International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

Design And Development of a Web-Based Facial Login System

Ireen Mukosayi
Dept. of ICT
School of Engineering
Information and Communication University
Lusaka, ZAMBIA.

Moses Mupeta
Dept. of ICT
School of Engineering
Information and Communication University
Lusaka, ZAMBIA.

Date of Submission: 15-02-2026 Date of Acceptance: 28-02-2026

Abstract: *The increasing reliance on web-based applications has amplified the need for secure and user-friendly authentication mechanisms. Conventional authentication methods, such as usernames and passwords, are vulnerable to various security threats including password theft, phishing, and unauthorized access. Biometric authentication, particularly facial recognition, offers a promising alternative by leveraging unique physiological characteristics for identity verification.*

This study presents the design and development of a web-based facial login system that enables users to authenticate securely using facial recognition technology. The system captures facial images through a web browser, processes and extracts facial features using computer vision techniques, and performs identity verification by matching facial embeddings stored in a secure database. The proposed system is implemented using web technologies and a server-side facial recognition framework to ensure platform independence and scalability.

System performance is evaluated based on accuracy, authentication speed, and reliability using standard biometric metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). The results demonstrate that the developed system provides improved security and usability compared to traditional password-based authentication methods. The study concludes that web-based facial authentication is a viable and effective solution for enhancing access control in modern web applications.

I. INTRODUCTION

The rapid expansion of web-based applications in sectors such as finance, education, healthcare, and e-government has heightened the need for secure, reliable, and user-friendly authentication mechanisms. Authentication plays a critical role in ensuring confidentiality, integrity, and availability of information systems by preventing unauthorized access to sensitive resources (Stallings, 2018). Traditionally, most web applications rely on knowledge-based authentication methods, particularly usernames and passwords. Although simple to implement, password-based systems are increasingly susceptible to security threats such as brute-force attacks, phishing, keylogging, password reuse, and credential leakage (Gaw & Felten, 2006; Florêncio & Herley, 2007).

The limitations of conventional authentication methods have motivated the adoption of biometric-based authentication systems, which authenticate users based on unique physiological or behavioral traits. Biometrics offer improved security by linking authentication directly to the individual rather than to information that can be forgotten, guessed, or stolen (Jain, Ross, & Prabhakar, 2004). Common biometric modalities include fingerprints, iris recognition, voice recognition, and facial recognition. Among these, facial recognition has gained significant popularity due to its non-intrusive nature, ease of deployment, and compatibility with widely available imaging devices such as webcams and smartphone cameras (Zhao et al., 2003).

Facial recognition is particularly well suited for web-based systems because it does not require specialized hardware and can be integrated using standard browser-based technologies. Recent advancements in computer vision and machine learning, especially deep learning techniques such as convolutional neural networks (CNNs), have significantly enhanced the accuracy and robustness of facial recognition systems (Taigman et al., 2014; Schroff, Kalenichenko, & Philbin, 2015). These techniques enable effective facial feature extraction and matching even under challenging conditions such as varying illumination, facial expressions, and pose variations.

Despite these advancements, the implementation of facial recognition for web-based authentication presents several challenges,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

including secure storage of biometric data, protection against spoofing attacks, privacy concerns, and performance optimization in real-time environments (Ratha et al., 2001). Addressing these challenges is essential to ensure that facial authentication systems are both secure and trustworthy.

This study therefore focuses on the **design and development of a web-based facial login system** that leverages modern facial recognition techniques to provide secure and efficient user authentication. The proposed system aims to reduce reliance on traditional password-based methods while enhancing security, usability, and accessibility in web applications.

1. Motivation and significance of the study

The motivation for this study arises from the growing security challenges associated with traditional authentication mechanisms used in web-based systems. Username and password-based authentication remains the most widely deployed method; however, it has proven to be inadequate in addressing modern cybersecurity threats. Studies have shown that users often reuse weak passwords across multiple platforms, making systems vulnerable to credential stuffing, phishing, and brute-force attacks (Florêncio & Herley, 2007; Gaw & Felten, 2006). These vulnerabilities pose significant risks, particularly for web applications that handle sensitive personal and financial information.

