Design and Implementation of Two-Factor Authentication (2FA) through Facial Recognition and Password/Code for Social Media

Olalekan Ihinkalu[1,2*]; Alfa Solomon[3]; Solomon J. Shigaba[4]; Okidi O. Joshua[5]; Victor Emmanuel[6]; Shaibu S. Victor[7]

[1]Department of Computer Engineering, Eastern Mediterranean University, Magusa, North Cyprus
[2,3,4,5,6,7]Federal University Lokoja, Kogi State, Nigeria, Department of Computer Science.

Correspondence Author: Olalekan Ihinkalu[1,2*]

Publication Date: 2025/03/25

Abstract: The social media has become a platform for individual, group of companies and people to interact with one another and also as sources of relevant information. It has aided interaction between individual and business services made through social networks. Some commonly used social media applications are Facebook, WhatsApp, Instagram, Snapchat, Twitter, and WeChat etc. The challenge with the social media is the possibility of people using other people's password to gain access to their account, however, the focus of this research work is to design and implement a 2FA authentication using password and facial recognition system to aid security on this application. Two factor authentication system is an authentication system in computer which uses a two-way verification mechanism for the person who wants to gain access to his/her personal account. The two factors which is used in this research are security code or password which is the first factor authentication and facial recognition system which is the second factor authentication. This research focuses on how the face recognition is use to identify the authentic owner of the account through web cam before given access to the user. The methodology used was Agile and the application was developed with PHP, CSS, BOOTSTRAP AND HTML technologies for the frontend and Django, MYSQL frame work for the backend.

Keyword: *Authentication, Facial Recognition System, Automated Teller Machines, Social Media Network, Two-Factor Authentication, Point of Sale and Media platform.*

How to Cite: Olalekan Ihinkalu; Alfa Solomon; Solomon J. Shigaba; Okidi O. Joshua; Victor Emmanuel; Shaibu S. Victor (2025). Design and Implementation of Two-Factor Authentication (2FA) through Facial Recognition and Password/Code for Social Media. *International Journal of Innovative Science and Research Technology*, 10(3), 895-903. https://doi.org/10.38124/ijisrt/25mar438

I. INTRODUCTION

Social media encompasses a range of digital platforms designed to foster human interaction, enabling the seamless exchange of information, ideas, and experiences within virtual communities and networks. Accessible through web-based applications on computers and mobile apps on smartphones and tablets, these platforms have revolutionized the way individuals and organizations communicate, engage with content, and build connections. By actively participating in these digital spaces, users contribute to dynamic ecosystems where they create, refine, and share information, driving collaboration and meaningful discourse across various fields. Beyond mere communication, social media serves as a repository for memories, a gateway to knowledge, and a medium for self-representation and professional branding. It also fuels creativity through various content forms, including blogs, podcasts, videos, and interactive gaming platforms. As digital interactions continue to shape human behavior and societal structures, the study of these evolving relationships has given rise to the field of technological self-studies. Notable platforms that exemplify this digital transformation, each boasting hundreds of millions of users, include Facebook, WhatsApp, Twitter, Snapchat, Instagram, and WeChat. [1, 11]

As a result of development in sciences and also in technology, many means of storage and exchange of information in different ways, transfer of data through the social media network, the security of information and data are very paramount. Informations need to be protected internally or externally from various attacks in order to prevent access to communication and also to ensure authenticity from both sender and receiver's end. The world generally is facing a lot of security challenges in all areas. Majority of our systems today rely solely on static passwords to verify user's identity.

Many users have tendencies to use obvious or simple password that can be guessable, also some use same password for multiple accounts, some even write the passwords and save them on their gadget or sites they visited to enable them remember the password, and brute-force can be applied to guess the passwords and the system is compromised. In order to resolve the password problems in social media platform we implement two factor authentications using facial recognition system [11].

II. REVIEW OF RELATED WORK

Social networking platforms are designed to cultivate connections among individuals, allowing them to share common interests and engage in interactive exchanges. This paper explores the rising security concerns surrounding these digital spaces and proposes strategies to safeguard users while maintaining a smooth and secure networking environment. It also examines a range of online applications, websites, and evolving digital tools that support extensive information dissemination and user engagement. Some of the security tips this paper cover for social media are Clearing browser history, two-factor verification using One Time Password (OTP), updating of Privacy Settings, avoid clicking adverts on social media, avoid using third party applications, reduction of connections with Virtual Private Networks (VPN) [2,10].

Every social media user authentication transaction uses two-way authentication mechanisms. When these two authentication system are carried out on distinct media, onetime passwords (OTP) have proven to be a more secure way than one factor authentication. The current implementation of OTP, on the other hand, limits authentication to the device rather than the user. As technology advances, the number of fraud incidents involving One Time Password based transactions has increased. As a result, there is a need to improve the security of One Time Password based transactions. This research presented is based on mathematically established properties of quantum cryptography, and it employs the quantum entanglement property to generate quantum One Time Password (QOTP) for biometric authentication. This proposed method considers the user's diverse quantum computing capabilities [3,13].

Today, almost everyone in this world uses any of the social media platforms. We send messages, share personal data, like, images & videos and many more. When comes about personal data, the security becomes a topic of great concern. Till now, many steps have been taken to protect the personal and important data from intruders. However, there are some challenges in these social media platforms. This research work represents one such problem and provided an adequate solution for this. To trounce the above discussed drawback, a technique can be used in which a pin or password could be set for individual/ each chatting, message or post which are highly confidential. This will give double security to the important data. If anyone gets access to the victim’s social media account, even then he/she will not be able to access the account for which another password has been set [4,14].

The Nigerian voting system has always been prone to various sorts of lacuna, so m-voting was proposed as a solution, it has a key flaw: securely storing the cast votes. To address this issue, blockchain technique was recommended, along with the use of two factor authentication to prevent illegible voters from voting. The main goal of this article is to create a mobile voting system that uses two-factor authentication to verify voters' identities and blockchain technology was adopted to secure and store the votes. Another system was suggested for tested with ISO 9241-11 usability model, with result indicating that it had a good usability rating, indicating that it can be used in a voting procedure [5, 7].

Password managers are important software tools that allow users to safely and securely store sensitive data such as passport and social security numbers, as well as banking passwords. However, it is always difficult for a user to remember or save a large number of login parameters for different web services. Managers of password entries solve both security and usability concerns users, so that it won’t be necessary to be used in various web services and applications. We present a two-factor authentication approach, as well as an advanced encryption scheme, as a methodology for achieving the proposed system in this work. As a result, the goal of this work is to create a secure system that uses biometrics with strong passcode that is encrypted to manage numerous user login credentials [6, 8, 9].

