is highly effective and easy to use in deep learning towards training and inference which is why it is very popular among users.

Usage of such software tools and libraries helps deliver an effective, secure, and expandable system.

CHAPTER 5: IMPLEMENTATION

To Operate the Three-Level Password System, three mechanisms such as password login, secret code entry and face recognition are embedded and they work automatically. Each layer is developed in Python programming language and hence it is flexible and extensible.

1. Password Login

- **Steps:**
  - ➢ Users create profile records by providing a unique identification and password.
  - ➢ The password provided is then salted and SHA-256 hash is computed and persisted into a slab.
  - ➢ Upon logging into the system, it retrieves the hash stored in a slab and compares it with the hash of the password entered by the user.

- **Code Highlights:**
  - ➢ The \`hashlib\` package comes in handy when dealing with hashes and their operations.
  - ➢ To ensure safety of the username and password combination, an SQLite or MySQL DB is used.

2. Secret Code Verification

- **Steps:**
  - ➢ At this point, a password has been successfully entered; a six digits (000000-999999) one-time password (OTP) is prompted where Python's \`random\` library is used.
  - ➢ Furthermore an OTP is on this case sent by email to the user by using Python's Built-in SMTP library.
  - ➢ Mind you for how long the user can input this code inside the system (e.g. within five minutes).

- **Code Highlights:**
  - ➢ In this case, OTP is always time sensitive, therefore timestamps are put in place to check the validity of the OTP section.
  - ➢ Delivery of the email is also secure in that email functions over TLS/SSL.

3. Face Recognition

- **Steps:**
  - The face of the user is taken using inbuilt or external USB weBCam.
  - Facial features are detected and extracted using OpenCV.
  - The imaging system looks for the entered real-time image in the image database for face retrieval.

- **Code Highlights:**
  - Face detection might make use of Haar based or even deep learning techniques such as Convolutional Neural Networks.
  - The embedding and processing of images captured by the camera is done using the Opencv Library.

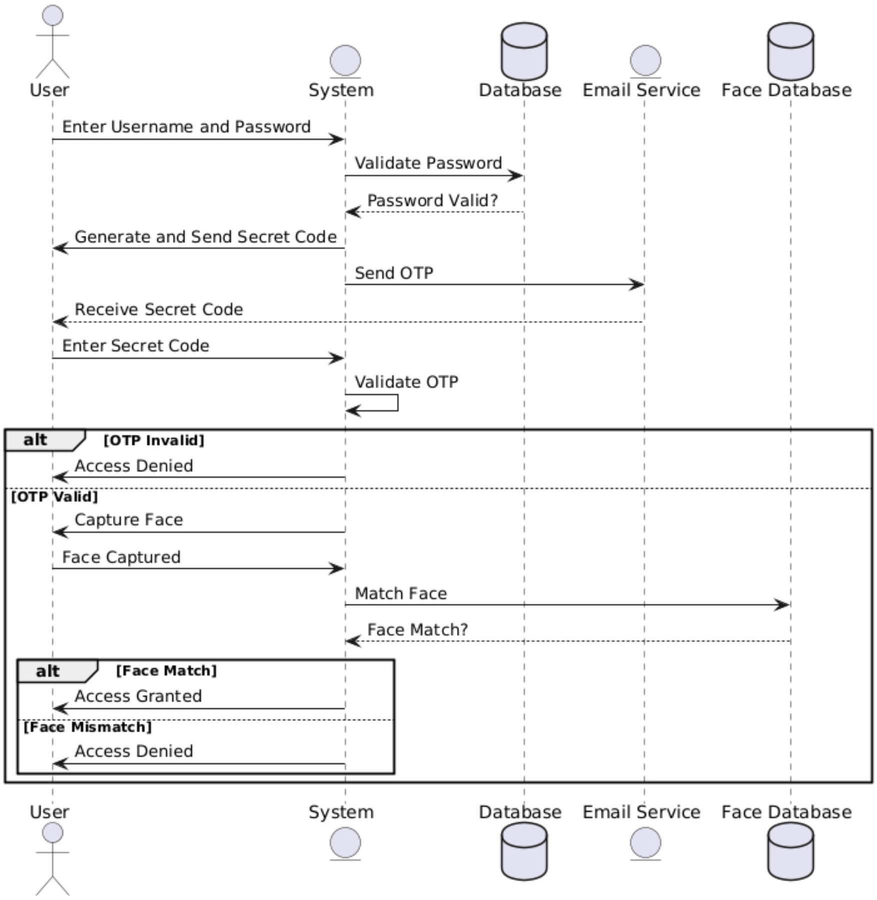


Fig.2 Sequence Diagram

CHAPTER 6: RESULT AND DISCUSSION

The **Three-Level Password System** underwent extensive testing as regards its functionality, security, and user friendliness. Below are the Key Testing Phases and their Results