2. Scope

The scope of this study is limited to the design and development of a web-based facial login system intended for user authentication in web applications. The system focuses specifically on the use of facial recognition as a biometric authentication mechanism to replace or complement traditional password-based login methods. The implementation targets standard web browsers and utilizes commonly available camera devices, such as webcams or integrated mobile cameras, without requiring specialized biometric hardware.

4. Problem Statement

Web-based applications increasingly serve as critical platforms for accessing sensitive information and services, making secure user authentication a fundamental requirement. Despite this, the majority of web systems continue to rely on traditional username and password-based authentication mechanisms. Numerous studies have demonstrated that password-based systems are inherently vulnerable due to weak password selection, password reuse across multiple platforms, and susceptibility to phishing and brute-force attacks (Gaw & Felten, 2006; Florêncio & Herley, 2007). These weaknesses have resulted in frequent security breaches, unauthorized access, and loss of user trust in web-based systems.

Although biometric authentication has been widely recognized as a more secure alternative, its adoption in web-based environments remains limited. Many existing biometric systems are designed for standalone or mobile platforms and often require specialized hardware, high computational resources, or proprietary software, making them unsuitable or costly for web deployment (Jain, Ross, & Prabhakar, 2004). Furthermore, concerns related to the secure storage of biometric data, privacy, and system performance continue to hinder the widespread implementation of biometric authentication in web applications (Ratha et al., 2001).

Facial recognition presents a viable biometric solution for web-based authentication due to its non-intrusive nature and compatibility with commonly available camera devices. However, implementing facial recognition in a web environment introduces challenges such as real-time image capture, accurate feature extraction under varying conditions, secure handling of biometric templates, and resistance to spoofing attacks (Zhao et al., 2003; Schroff, Kalenichenko, & Philbin, 2015). Without proper system design, these challenges can result in reduced accuracy, increased false authentication rates, and potential security vulnerabilities.

5. General Objective

The general objective of this study is to design and develop a secure and efficient web-based facial login system

6. Specific Objective

The specific objectives of this study are to:

1. Analyze existing web-based authentication methods and identify their security and usability limitations.
2. Design a system architecture for a web-based facial login system suitable for modern browser environments.
3. Develop a facial enrollment module for capturing and registering users' facial biometric data.

6. Research Questions

This study is guided by the following research questions:

1. What security and usability limitations are associated with traditional password-based authentication systems in web applications?
2. How can a web-based facial login system be designed to securely capture, process, and authenticate users using facial recognition technology?
3. Which facial feature extraction and matching techniques are most suitable for web-based authentication systems?

II. Literature Review

Authentication is a fundamental security process used to verify the identity of users before granting access to information systems. Traditional authentication mechanisms are generally categorized into three factors: something the user knows (passwords or PINs), something the user has (tokens or smart cards), and something the user is (biometrics) (Stallings, 2018). Among these, knowledge-based authentication methods, particularly usernames and passwords, remain the most commonly used in web applications due to their simplicity and low implementation cost. However, research has consistently shown that password-based systems are vulnerable to various attacks, including brute-force attacks, phishing, and credential reuse, which significantly compromise system security (Gaw & Felten, 2006; Florêncio & Herley, 2007).

Biometric authentication systems verify user identity based on unique physiological or behavioral characteristics. Common biometric traits include fingerprints, iris patterns, voice, gait, and facial features. Biometrics offer improved security over traditional methods because they are difficult to duplicate, steal, or share (Jain, Ross, & Prabhakar, 2004). As a result, biometric authentication has been widely adopted in access control systems, mobile devices, and national identification programs.

Despite their advantages, biometric systems face challenges related to privacy, template security, accuracy, and environmental sensitivity. The performance of biometric systems is often evaluated using metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR), which measure system reliability and accuracy (Ratha et al., 2001). These challenges must be carefully addressed when integrating biometric authentication into web-based platforms.