Authentication bypass is something that all types of debit card fraud have in common. As a result, only a safe and trustworthy authentication system can ensure a secure debit card transaction system. Many techniques to ensuring a safe authentication system have been adopted, but many of these approaches focused on Automated Teller Machines /Point of Sale (POS) terminals or E-commerce/Online transactions, therefore failing to provide full security on all fronts. In this paper, we propose a multi-factor debit card system that combines a classic Personal Identification Number code (PIN) with a mobile phone provided an (OTP) with a biometric authentication alternative to solve this problem (fingerprint). We show that this strategy protects the safety of both parties [12].

III. REVIEW OF EXISTING SYSTEM AND PROPOSED AUTHENTICATION METHOD

The existing system was designed and implemented on a two-factor authentication (2FA) login system using SMS with OTP for social media. Whereby, the first authentication is password and the second authentication uses OTP, sent to their registered number, when entered correctly give access to the user to gain access to the account [2,10].

In this research, the two types of user authentication used for this project are something you know (security code or password) and Something you are (face recognition). The first factor which we are using for authentication is the security code or password while the second factor is face recognition for social media as in the proposed system. Initially, the face of the concerned person will be stored in the database when he/she enters the system for the first time. Whenever the person wants to gain access to the system, the face of the user would be matched and compared with the earlier taken image that is stored in the database and verifies to see if the face matches, then access is granted. Only if the parameters are correct, that access is granted, else access is denied.

➢ *Justification for the Proposed System*

- Face identification/verification. unlike the existing system that uses OTP, no full identification/verification, that is, anyone can enter the code and the system gives access without confirming if it is the real owner of the account, if the code is correct, thus increasing accuracy.
- To improved security on social media. Face detection techniques helps improve surveillance efforts to track down hackers and criminals. Personal security is top most enhanced by this methods.
- Easy to integrate. Face recognition and facial detection technology is easy to integrate, and the solutions is compatible with all security software.

IV. METHODOLOGY

This section of the project describes the method utilized to achieve the stated objectives of the proposed system. The methodology used in this project is Agile methodology due to its sequential, iterative release and testing for bugs of each phase successful completion of the project. The project is developed using HTML, CSS, Bootstrap and JavaScript for building and implementation of the proposed system. Figure 1 below represents the processes involved in the Agile Methodology.

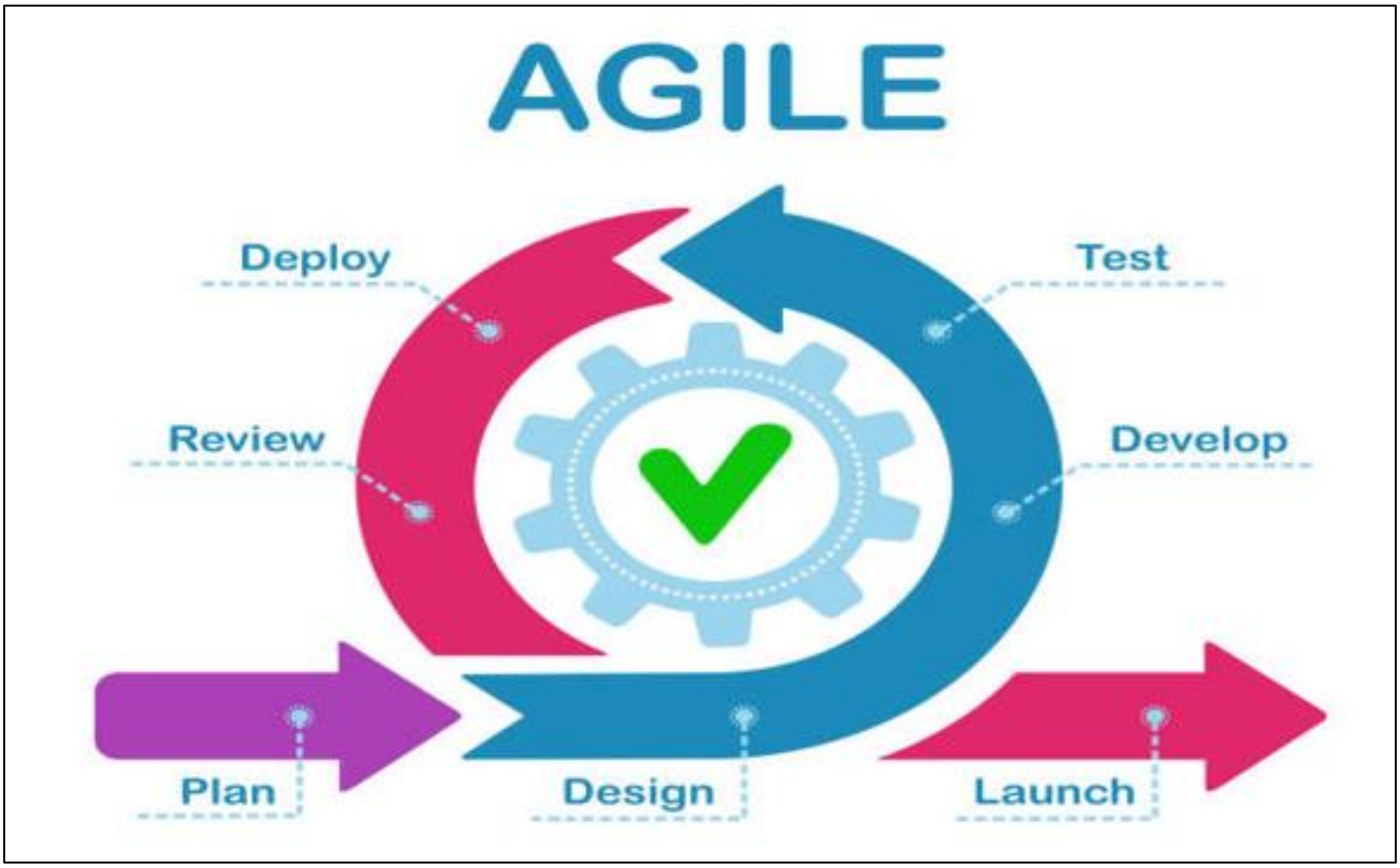


Fig 1 Agile Methodology

➢ *Here's an Overview of the Basic Agile Methodology Process:*

- **Requirements Gathering:** Requirement Gathering also known as planning stage is the stage where initial user problem is identified and look for possible solution in solving it. In this project the problem identify is the hacking of user account and the possible solution is to implement two factor authentications for web applications.
- **Design:** In this phase the architects, designers and developers work in unism to develop the software architecture. We sketch the design and with our previous idea about other application that uses two-factor authentication.
- **Develop**: the engineers work in accordance to the stipulated designed software architecture and build user stories in time-boxed sprints using the following tools Django, HTML, CSS, Bootstrap, JavaScript and jQuery.
- **Testing:** This phase, the Agile Testing team members springs in at the end of every cycle to identify inconsistencies and bugs. They conducts various test on the software and reports the bugs back to the developers. Then the developers fixes the code in the following sprints. The code was tested using web browser and necessary bug were fix.

