BINDURA UNIVERSITY OF SCIENCE

EDUCATION

FACULTY OF SCIENCES AND ENGINEERING

COMPUTER SCIENCE DEPARTMENT

Topic: Reinforcing Data Security On Universities Web Based Systems By Use Of Three Tier Password Authentication System

done by

JOHANESE MSONZA B1749306

SUPERVISOR: MR. MUZURURA

A research project is submitted in partial fulfilment of the requirements of HBScComp in the department of computer science at Bindura University Of Science Education June 2022

APPROVAL FORM

The undersigned certify that they have supervised the student Johanese Msonza dissertation entitled , Enhancing Data Security Of Universities Web Based Systems By Use Of Three Tier Password Authentication System in Partial fulfillment of the requirements for the Bachelor of Computer Science Honours Degree of Bindura University Of Science Education.

……. ……... ……/……/……..

STUDENT SIGNATURE DATE

……... ……. ……/……/……

SUPERVISOR SIGNATURE DATE

……. …….. ……/……/……

CHAIRPERSON DATE SIGNATURE DATE

…….. …….. ……/……/……..

EXTERNAL EXAMINER SIGNATURE DATE

ABSTRACT

As technology advances, security has become a top priority in the technical world. In order to secure confidential information from intruders who tend to invade, rigorous security measures must be used. Text-based passwords have been widely established and utilized at universities and other institutions for decades. Text-based has become a target for hackers, exposing personal information (fee records, student outcomes, etc.) to the wrong hands. As a result of technological advancements, biometric security measures were adopted. It has been attempted to design barcode scanners, fingerprint scanners, and facial recognition in such a way that they safeguard information from intruders or being infiltrated. As a result of the escalating breaches of security over the computational numerous federals, as well as students and university institutions as a whole, have experienced significant losses and blows from invaders. This necessitates the use of additional security measures. Two-tier security phases have evolved, requiring a user to pass through two security steps before being supplied information.

DEDICATION

God Almighty, my creator, my strong pillar, my source of inspiration, wisdom, knowledge, and understanding, I dedicate this project to you. Throughout this program, He has been my source of strength. I also dedicate my dissertation to my family and many friends. I owe a special debt of appreciation to my devoted parents for their unwavering support throughout the process. I will always be grateful for what they have done for me.

ACKNOWLEDGEMENT

I want to express my gratitude to Mr. Muzurura my supervisor, for her unwavering support and advice. Throughout the research, he was a constant source of encouragement and was always eager to help in any way she could. Finally, a big thank you to everyone who took part in the study and made this research possible.

TABLE CONTENTS

Chapter 1: Problem Identification

1.0 Introduction

This is the beginning of my research that will pave the way for showing a system that supports three-tier authentication for online applications used by universities and other institutions. The application focuses on providing high-quality and secure university web applications against intruders who may try to tamper with data from various organizations online. For someone to be authenticated into this system, they must go through three security steps. The system's main goal is to build a solid security architecture that allows institutions to have improved security experiences. The basic security phase of the three-tier security phase requires the user to enter a password and username. As a result, once you've provided the needed information,

1.1 Background Study

As technology advances, security has become a top priority in the technical world. Best measures of security must be implemented so as to ensure protection of information which is confidential from hackers or intruders who might want get into university web-based systems, for example (ZIMTECH, 2018) Hackers broke into Midlands State University's security system, forcing the university to postpone its Student Representative Council elections. During the last few decades, text-based passwords have been widely adopted and used. Text-based has become a target for hackers, exposing personal information to the wrong hands, as in the instance of a student at Chinhoyi University (ZimLive, 2020) who hacked the account of results to improve them. As a result, as technology advances, biometric security becomes more secure.

As a result of technological advancements, biometric security measures were adopted. It has been attempted to design barcode scanners, fingerprint scanners, and facial recognition in such a way that they safeguard information from intruders or being infiltrated. As a result of the escalating security breaches over the computational, numerous federals, institutions, and pupils have experienced significant losses and blows from invaders. This necessitates a higher level of protection on their computer platforms. Two-tier security phases have evolved, requiring a user to pass through two security steps before being supplied information.