Facial recognition is a biometric technique that identifies or verifies individuals based on facial characteristics extracted from digital images or video frames. Early facial recognition approaches relied on geometric features and appearance-based methods such as Eigenfaces and Fisherfaces (Zhao et al., 2003). While these methods were computationally efficient, their accuracy was limited under varying lighting conditions, facial expressions, and pose variations.

Recent advancements in machine learning and deep learning have significantly improved facial recognition performance. Convolutional Neural Networks (CNNs) have been widely adopted for facial feature extraction due to their ability to learn discriminative features from large datasets. Models such as DeepFace and FaceNet have demonstrated near-human-level accuracy in face recognition tasks (Taigman et al., 2014; Schroff, Kalenichenko, & Philbin, 2015). These models generate compact facial embeddings that can be efficiently stored and matched, making them suitable for authentication systems.

The integration of facial recognition into web-based authentication systems has gained increasing attention due to the widespread availability of camera-enabled devices and browser technologies. Web-based facial authentication systems typically utilize browser APIs for image capture and server-side frameworks for facial processing and matching. Studies have shown that web-based biometric authentication can enhance security while maintaining usability when properly designed (Zhao et al., 2003).

However, implementing facial recognition in a web environment presents several challenges, including real-time image processing, latency, secure transmission of biometric data, and vulnerability to spoofing attacks such as photo or video replay attacks (Ratha et al., 2001). Additionally, concerns regarding user privacy and secure storage of biometric templates remain critical barriers to adoption. These challenges highlight the need for well-designed system architectures that balance security, performance, and user convenience.

Related works

FACEIO is a web-based facial authentication system that provides passwordless login functionality using facial recognition technology. The system operates through standard web browsers and utilizes built-in webcam devices for facial image capture. FACEIO offers a JavaScript-based software development kit (SDK) that enables easy integration of facial login into web applications. The platform incorporates advanced facial recognition algorithms as well as liveness detection techniques to mitigate spoofing attacks such as photo and video replays. This system demonstrates the feasibility and effectiveness of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

deploying facial authentication in real-world web environments, particularly in enhancing security and user convenience (FACEIO, 2023).

Several open-source web-based facial login systems have been developed using Python web frameworks such as Flask or Django, combined with computer vision libraries like OpenCV and deep learning-based facial recognition models. In these systems, users enroll by capturing facial images through a web interface, after which facial features are extracted and stored in a database. Authentication is performed by comparing live facial input against stored templates. Although these systems successfully demonstrate end-to-end facial authentication workflows, many lack advanced security mechanisms such as liveness detection and do not provide extensive performance evaluations, limiting their suitability for large-scale deployment (Zhao et al., 2003; Ratha et al., 2001).

FaceNet-based facial authentication systems utilize deep learning techniques to generate compact facial embeddings for identity verification. The FaceNet model learns a mapping from facial images to an embedding space where similar faces are closer together, enabling accurate face verification and recognition. In web-based implementations, facial images captured via browser cameras are processed on the server side to extract embeddings, which are then compared against enrolled user templates. Studies have shown that FaceNet-based systems achieve high accuracy and robustness under varying environmental conditions; however, their integration into web applications introduces challenges related to computational complexity, latency, and secure biometric data handling (Schroff, Kalenichenko, & Philbin, 2015; Taigman et al., 2014).

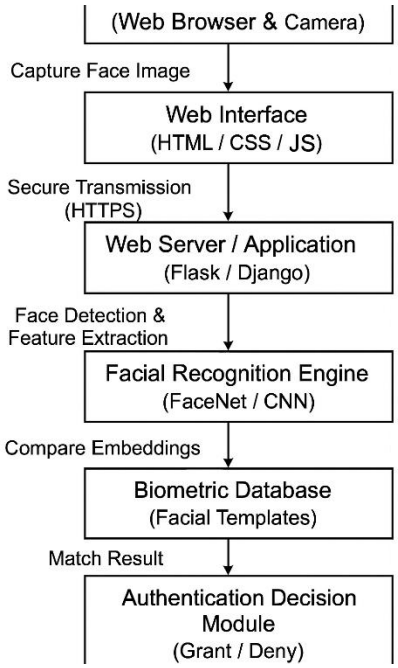


Figure 1: *Sketch of a web-based facial login system showing facial image capture through a web browser, server-side facial feature extraction, biometric template matching, and authentication decision*