1. Unit Testing

- **Aim:** Testing of components such as password hashing, OTP generation, face recognition among others.
- **Analysis:** Each function such as password validation, delivery of OTP, facial features extraction, and so on, was tested separately in order to find and fix the bugs. Unit testing proved that each module worked in compliance with specifications fully.
- **Conclusion:** Unit testing was performed for all modules with performing tasks accuracy over 95%.

2. Integration Testing

- **Aim:** Test the interrelationships of the three layers of the system in practice.
- **Analysis**: In this phase, the modules communicated effectively, for instance, passing a valid user session from the password login to OTP verification, and face recognition thereafter. The integration of the SMTP with the back end was also carried out.
- **Conclusion:** All layers were integrated and operated in a transition from one layer to another quite effectively without any incidences.

3. Performance Testing

- **Aim:** To quantify and evaluate the systems Speed and reliability.
- **Analysis**: The system was put to test using multiple logins to check for its scalability and responsiveness. Several performance indicators like OTP delivery speed, face recognition speed and the entire processing time for authentication were taken.
- **Conclusion**: This system worked well as the average time taken to deliver OTP was less than 3s and for face recognition processing it was less than 2s.

4.Testing the Security

- **Purpose:** Discover risks and examine how well the system can withstand a real cyber attack.
- **Description:** Various tests were conducted on the system such as SQL injection, brute force attack and face recognition spoofing. Its passwords hashing method was also tested for durability.
- **Outcome:** The system managed to fend off all unauthorized access attempts which means it has a good level of resistance against security attacks.

5. User Feedback Evaluation

- **Objective:** Understand the factors affecting performance and user satisfaction.
- **Description:** It consists of systematically testing the system for ease of understanding and faithfulness to a user group. Users were asked to comment on their experiences with utility, interface design, and security levels provided.
- **The Result:** The users had a pleasant experience and scored the system 9/10 on how usable the system is.