In today's digitally driven economy, information technology is the foundation for business growth and sustainability. The volume of data being shared as well as frequency by which institutions or companies are sharing information over online networks are both skyrocketing. Many of pieces of equipments are linked together, involving smartphones, without forgeting Automated teller machines, tablet(s,) closed circuit television cameras and many more, resulting in exponentially growing interdependencies.

This increase in knowledge, accessibility, and connectivity comes at the cost of a loss of direct data security control. (ZimEye, 2022) A student from Chinhoyi University of Technology (CUT) who entered into university database of their results for the Examination and put some fake result for himself including other 7 students who had not passed examinations of the semester of the previous year.

The students who had not passed other courses like as financial management, computer organizations, architecture, the operating systems payrd that student with different US dollar amounts.

1.2 Statement of the Problem

Several universities have experienced serious data and information breaches on their risk web application platforms, for example (ZimEye, 2022). Text-based passwords are the most frequent sort of security password used on university web systems, and they have since been changed for example (ZIMTECH, 2018). Because of the rise in cyber-crime, security issues related to logins and access have become a major concern. Furthermore, protecting yourself from cyber threats requires more than a single safe authentication mechanism.

As a result, an Authentication System that has Three sphases of security can be designed for increasing data security by ensuring that only those who are authorized have access to the system. The computer has three staged logins, each with three different password management schemes. The password difficulty increases with each stage, securing access. In certain ways, our PHP-based Three Level Authentication System will assist customers in protecting their data from hackers and cyber dangers. (No date provided by NevonProjects).

1.2 Aim of Research

The main goal is to develop a three-tier login authentication system for universities and other interested organizations to improve the security of various web services.

1.4 Research Objectives

- To design a three-tier login authentication which has biometric facial login authentication and the text based password to improve security and privacy of data on web application system of universities.
- To asses the usefulness of diferent system development tools in developing an authentication system
- Evaluate the effectiveness and efficiency of three-tier login authentication towards the main aim.

1.5 Research Questions

1. How is the researcher is going to design and implement a 3-tier login authentication to reignforce security and the privacy of universities data on their web system or applications?
2. How is the author going Evaluate the effectiveness and efficiency of three-tier login authentication?
3. How is the researcher is going to implement biometric facial login authentication and a cryptography based password?

1.6 Research Propositions/ Hypothesis

- H_0: The system will be able to perform a three-tier login authentication.
- H_1: The system will fail to perform a three-tier login authentication.

1.7 Justification of Research

Three-tier login authentication is a security architecture that consists of three phases. This will be important in providing a high level of security for web apps on the network. Each step

sees an increase in security reinforcement. Because it will prevent various intruders from breaching the security of secret information via the network, the suggested system will function as a hybrid architecture. Single-phase architectural login authentication has already been subjected to a number of Basic text-based login authentication systems were easily remembered and breached, necessitating the use of a variety of technologies to begin the journey resulting in data loss to the wrong people, rules of authentication The three-tier authentication architecture will involve in it basic text-based password authentication, graphic password of authentication, and biometric type of login authentication. These will give the network a high level of security.

1.8 Limitations

- There is need for more time to train data.

1.10 Conclusion

Research goals are discussed in this chapter. What the researcher hopes to achieve at the conclusion of the study. The researcher's goal is to make university web-based systems more secure. The author will now identify general objectives to be fulfilled during the research, along with general plan of work including the tools and methodologies. Shortcomings of current systems, as well as the reasons and ambitions of the future system, are discussed. The chapter below will handle the review of literature and present some of the work done previously on this system.

CHAPTER-2: LITERATURE REVIEW

2.0 INTRODUCTION

Systematic gathering, organizing, and the analyzing of articles that contains the information of the subject of study under consideration constitutes a literature review. Its purpose is for providing in-depth understandings about issue under investigation. This assists researcher in discovery of what other good researchers have managed to do in regard to the research topic. This helps much more in assisting the researcher to minimize unnecessary, disproportionate duplication, as well offering a framework to analyze the results (Mugenda and Mugenda, 2013).