- **Deployment:** In this phase, the Agile Developer involves launching the completed user stories in the market. They start with the launching of Minimum Valuable Product (MVPs), i.e., the basic versions and the following user stories and launches follow as the initial feedback flows in. When all the user stories are delivered and launched, the deployment is called the full-fledged product deployment.
- **Review:** Once the initial development stages are complete, the team presents the final outcome to the owner to confirm that it meets the required standards. From there, the Agile process continues—either by starting a new iteration to improve the product or moving forward to the next phase for further growth and refinement..

➢ *Justification for Iterative Development Approach (Agile Methodology)*

- *The following are the justification for Iterative Development Approach:*

✓ **Complete visibility of the progress of each project in real-time:** Another advantage of using an agile approach is the transparency of each project thanks to feedbacks due to frequent exchanges with clients. This allows them to feel more involved and ask for changes throughout the project.

✓ **Stakeholders Engagement:** This is done whereby, collaboration occurs with different stakeholders in each phases of the project, a dynamic system is built based on the trust and confidence of the various team member and this will forge stronger and greater relationships among the teams.

✓ **Cost Optimization:** The iterative development approach enhances cost management by allowing teams to reassess the budget at the end of each sprint or development cycle. This continuous evaluation enables informed decision-making on whether to proceed, modify tasks, put development on hold, or terminate the project based on resource allocation and priorities.

✓ **Enhanced Quality:** By adopting an iterative development approach, teams can divide projects into smaller phases, known as sprints, and work collaboratively to achieve high-quality outcomes.

✓ **Rapid Adaptability:** Another key advantage of this approach is its speed and adaptability, as it is designed to accommodate change throughout the development process. If project objectives shift, the methods and workflows are quickly adjusted to align with new requirements and expectations.

V. RESULT AND DISCUSSION

➢ *Architectural Design of System Architecture*

A web-based system is structured into two core layers: the user interface usually the (front-end) and the database and server-side logic (back-end). The front-end, commonly known as the client-part, is everything that the user sees and interacts within inside their browser. The main purpose of the client-side is to collect data from users. It is written in variants of HTML, CSS, Bootstrap and JavaScript. After which, we have the back-end, also known as the server-part of the app. It is the part, which is not accessible by users; it stores and manipulates data. The backend processes HTTP requests which essentially "fetch" the data (text, images, files,….) etc. called for by the user. And Django Framework was used to design the application backend, this system architecture is shown below in Figure 2.

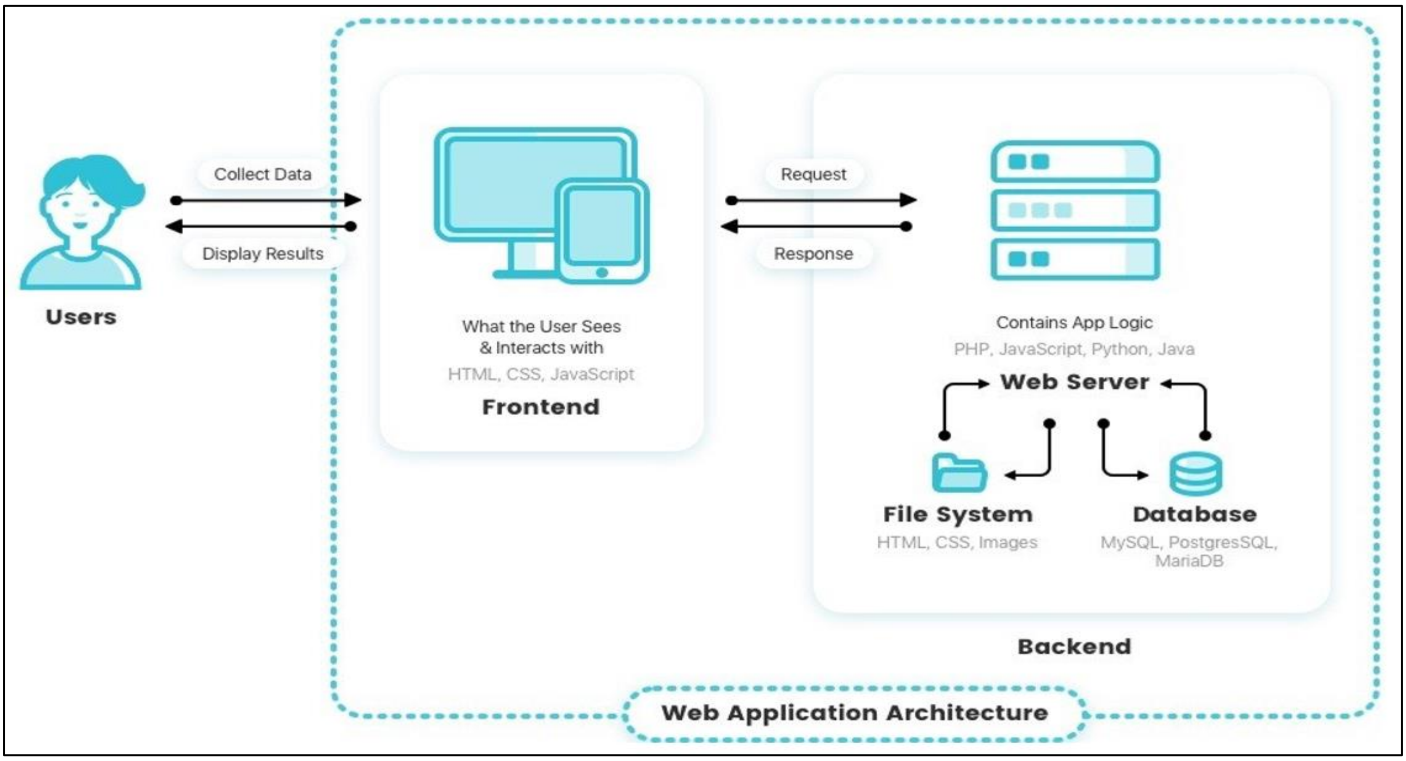


Fig 2 System Architecture [15]

- *Use Case Diagram*

Use case diagrams is used to perform requirements analysis phase in order to understand the core functionalities and usage scenarios associated with the identified requirements. Use case diagram usually shows a look at the system from an outsider (e.g. user) view. The system is treated as a black box and it solely identifies what the system may be used for. Some components of this use case diagram include, Actors, Associations, Use cases, and the system boundary.