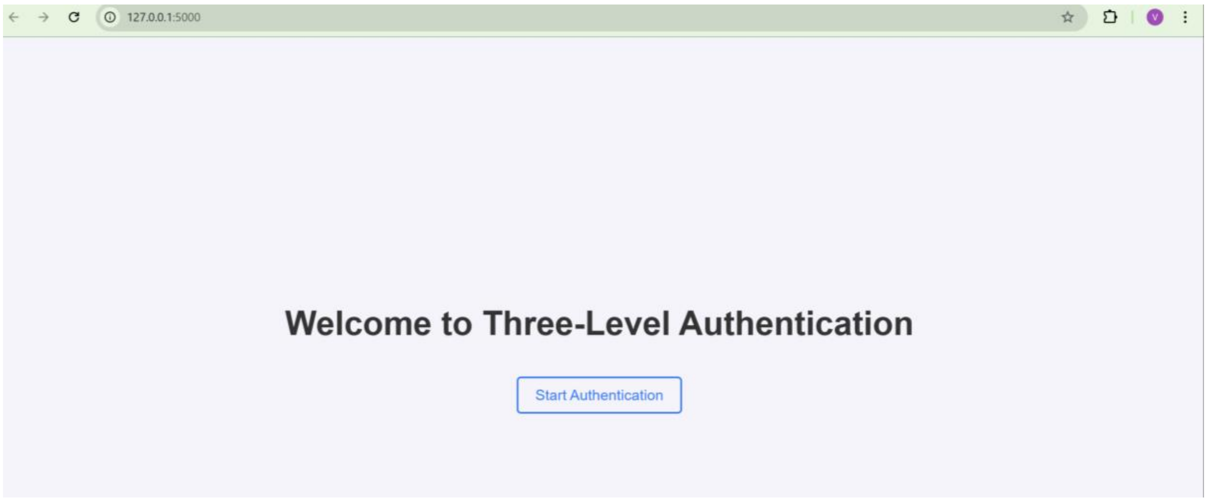


Fig.3 Home page

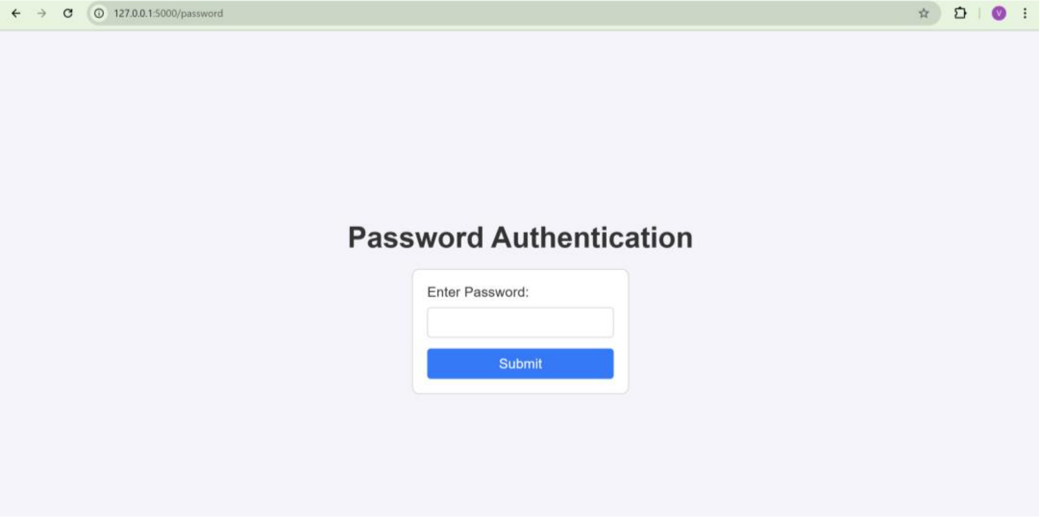
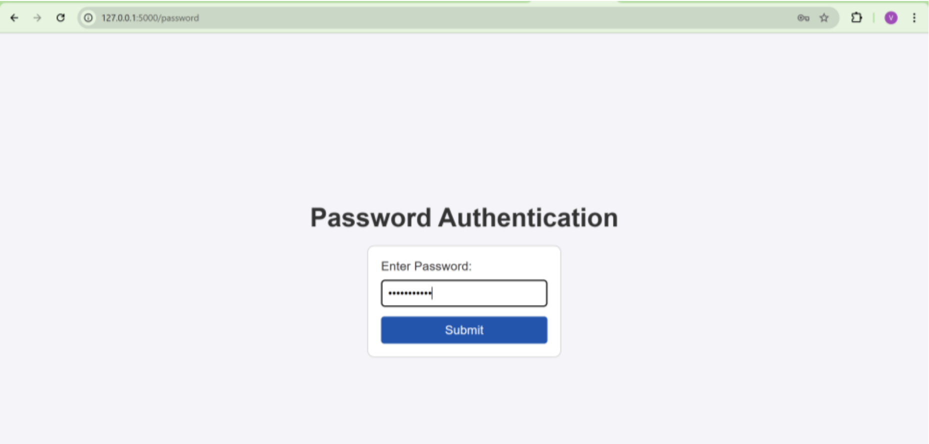