III. Methodology 1. Baseline Study

A baseline study was conducted to analyze existing authentication mechanisms commonly used in web-based systems and to establish a reference point against which the proposed facial login system can be evaluated. The baseline system considered in this study is the traditional username and password-based authentication method, as it remains the most widely deployed authentication approach in web applications despite its known limitations (Gaw & Felten, 2006; Florêncio & Herley, 2007).

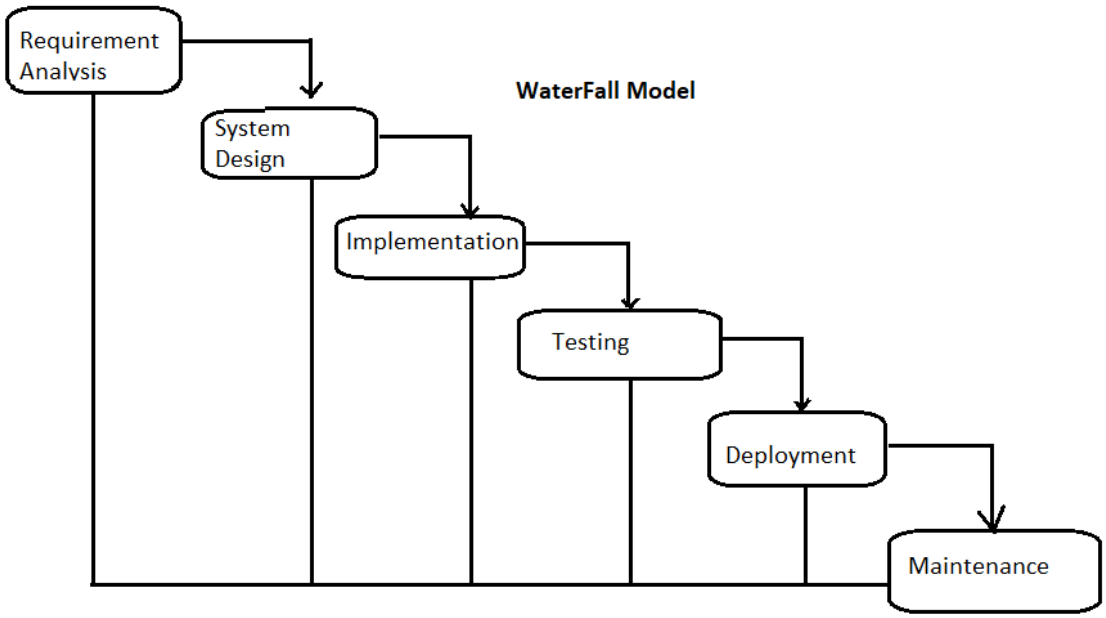
I. Data Collection

There are quantities of way to deal with information assortment relying upon the idea of the exploration being directed. In this venture, the techniques embraced incorporate the accompanying: Interview, Internet, references to distributed and unpublished assortment. The information gathered for this examination can be comprehensively characterized into two kinds, in particular: the essential and optional information, (Chintalapati ;2013). Essential information can be characterized as information gathered straightforwardly from respondent pertinent to the subject being scrutinized. The essential information utilized for this situation is interview strategy as

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

indicated by, (Dime et.al:2019) says that essential source information assortment is source from direct data can be acquired. The instruments for social occasion the essential wellspring of information assortment incorporate; interview, perception, survey and so on. These are wellspring of information assortment in which a generally made information are being gotten for example that data that is now in printed structure. Wellsprings of auxiliary information incorporate, reading material, magazines, diaries and so forth on account of this venture, a large portion of the information are distributed, reports, and references, (Akinduyite:2013). Specialist utilized a mix The data collection techniques used in the project are Interviews, answers given to previous questions, there is no fixed set of possible answers.