- ✓ **Actors:** They refer to external entities, such as individuals or systems that interact with the system that was modeled.
- ✓ **Use Cases:** These define the specific functionalities of the system, representing the actions performed by an actor. For example, a customer may "view the product catalog," "select items for purchase," and "complete the payment process."
- ✓ **Associations:** These depict the connections between actors and use cases, represented by solid lines linking an actor to the corresponding system function they engage with.
- ✓ **System Boundary:** this majorly represents the scope of the system that the actor is interacting with.

The use case has two (2) main actors and about sixteen (16) use cases. The Administrator manages the system, User are the main client that uses the system. The following use case diagram illustrate the complete system. The Use-case diagram is seen in figure 3 below.

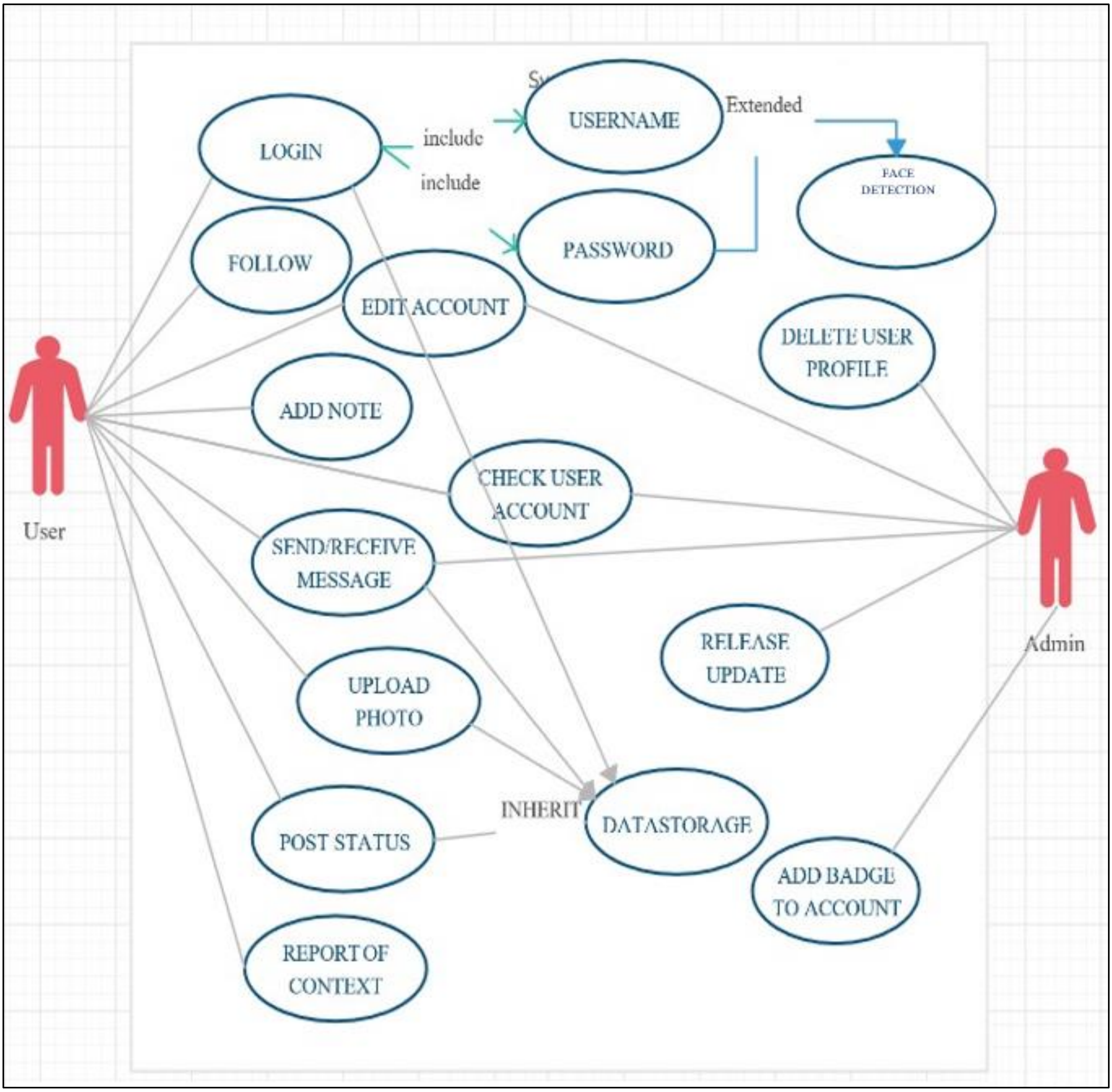


Fig 3 The Use-Case Diagram of the Web Application

➢ *Application Algorithm*

The application algorithm is a step by step process of how the system is able to achieve its goal. The application algorithm shows the interaction between the user and the system at each process. The figure shows the diagrammatic representation of the algorithm and below is the stated algorithm for the application.

- Step 1: User start/Launch Application
- Step 2: User click on create account as a new user or login as a member
- Step 3: After filling the form the webcam comes up to capture users face.
- Step 4: Grant user permission if both parameters are corrected i.e. the password and the face identification.
- Step 5: If login is successful then user can perform tasks on their dashboard.
- Step 6: End/Exit Application.