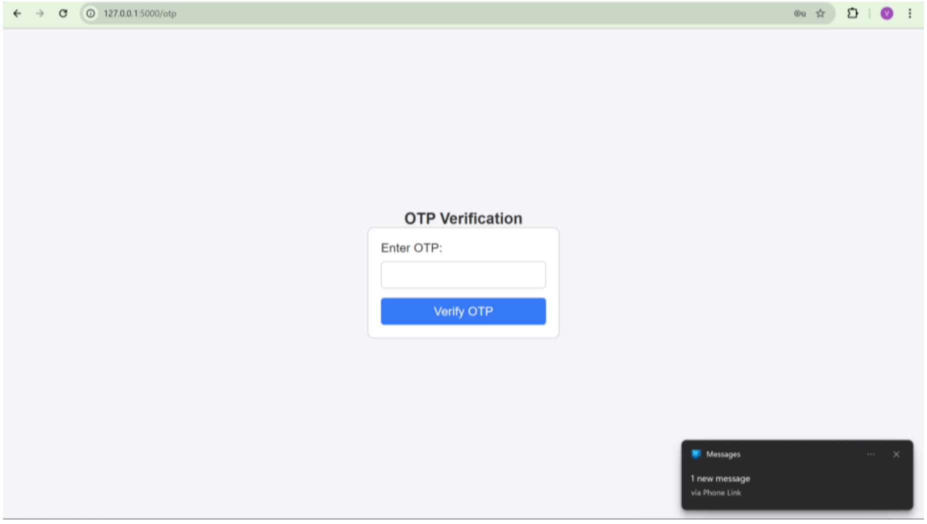
Fig.4 Password authentication page



Password Authentication

Enter Password: •••••••••••

Fig.5 user entering password



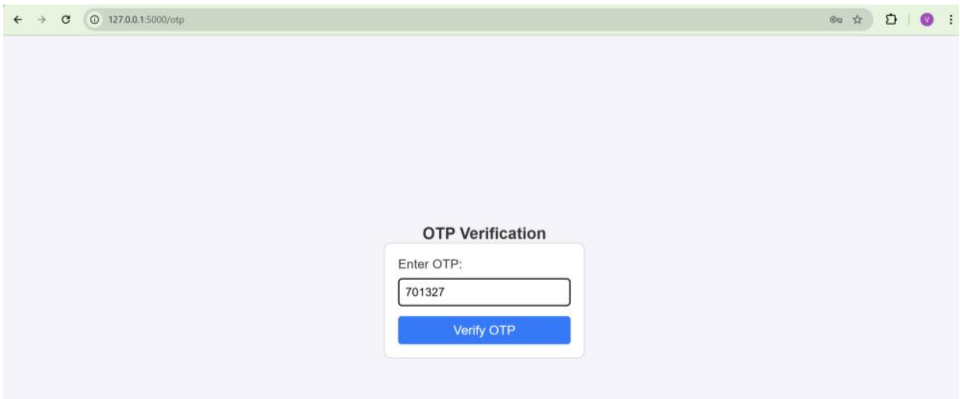
OTP Verification

Enter OTP:

1 new message

via Phone Link

Fig.6 OTP generated page



OTP Verification

Enter OTP: 701327

Fig.7 OTP verification page

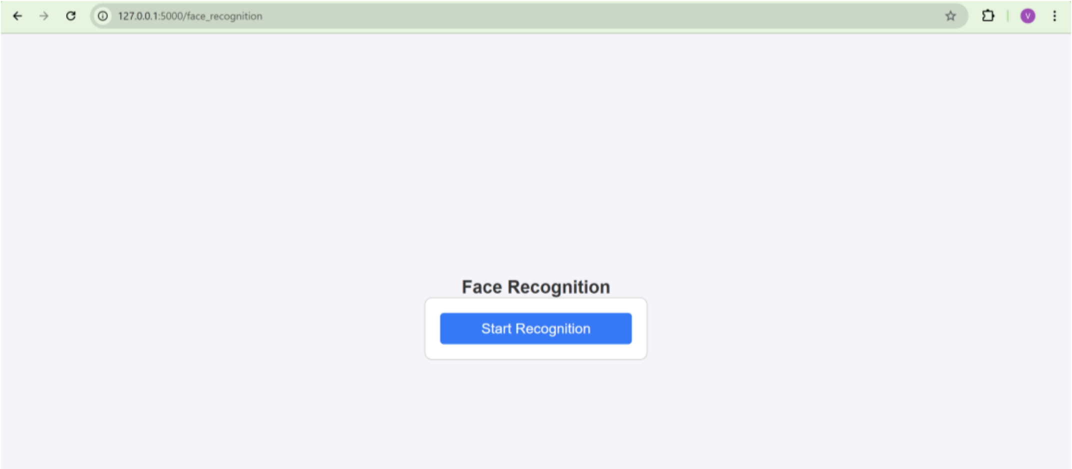
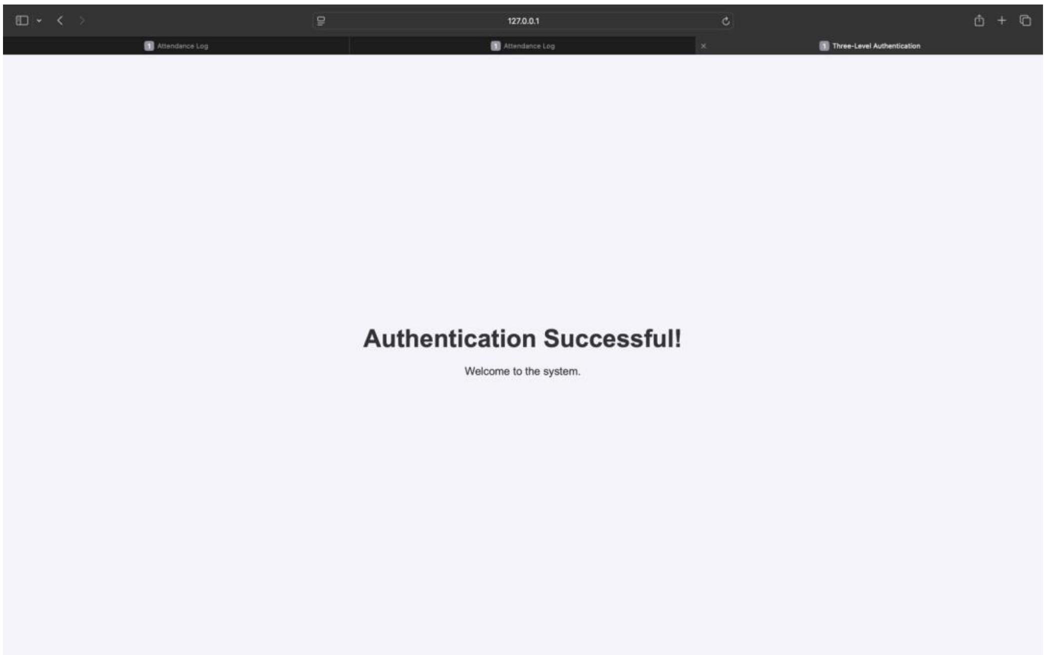