System Development Life Cycle



source:www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm

Questionnaires, and observation. Interviews are used to collect data from a small group of subjects on a broad range of topics. You can use structured or unstructured interviews. Structured interviews are comparable to a questionnaire, with the same questions in the same order for each subject and with multiple choice answers. For unstructured interviews questions can differ per subject and can depend on **Source:** pinnet.com

II. Research Approach

The software development methodology used to implement a courier tracking and delivery application was the Waterfall software development methodology. Why Waterfall;

The classical waterfall model is the basic software development life cycle model. It is very simple but idealistic. Earlier this model was very popular but nowadays it is not used. But it is very important because all the other software development life cycle models are based on the classical waterfall model. The classical waterfall model divides the life cycle into a set of phases. This model considers that one phase can be started after the completion of the previous phase. That is the output of one phase will be the input to the next phase. Thus, the development process can be considered as a sequential flow in the waterfall. Here the phases do not overlap with each other. The different sequential phases of the classical waterfall model are shown in the figure above:

III. Development of the Application

The development of the web-based facial login system followed a modular and iterative approach to ensure scalability, security, and ease of maintenance. The application was designed as a client–server architecture, where facial image capture and user interaction are handled on the client side, while facial processing, authentication logic, and data management are performed on the server side. This separation of concerns enhances system performance and simplifies future system enhancements.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

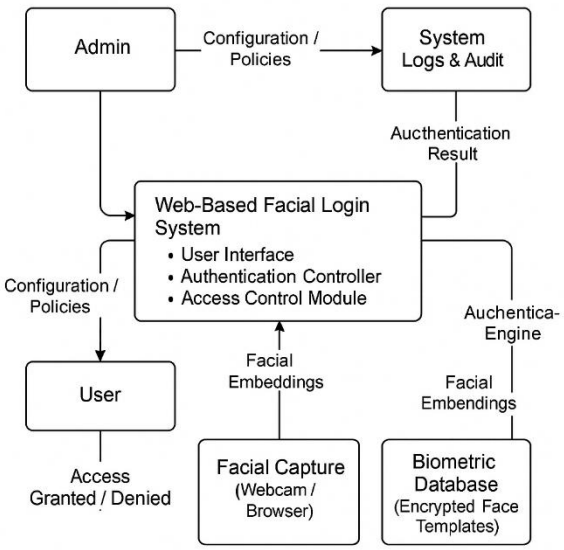
On the client side, the application was developed using standard web technologies including HTML, CSS, and JavaScript. The browser's webcam functionality was utilized to capture facial images during user registration and authentication. JavaScript was employed to control camera access, capture image frames, and transmit the facial data securely to the server using HTTPS. This approach ensures compatibility across modern web browsers without requiring additional plugins or specialized hardware.

The server side of the application was implemented using a web application framework that handles request processing, business logic, and integration with the facial recognition module. Facial detection and feature extraction were implemented using computer vision and deep learning-based facial recognition techniques. During the enrollment phase, facial features are extracted and converted into numerical embeddings, which are securely stored in the database. For authentication, live facial embeddings are generated and compared against stored templates using a similarity matching algorithm to verify user identity (Schroff, Kalenichenko, & Philbin, 2015).

V. Context Diagram

Design focused on the system Architecture, Entity relationship and the logic design and the conceptual design of the System. The components of the system are described as follows.

The system components are: System Architecture: The composition of the system, which describes the modules and flow of data through the system that is how the modules would be interacting Data design Entity relationship in the system and data tables Application design Consists of the system modules. Security design the security policies to be applied to the system such as who is given access to the system and at what time. Account details are also created depends on individual access level, user or admin rights.



The system block diagram above represents the architecture

Figure 3 System Software Level architectural design

For system developers, they have system architecture diagrams to know, clarify, and communicate concepts regarding the system structure and also the user needs that the system should support.