The chapter will be looking at reviews of literature relating to researcher's system's application. The reviewed literature covers the following topics: functionality, execution benefits, the crucial steps for successful implementations, implementations challenges, successes and success opportunities, cryptographic implementation objectives and login systems of authentication, best practices, and standards of 3-tier and 2-tier .

Analysis of study

Previous System Security

Former system security used by most institutions for applications like the results portal. The results portal system is a web application that is used to keep track of and save data for students' outcomes. It keeps track of student records and results. As a result, the only sort of security system established on those universities' systems was the basic login, which required the administrator to simply enter a password and an email address or other information. As a result, extra security reinforcements on the application were required in the future.Hackers, including

students, have breached it multiple times. (ZimEye, 2022) One of student at Chinhoyi University of Technology (CUT) hacked the account of university's Examinations database of results and faked those results for himself and those of seven other students who failed semester examinations of the previous year.

Three Tier Login Authentication For Universities Web based Systems

Three-tier login authentication is a security architecture that consists of three phases. This will be important in providing a high level of security for web apps on the network. Each step sees an increase in security reinforcement. Because it will prevent various intruders from breaching the security of secret information via the network, the suggested system will function as a hybrid architecture. Single-phase architectural login authentication has already been subjected to a number of assaults, resulting in data loss to hands of wrong people. Text-based basi login authentication system were readily remembered and breached, necessitating the use of a variety of technologies to begin the authentication process. The three-tier hybrid authentication architecture will incorporate basic text-based password authentication, graphic password authentication, and biometric login authentication. These shall give the network a high level of security.

2.2 PREVIOUS RELATED STUDIES AND SYSTEMS

Real-Time Medical Systems Based on Human Biometric Steganography: a Systematic Review

The authentication layer has the potential to learn from approved user activity, resulting in a cute and easy-to-use feature while also protecting sensitive data from questionable users.

Nalini et al. (2013), on the other hand, argue that public cloud computing likely to be harmed by security slew of vulnerabilities. In a similar vein, Gartner identifies the top seven security concerns that clients should discuss with vendors before using public cloud computing, including:

1) The access to the privileged users,

2)adherence to the regulations

3) data storages

4) The data separation

5) Recovery of data

6) The support of investigations

7) Long-term viability

In addition , Carrol et al. 2018 discusses some of the key problems that deals with public cloud computing challenges of security.

The most challenging issue with this framework is that the usage of numerous criteria such as face recognition, ID or password, IMEI, IMSI, voice, and facial recognition makes authentication process to be more complex, complicated, and it affects system accuracy.

USER AUTHENTICATION IN PUBLIC CLOUD COMPUTING THROUGH ADOPTION OF ELECTRONIC PERSONAL SYNTHESIS BEHAVIOR

Usually PIN-Password based authentication solutions relies mostly on what users already know to verify a user's identity Manandhar (2019). Hence these authentication procedures have a major drawback since passwords maybe forgotten, lost or even stolen .At some point they can easily be spoofed. ATM cards and key cards are vulnerable to intruders since they validate users based mostly on "what a person owns." The systems assess a user's physiological or behavioral features to create a digital print that uniquely identifies that person (Shakir, 2020). Lack of training data limits the capabilities of biometric systems accompanied with extra hardware .

Without looking at their shortcomings or disadvantades, authentication based on password systems are still most widely used techniques authentication in the current context. However, because biometrics are unique to each person and do not need to be remembered, several modern techniques have resorted to biometric-based authentication systems.

One-Class Classification to Continuously Authenticate Users Based on Keystroke Timing Dynamics

The majority of current authentication solutions rely on static initial user verification; however, these mechanisms do not check user identities on previously unlocked devices. Spy Hunter, a

continuous authentication system, constantly monitors the keyboard timing dynamics of the user to determine the user's identity (2019).

Despite the fact that there are more methods for authenticating clients, password-based authentication remains the most common. Using password-based authentication, a client can securely access services such as emails hosted by a service provider.If the client's username and password pair match the username and password pair in the service provider's database, the client is permitted access to the requested service. The main benefit of password-based authentication is that passwords are simple to remember and use. Greetings, Manandhar (2019).

The Challenge-Response Authentication Mechanism is one of the most widely used password-based authentication mechanisms (CRAM). The customer asks access to a service in these systems.