➢ *System or Program Modules Specification*

The System or Program has two (2) modules specification which include; frontend and Backend(database) from the frontend we have two modules which are sign-in and sign-out which are the major input for the users, after which the user sign-up, the web cam comes up for face verification, before user's dashboard will open. The modules are represented in Figure 4 below:

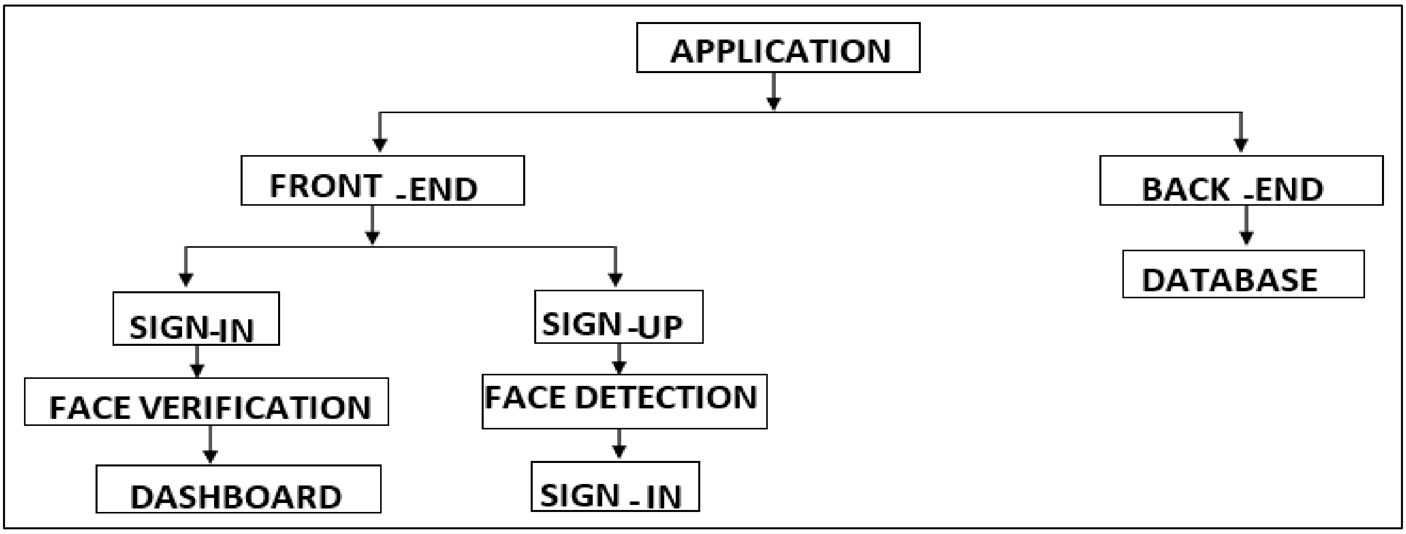


Fig 4 System or Program Modules Specification

➢ *Development Process*

The system development process started with the requirement/planning phase where communication with the intended users and stakeholders took place, current system was observed, existing documents were analyzed, and requirements (functional and nonfunctional) were gathered. It was followed by the analysis phase where the requirements and feasibility of the intended system were analyzed, then I made progress to the designing phase, where the physical and logical design of the system was produced. The development process proceeded to the implementation and testing phase where the logical and physical designs are translated into computer programs, and the outputs are validated with that of a real-life system, whenever the output is undesirable, the development process iterates to the analysis phase; this is continued until the desired system is developed. We described the development process of the application in Figure 4.8 next is Design, and then implementation which also involves an iterative process of testing the system until the desired result is achieve.