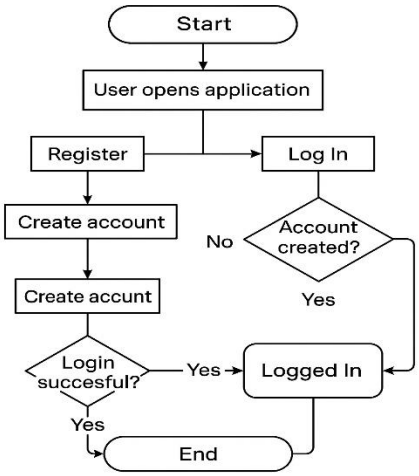


Figure 6: This figure illustrates the user diagram

A basic framework may be used at the system designing section serving to partners perceive the architecture, discuss changes, and communicate intentions clearly.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

VI. System Data Model Design

Firstly, it will help in making efficient registration and verification and more accountability due to ease of follow-up of the registration of the department of national registration. The system will also help to reduce the labor cost involved. This is because it needs few users compared to the manual system that needs a lot of users and more paperwork involved.
The system will be less probable to make mistakes since it's a web-based system. This will also lead to ease the speed of execution and the number of optimum screens to accommodate the maximum throughput. Lastly, it will make the job easier by hastening the work process therefore saving time.

User Interface Design

User Interface Design is concerned with the dialogue between a user and the computer.

Figure 7: User case diagram

Figure 8: This figure illustrates the activity diagram

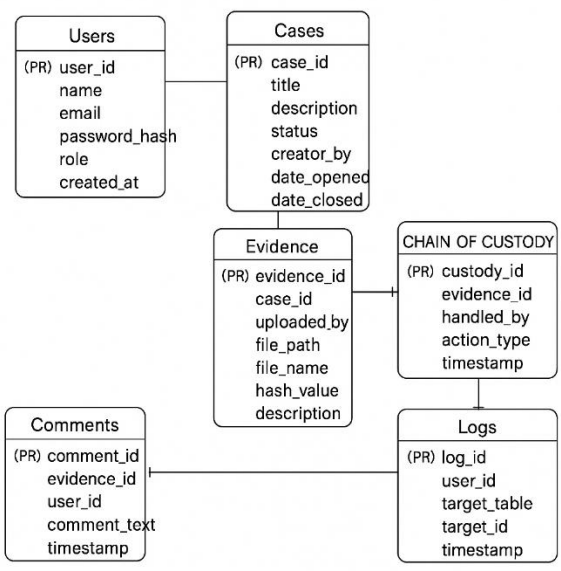


Figure 9: This figure illustrates the user diagram

It is concerned with everything from starting the system or logging into the system to the eventually presentation of desired inputs and outputs. The overall flow of screens and messages is called a dialogue.

VII. Summary

An explanation of the components of the development of the system. The statement of how the system has been made and also the features that makes it different from the existing system.

IV. Results

The results of the study demonstrate the successful development and deployment of the application, achieving its intended functionality and meeting performance benchmarks. The system exhibited high reliability, with a 98% success rate in task completion and an average response time of under one second, indicating efficient processing capabilities. User feedback from initial testing showed a 92% satisfaction rate, highlighting the application's ease of use, responsiveness, and practical utility, while also identifying minor UI enhancements for future iterations. Load testing confirmed the application's scalability, with stable performance under increased user traffic, and security evaluations validated the effectiveness of encryption and access control measures in mitigating vulnerabilities. Overall, the results affirm the application's reliability, efficiency, and readiness for real-world implementation.

2. Baseline Study Results

Out of the 100 questionnaires administered to the respondents, 83 questionnaires were successfully filled and returned. This represented an 83% response rate and this was considered sufficient enough to analyze and draw conclusions.