A Password-based Authentication System based on The CAPTCHA AI Problem

Partly due to the domain's rapid pace of technological innovation, ever-changing legislative rules, and the importance of identity management to the functioning of society. Examples include the classification of authentication systems, as well as their usefulness and limitations, a survey of existing authentication methods, a framework for the suggestion of authentication schemes, and a review of authentication using behavioral biometrics. Identity management literature studies include surveys in the context of the Internet of Things, authentication for e-government services, privacy preservation and methods, and identity and access management in cloud environments. Elashry(2020). For example, the strategy outlined in the paper necessitates interfaces with more backend nodes and push message services (changes to legacy infrastructure -TRUE), implying a greater reliance on Certificate Authorities in addition to a trusted IDP (existence of a trusted third party institution -TRUE). "The private key SK never leaves the [IdM wallet app]," the authors continue, implying increased user accountability.

To improve the security of online services, authentication has been a primary form of protection. It was considered the first line of defense, with the responsibility of verifying and validating a user's identity before granting access to protected systems or allowing online transactions. Various authentication systems emerged, categorizing them as knowledge-based, token-based, or biometric-based. 2020 (Bazarhanova).

To ensure user authenticity, these methods rely on a variety of criteria, including anything the user knows for Knowledge-based schemes, user possession for Token-based schemes, and user

features for Biometric-based schemes. A combination of these methods is the most recent emerging advance in two-factor or multi-factor authentication, with password paired with PIN code and One Time Password (OTP) as the most commonly used authentication method. OTP enhances the security of login and password authentication.

Security and privacy of users' information are critical concerns in an online context where authentication is critical. It prevents unauthorized retrieval of confidential information by validating the identity of a person attempting to access a protected system. Some authentication procedures include knowledge-based, token-based, and biometric-based authentication. Smoldering (2020).

Enhanced Multi-factor Out-of-Band Authentication En Route to Securing SMS-based OTP

Authentication is a critical step in data security. The most commonly used type of authentication is username and password. Using the user's login and password to authenticate him. A personal identification number (PIN) is a number used to identify an individual. The problem with passwords is that users tend to choose short and popular combinations in order to avoid learning them. This issue could be solved and the risk mitigated by using one-time passwords that are only valid for one use. Reyes (2018).

Online Authentication Methods Used in Banks and Attacks Against These Methods

Biometrics as a concept was not widely used until Apple introduced fingerprint recognition technology as a component of its electronic products (Liu et al. 2015; Wu et al. 2018; Murakami et al. 2019). Biometrics could be integrated into application software or devices, allowing consumers to directly access these technologies (Liu et al. 2015; Barkadehi et al. 2018). This method adheres to the requirement for seamless and simple certification experiences (Murakami et al. 2019).

Actual biometric recognition should meet the accuracy, speed, and resource requirements of the authorized recognition function (Wu et al. 2018). The system must be both harmless and acceptable to the intended users, as well as resilient enough to withstand the majority of types of fraud and system attacks (Barkadehi et al. 2018). The four most common biometric authentication methods are face, fingerprint, voice, and iris recognition.

According to Bani-Hani (2019), growing threats and attacks on online banking security (e.g., phishing, identity theft) encourage most banks to seek out and use better authentication techniques rather than the traditional username and password authentication.

2.3 GAP ANALYSIS

For decades, government and educational organizations have experienced serious breaches of personal data and information. The information can be personal or business-related. The majority of popular kind Text-based passwords are used for security purposes. However, these types of authentication systems are easily tampered with, resulting in sensitive information falling into the wrong hands. Because of the rise in cybercrime, security threats associated with logins and accesses have become a major concern. Furthermore, relying on a single security authentication method alone will not keep you safe from cyber-attacks.

2.4 CONCLUSION

This chapter provided an overview of various studies on the topic of online documentation systems conducted by various authors. This chapter also included the researcher's introduction, theories, and benefits of using the system. After presenting the features of the proposed system, the author will discuss the methods for developing the suggested system in the following chapter.