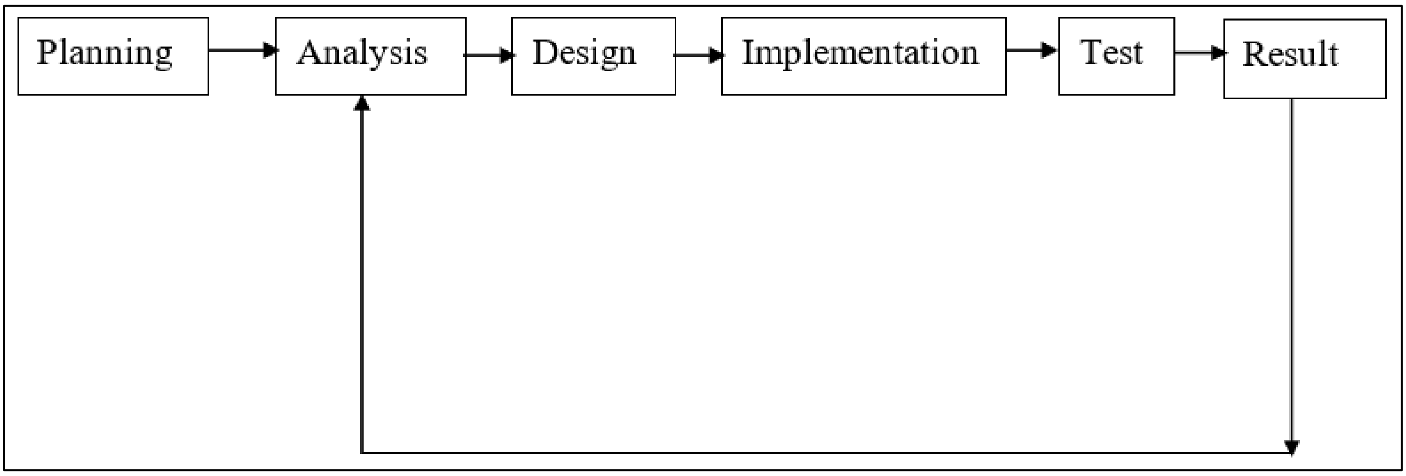


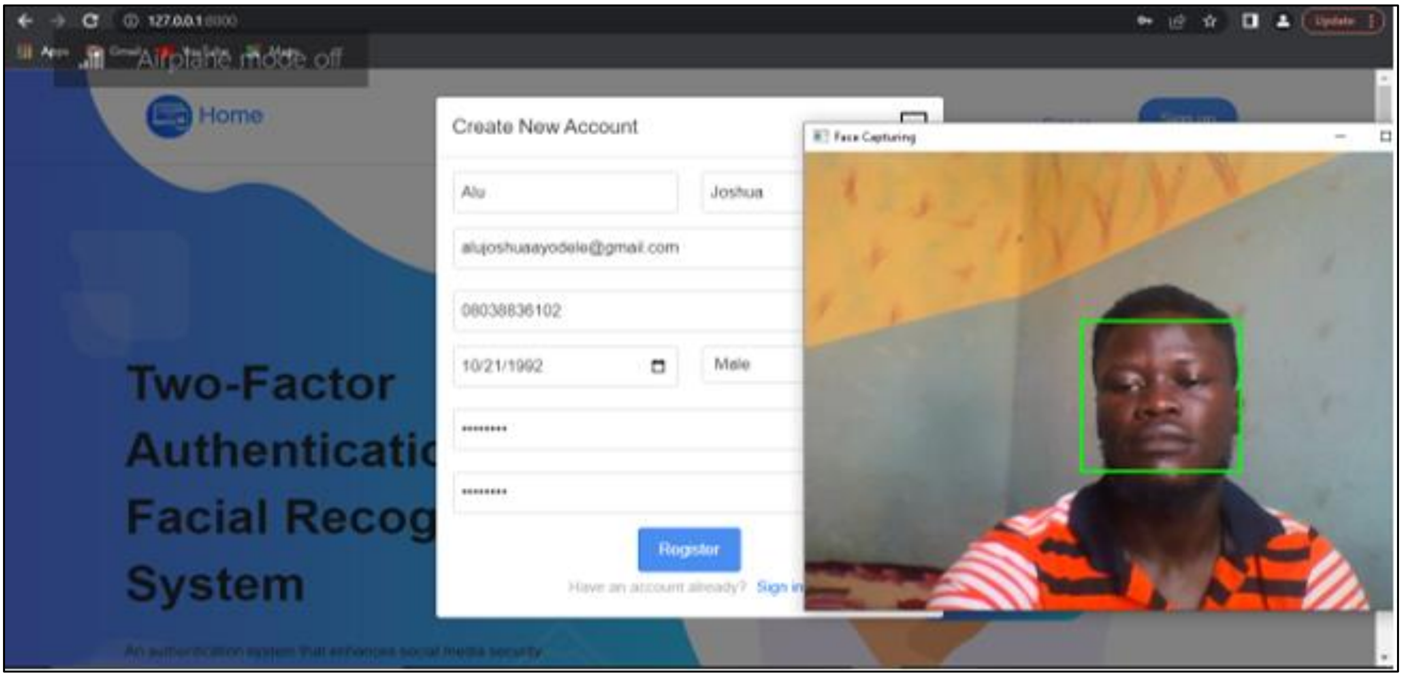
Fig 5 Development Process of the System

➢ *Application Implementation*

Application implementation however, is the actual development of the system based on detailed design specifications and it comes after coding which include sign-up page, signin page, user's dashboard and database of the application.

- *Sign-Up Page*

This is the page that accept input from user's, which allow user to enter their details to be registered and store in the database. Figure 6 below shows Sign-Up page.


Create New Account

Alu
Joshua
alujoshuaayodele@gmail.com
08038836102
10/21/1992
Male
•••••••••
•••••••••

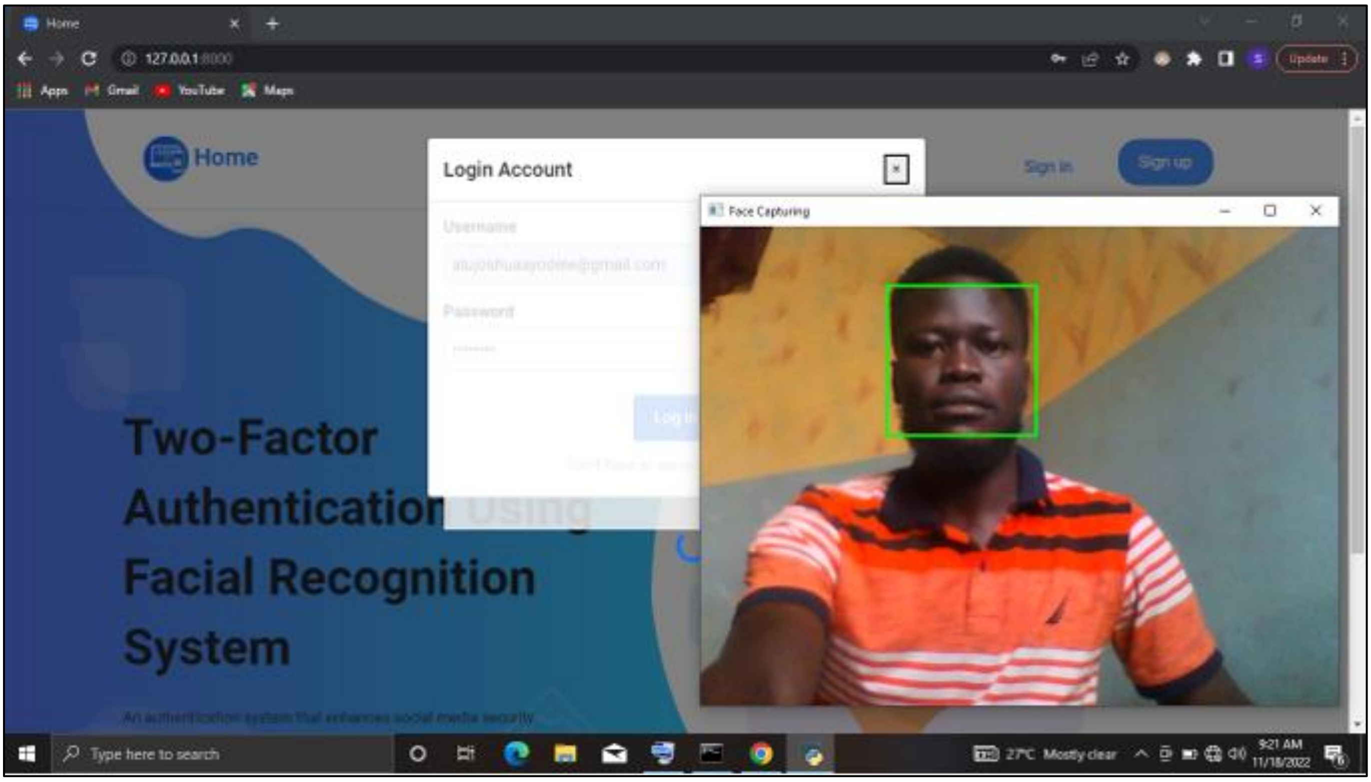
Register

Have an account already? Sign in

Fig 6 Sign-Up Page

- *Sign-In*

User's Login with their details according to their registered details if correct permission can be granted into their dashboard Figure 7 below shows Sign-In page.