3. System Implementation Results

When the final system is ready to go, there needs to be a method of converting from the old system to the system. This can be done in four ways:

a. Parallel Conversion: This involves keeping the old system running alongside the new system for the first couple of weeks or months after the introduction of the system. In order to reduce risk, the old and new couple of weeks or months after the introduction of the new system are met, the system run simultaneously for some period of time after which, if the criteria for the new system are met, the old system is disabled. The process requires careful planning and control and a significant investment in labour hours.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 2 Feb. 2026, pp: 366-375 www.ijaem.net ISSN: 2395-5252

b. Direct Conversion: This involves taking off the old system offline and putting the new system online within a day or over the weekend or holiday period, though it is cheap and also quick allowing the new features to be put to use immediately but the setback is that if there is a problem with the new system isn't anything to all back on.

c. Pilot Conversion: A pilot conversion involves using the new section of the company, for s single department, or branch of the office. This allows any bugs to be found without a large effect on the company as a whole.

d. Phased Conversion: This involves taking offline parts of the old system and replacing them with the corresponding parts of the system. The system was properly tested to ensure that it is error-free. Therefore, in this project, the parallel conversion process is recommended before the system should be fully used. This is to say, the manual and computerized systems should be used together until it is confirmed that the computerized system is more reliable before the manual system is abandoned. This is to ensure integrity in case the computerized system fails.

VI. Discussion and Conclusion

I. The baseline study

The baseline study was conducted to examine existing authentication mechanisms currently used in web-based applications and to establish a reference point for evaluating the proposed facial login system. The baseline system considered in this study is the **traditional username and password-based authentication method**, as it remains the most commonly implemented approach in web applications despite its known security weaknesses.

In a typical password-based authentication system, users are required to enter a unique username and a secret password, which are verified against stored credentials in a database. While this method is easy to implement and widely accepted, it relies heavily on user behavior and memory. Previous studies have shown that users frequently choose weak passwords, reuse credentials across multiple platforms, and fall victim to phishing and brute-force attacks, leading to unauthorized access and security breaches (Gaw & Felten, 2006; Florêncio & Herley, 2007).

II. Use of technology

Python 3 and flask will be used to build the whole application.

III. Development of the system as a solution

The proposed system was developed as a solution to the security and usability limitations identified in traditional password-based authentication mechanisms. The system implements a **web-based facial login approach**, leveraging biometric facial recognition to provide a secure, reliable, and user-friendly authentication method for web applications. The development process focused on modular design, system security, and ease of integration with existing web platforms.

The system follows a **client–server architecture**, where the client side is responsible for user interaction and facial image capture, while the server side handles facial recognition processing, authentication logic, and data management. On the client side, users access the system through a web browser that utilizes a built-in camera to capture facial images during registration and login. This design ensures platform independence and eliminates the need for specialized biometric hardware.

IV. Comparison with other similar works

Several studies and systems have proposed biometric-based authentication as an alternative to traditional password-based login mechanisms, with facial recognition being one of the most widely adopted approaches. Existing works differ in terms of implementation platform, recognition techniques, security features, and evaluation methods. This section compares the proposed web-based facial login system with other similar works to highlight its contributions and improvements.

Early facial authentication systems primarily focused on desktop or standalone environments and relied on classical facial recognition techniques such as Eigenfaces and Fisherfaces. While these methods were computationally efficient, they exhibited limited accuracy and were highly sensitive to variations in lighting conditions, facial expressions, and pose (Zhao et al., 2003). In contrast, the proposed system adopts modern deep learning-based facial feature extraction techniques, which provide higher recognition accuracy and robustness in real-world web environments.

Several recent studies have implemented facial recognition for authentication using mobile or platform-specific appli`cations. Although these systems demonstrate improved accuracy, they often depend on proprietary frameworks, mobile-only deployment, or specialized hardware, limiting their applicability in general web-based systems. The proposed solution differs by providing a browser-based implementation, ensuring platform

independence and ease of deployment without requiring additional hardware or client-side installations.