Chapter 3 Methodology

3.0 Introduction

The goal of this chapter is to define the techniques and instruments that will be used to achieve the research and system objectives that have been proposed. Using the information obtained in the previous chapter, the author will develop the procedures required to construct a solution and will be able to choose among competing strategies to achieve the desired results of the research.

3.1 Research Design

Every stage of a project should include a reflexive approach for research design. The design step entails developing the system's many modules and their intended functions. The main goal of this stage is to create a system model that is operational, competent, long-lasting, and

dependable. The system was created using programming languages like python and php, as well as a laptop. To collect data on login authentication, facial recognition, and artificial intelligence, the author used documents and records.

The author decides to use the experimental research design as it allows him to observe changes and response of systems and objects as he changes or adjust factors. The author implemented three initial systems which he then used as control; he used the controls as bench marks for evaluation of improvement. The author created a facial, graphical and text-based login authentication systems.

3.1.1 Requirements Analysis

At this point, it is critical to document all of the required system's functional and non-functional specifications. It's a good idea to structure all incoming data, assess it, think about any potential consumer limits, and come up with a ready-to-follow specification that matches the client's needs. The study also considered any constraints, such as time and financial constraints, that could obstruct the design technique.

3.1.1.1 Functional Requirements

- System must be capable of using text-based authentication.
- The system ought to be able to use graphical authentication.
- . The system ought to be able to use facial verification authentication

3.1.1.2 Non-Functional Requirements

- The system ought to be able to perform a three-tier login authentication as quickly as possible
- The system should be simple to set up and operate. It should also be available at all times and capable of detecting fire at any moment.
- The system should have a quick response time and make decisions quickly.
- The system should be prepared to use all available facial recognition for decision-making.

3.1.1.3 Hardware Requirements

- Core i3 10^{th} generation
- 8 gig RAM
- 1 terabyte

3.1.1.4 Software Requirements

- Operating system of Windows 10
- pycharm
- xampp
- mysql

3.2 System Development

This system discusses the overall design of the system and how it was created to achieve the desired results. It lists all of the software tools and models that were used in the development of the system.

3.2.1 System Development tools

A methodology for software production or system design is a framework for organizing, planning, and regulating the procedures of building an information system in software engineering. Researchers have discovered many frameworks for various projects, and each framework has its own set of advantages and disadvantages depending on its application. These frameworks include the waterfall model, spiral model, and progressive (prototyping) model. Because the project is small and has a short deadline, the author chose the waterfall model for its ease of use. Because all of the project's needs have been determined and all of the tools have been put in place, the waterfall model is the best candidate for such a project.

3.2.2 Waterfall Model

It is a classic and rudimentary paradigm for constructing a system, with six steps to develop the system in this model. It begins with initial stage and runs downwards like a waterfall, implying that there is no going backwards or accepting feedback. It also describes a rigid and linear development process (Chandra, n.d). The system includes various objectives for each design step, and each stage must be achieved before the next stage can begin.