Login Account

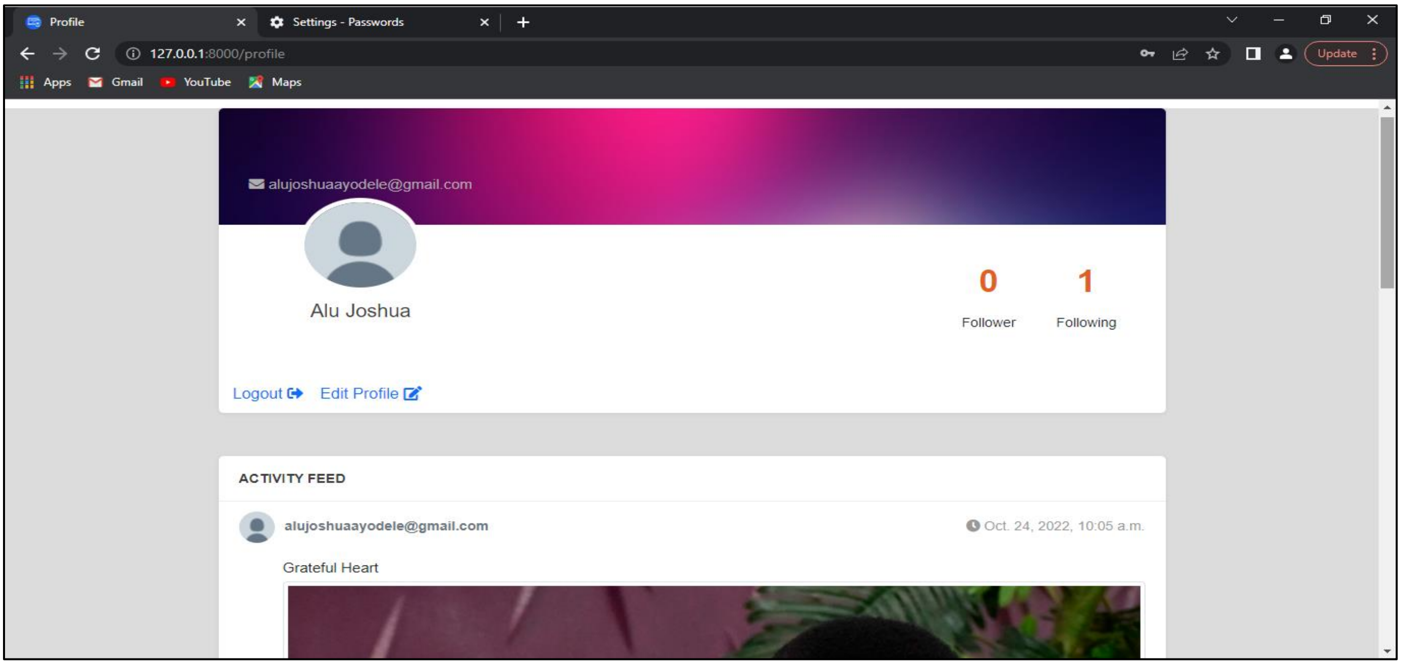
Username
alujoshuaayodele@gmail.com
Password
•••••••••

Log in

Fig 7 Sign-in Page

- *User's Dashboard*

The User's Dashboard is the result gotten from the system after users has login successfully, it entails activity feeds, the number of followers and following the user have and also user can edit profile. Figure 8 shows the user dashboard after the users account is created.



alujoshuaayodele@gmail.com

Alu Joshua

0 Follower

1 Following

Logout Edit Profile

ACTIVITY FEED

alujoshuaayodele@gmail.com Oct. 24, 2022, 10:05 a.m.

Grateful Heart

Fig 8 User's Dashboard

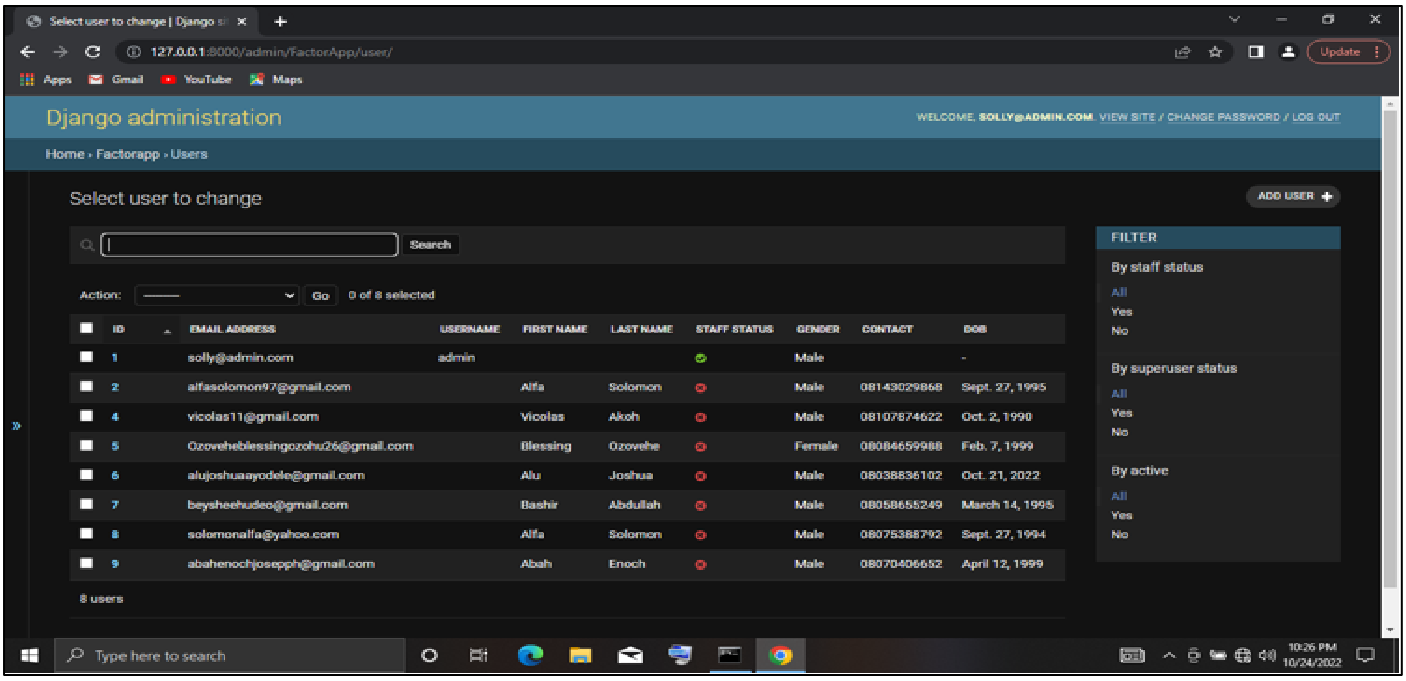
➢ *Database*

This shows the organization or arrangement of data according to the database model, which is referred to as the database schema, this system consists of signup users' data which is store on the database. Figure 9 shows the database of the system.

- *Description of Tables*

This best describes the type of datatype (character, string and integer) each table in the database contain.