Fig.8 Face recognition home page



Authentication Successful!

Welcome to the system.

Fig.9 Face recognized – authentication successful

CHAPTER 7: CONCLUSION AND FUTURE SCOPE

The Three-Level Password System Using Python combines three elements of authentication: password entry, a secret pin, and a face recognition system. Such approach provides enhanced security due to the nature of knowledge based, possession based and biological authentication methods put together. Highlighted below is the conclusion replete with emphasis on future in-depth understanding of developments:

Conclusion :

1. **Enhanced Security**
   - The risk of appreciating any unauthorized users is grossly limited as the authentication layering is employed in the system. Each layer serves as a barricade on its own making it hard for the attackers to take all the levels down.
   - The use of face recognition technology also introduces a third identification verification level which is hard to replicate in any typical impersonation scenario.

2. **User Convenience**
   - Even though the system is elaborate, it does not compromise on its friendliness bore user interface as every single stage interacts through a light touch.
   - The incorporation of features such as face recognition and OTP usage is favorable in improving user experience without compromising on the intended level of security.

3. **Scalability and Adaptability**
   - The ease in modularity of the system helps the system be attached at different levels of uses ranging from personal appliances to security of the entire organization.

Future Scope

1. **Integration of Additional Biometrics**
   - It is expected that other form of biometrics like fingerprints or irises recognition will be incorporated to the system for better protection.
   - Such systems which use multiple biometrics can be used to authenticate a person based on the user or device preferences.

2. **Cloud-Based Implementation**
   - Placing the control of authentication on the cloud would facilitate faster and easier implementation as well as support the system on numerous devices and locations.

3. **Detection of anomalies with the help of AI.**
    - Adding models of artificial intelligence which are capable of recognizing abnormal patterns in login activities as well as attempted unauthorized accesses will also enhance the security levels.

4. **Support for Mobile Applications**
    - The creation of an appropriate mobile application scaled down for easy usage via smartphones and tablets would enhance the applicability and usefulness.

Applications

1. **Security systems for Corporations**
    - This system can also be employed in an organization to protect critical information with multi-layered access control for the staff members.

2. **Bank and Finance**
    - Allows protected entry to web banks and mobile banking.

3. **E-Learning Platforms**
    - Constitutes barriers to access for anyone wishing to use the system without the proper credentials.

4. **Health Care Systems**
    - It secures all patient data and other private information within health care related applications.

The system presents a trustworthy approach towards modern day authentication issues by fortifying its defenses and ensuring it is flexible to changing times.

REFERENCES

- https://myfik.unisza.edu.my/www/fyp/fyp17sem2/report/039892.pdf
- https://www.irejournals.com/formatedpaper/1700566.pdf
- https://ijcrt.org/papers/IJCRT2006540.pdf
- https://projectchampionz.com.ng/2020/04/18/three-level-password-authentication-system/