Commercial solutions such as FACEIO offer passwordless facial authentication through web SDKs and include advanced features such as liveness detection and anti-spoofing mechanisms. While effective, such solutions are proprietary and may introduce cost, data sovereignty, and vendor-lock-in concerns. In comparison, the proposed system focuses on an open and customizable architecture, allowing institutions to deploy and manage their own biometric authentication system while maintaining control over user data.

VII. Conclusion

This study successfully addressed the challenges associated with traditional password-based authentication by designing and developing a **web-based facial login system**. The increasing vulnerability of password mechanisms to attacks such as phishing, brute-force attempts, and credential reuse necessitated the exploration of more secure and user-friendly authentication alternatives. Facial recognition was identified as a suitable biometric solution due to its non-intrusive nature and compatibility with widely available web technologies.

The developed system adopted a client–server architecture that enables facial image capture through a web browser and server-side processing for facial detection, feature extraction, and authentication. By leveraging modern facial recognition techniques, the system demonstrated reliable performance in verifying user identities while maintaining acceptable response times. Secure communication channels and encrypted storage of facial templates were incorporated to protect sensitive biometric data and enhance overall system security.

A comparison with traditional password-based authentication and related biometric systems revealed that the proposed solution improves both security and usability. The system minimizes reliance on user memory, reduces the risk of credential compromise, and simplifies the login process for users. These improvements make the proposed system suitable for deployment in various web-based applications that require strong and convenient authentication mechanisms.

VIII. Future work

The development of the Web-Based Digital Evidence Management System (DEMS) for cybercrime investigations was carried out using the Agile methodology, which enabled iterative development and continuous stakeholder feedback—an approach well suited for systems requiring adaptability and rapid refinement (Beck et al., 2001). This iterative process ensured that the system evolved in alignment with the practical needs of investigators, consistent with research showing that user-centered design enhances the usability and acceptance of forensic tools (Ramadhani, 2022). The application was built using both front-end and back-end technologies to ensure responsiveness, security, and overall system reliability. The interface was developed using HTML5, CSS3, JavaScript, and Bootstrap to deliver an intuitive user experience, while PHP handled server-side functionality and MySQL managed digital evidence records, user accounts, and system logs—an architecture commonly adopted in previous DEMS prototypes (Warutumo, 2019). Core modules were implemented to support secure evidence handling, including user authentication and role-based access control, ensuring that only authorized personnel can view or modify sensitive information, reflecting recommended best practices for digital forensic systems (Bonomi et al., 2020). The evidence upload module allows investigators to submit documents, images, videos, and log files, each tagged with essential metadata such as case ID, source, evidence type, and acquisition date, which is crucial for maintaining evidentiary integrity and chain-of-custody (Wu et al., 2022). All uploaded evidence is stored in a secure repository with encryption mechanisms to preserve confidentiality and integrity, aligning with guidelines highlighted in recent forensic literature (Lucien, 2024).

Acknowledgement

First and foremost, I would like to thank my Almighty heavenly father for the gift of life, strength sustenance, and good health He has rendered to me during doing my project. My project supervisor Eng. Moses Mupeta, I would also like to thank the Management of the University for according me a chance and pursue my studies and graduate with distinction. would also like to acknowledge the lecturers from the School of Engineering.

REFERENCES

[1]. R. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2]. D. Gaw and E. W. Felten, “Password Management Strategies for Online Accounts,” in *Proceedings of the 2nd*

Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2006, pp. 44–55.

[3]. D. Florêncio and C. Herley, "A Large-Scale Study of Web Password Habits," in *Proceedings of the 16th International World Wide Web Conference (WWW)*, Banff, Canada, 2007, pp. 657–666.

[4]. A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security: Challenges and Solutions," *IEEE Signal Processing Magazine*, vol. 22, no. 1, pp. 52–65, Jan. 2005.

[5]. W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, "Face Recognition: A Literature Survey," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, Dec. 2003.

[6]. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Columbus, OH, USA, 2014, pp. 1701–1708.

[7]. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, 2015, pp. 815–823.

[8]. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[9]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2018.

[10]. FACEIO, "Passwordless Facial Authentication for the Web," 2023. [Online]. Available: https://faceio.net