- ✓ Email (char, string and int)
- ✓ First Name (char, string)
- ✓ Last Name (char, string)
- ✓ Gender (string)
- ✓ Phone Number (int)
- ✓ Date of Birth (string and int).


Select user to change | Django si
127.0.0.1:8000/admin/FactorApp/user/
Apps
Gmail
YouTube
Maps
Update
Type here to search
10:26 PM
10/24/2022

Django administration

WELCOME, SOLLY@ADMIN.COM. VIEW SITE / CHANGE PASSWORD / LOG OUT

Home › Factorapp › Users

Select user to change

ADD USER +

Search

Action: ——— Go 0 of 8 selected

☐	ID	EMAIL ADDRESS	USERNAME	FIRST NAME	LAST NAME	STAFF STATUS	GENDER	CONTACT	DOB
☐	1	solly@admin.com	admin			✓	Male		-
☐	2	alfasolomon97@gmail.com		Alfa	Solomon	✗	Male	08143029868	Sept. 27, 1995
☐	4	vicolas11@gmail.com		Vicolas	Akoh	✗	Male	08107874622	Oct. 2, 1990
☐	5	Ozoveheblessingozohu26@gmail.com		Blessing	Ozovehe	✗	Female	08084659988	Feb. 7, 1999
☐	6	alujoshuaayodele@gmail.com		Alu	Joshua	✗	Male	08038836102	Oct. 21, 2022
☐	7	beysheehudeo@gmail.com		Bashir	Abdullah	✗	Male	08058655249	March 14, 1995
☐	8	solomonalfa@yahoo.com		Alfa	Solomon	✗	Male	08075388792	Sept. 27, 1994
☐	9	abahenochjosepph@gmail.com		Abah	Enoch	✗	Male	08070406652	April 12, 1999

8 users

FILTER

By staff status
All
Yes
No

By superuser status
All
Yes
No

By active
All
Yes
No

Fig 9 Database

VI. CONCLUSION

Two-factor authentication (2FA) is one of the most efficient and effective way to make sure users are who they say they are and they comply with the input criteria to access an application. In conclusion, this research paper was to design and also implement as a two factor authentication using password and facial recognition system to aid security on social media. Two factor authentication helps secure the application from unwanted user by using a two-way verification mechanism for the person who wants to gain access to his/her personal account. The two factors authentication which was used in this research are security code or password which is the first factor authentication and facial recognition system which is the second factor authentication. This research focused on how the face recognition was used to identify the authentic owner of an account through web cam before given access to the user.

REFERENCES

[1]. Agbo F. J., Adewumi S. E. & Olalekan I.” Computer Viruses: A framework for modeling infection Susceptibility of Workstations”, Advance in Computer Science and Engineering, Vol.14, Number 2, 2015, pages 97-109. ISSN: 0973-6999; http://dx.doi.org/10.17654/ACSEMay2015_097_109

[2]. Ogbuju E., Ejiorfor V., & Olalekan I. “Sentiment Analysis for Rules –driven Instant Messaging”, Confluence Journal of pure and applied sciences. Vol.1, No.1, Nov. 2017, www.cjpas.fulokoja.edu.ng

[3]. Olalekan I. & Chefranov A. G. “Analysis, Design and Implementation of a Voting System Using a Novel Oblivious and Proxy Signature”, Eastern Mediterranean University Institutional Repository, Vol. 7, 2019, http://irep.emu.edu.tr:8080/jspui/bitstream/11129/5005/1/Ebenezerolalekan.pdf

[4]. Olalekan I. & Chefranov A. G., “Voting System Using Oblivious and Proxy Signature: A Privacy Flaw and its Fix,” http://www.pphmj.com; Advance in Computer Science and Engineering, Vol.19, June 2022, http://dx.doi.org/10.17654/0973699922001,

[5]. Olalekan I., Adewumi S. E & Helen E. O., “Adopting EVS as Solution to Nigeria Election using Proxy, Oblivious and Blind Signature, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) Vol. 11, Issue 9, September 2022 DOI:10.17148/IJARCCE.2022.11901

[6]. Olayiwola B., Olalekan I. & Veronica C., “Application of hourglass matrix in GoldreichGoldwasser-Halevi encryption scheme: Journal of the Nigerian Society of Physical Sciences (JNSPS). Vol.4, October 2022, DOI:10.46481/jnsps.2022.874

[7]. Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. Implementing a MobileVoting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. Lecture Notes in Networks and Systems,(2020),pg. 857–872. https://doi.org/10.1007/978-981-15-3369-3_63.

[8]. Alese, T., Owolafe, O., Thompson, A., & Alese, B. A User Identity Management System for Cybercrime Control. Nigerian Journal of Technology, Vol. 40(1), (2021), pg. 129–139. https://doi.org/10.4314/njt.v40i1.17

[9]. Ekundayo, H. A., Aminu, E. F., & Alabelewe, O. R. A Two Factor Authentication Protective System for Managing User Login Credentials. AICCTRA2019, (2019), pg. 95–100. Retrieved from http://repository.futminna.edu.ng:8080/jspui/handle/123456789/3539.

[10]. Majid, I., & Kouser, S. Social media and security: how to ensure safe social networking. International Journal of Humanities and Education Research, Vol. 1(1), 2019, pg. 35–38. Retrieved from http://www.humanitiesjournal.net/

[11]. Manoj, D. K. S. Cyber-Security: Detecting Identity Deception on Social Media Platforms. International Journal of Electrical Engineering and Technology (IJEET), Vol.12(1), (2021), pg. 98–108. https://doi.org/10.34218/IJEET.12.1.2021.011

[12]. Ojewale, M. A., & Yomsi, P. M. Multi-Factor Authentication and Fingerprint-based Debit Card System. U.Porto Journal of Engineering, Vol. 5(2), (2019), pg. 19–28. https://doi.org/10.24840/2183-6493_005.002_0003

[13]. Sharma, M. K., & Nene, M. J. Two ‐ factor authentication using biometric based quantum operations. Security and Privacy, Vol. 3(3), (2020). https://doi.org/10.1002/spy2.102

[14]. Singh, C., Katiyar, D., & Goel, G. SOCIAL MEDIA SECURITY. International Research Journal of Engineering and Technology (IRJET), Vol. 7(5), (2020), pg. 1196–1198. Retrieved from http://www.irjet.net/

[15]. “System Architecture” [online] Available: https://reinvently.com/blog/fundamentalsweb-application-architecture/ [Accessed 20/12/2022].