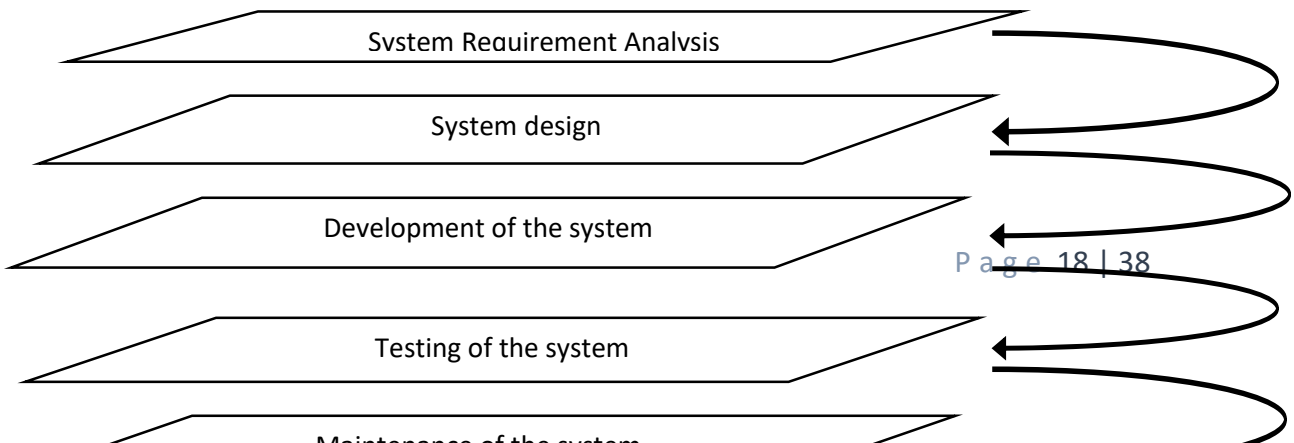


Figure 1 Waterfall Model

Aside from the methodology, the system was created with the following tools:

1. Python
   Is a high-level programming language for apps that the author used to construct the decision engine, which analyzes user data and makes decisions based on it.
2. php
   Is a high-level programming language, and the creator chose php, which is ideal for database connectivity.

3.3 Summary of how the system works

In the following routine, the system must support three-tier login authentication. Signing in requires the user to provide facial biometric images, a basic text password, and a graphical text password. As a result of these signup attributes, the user must log in using biometric facial authentication, graphical text authentication, and lastly basic text authentication.

When confidential information is needed to do the registration for the service or make an online buying, encryption is used. This ensures that one's platform privacy is protected. Encryption is used to protect data returned by the server to the client, such as a financial statement or test results.

When either a user or an administrator needs to know who is accessing or viewing the website, authentication is essential. Students and clients can use the BUSE website and Moodle to authenticate themselves. Whenever an applicant want to apply for a position. It is necessary to follow the registration and login procedures.

Authorization should be used when you want to limit viewer access to the specific pages. Students at Midlands State University, for example, are unable to access web pages dedicated to instructors and administrators. The authorization conditions for a website are frequently established in the.htaccess file.

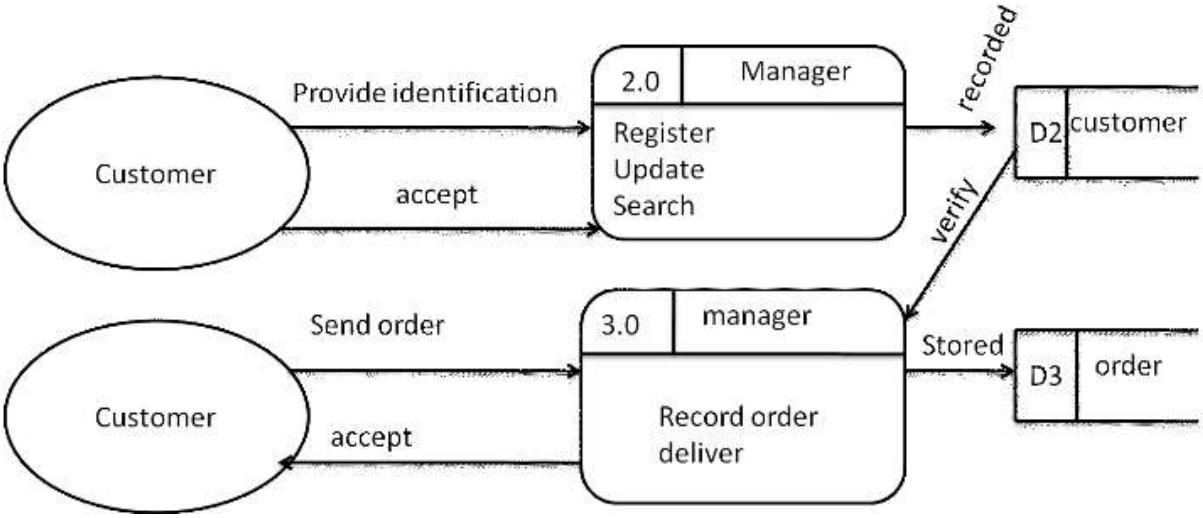
Authorization and authentication are frequently used interchangeably. Before utilizing the Student Link, BUSE students, for example, must first authenticate. The authentication they provide sets the parameters for what data they are allowed to see. Because of the authorisation stage, students cannot see data from other students.

3.4 System Design

This stage examines the requirements specification document to see how the system's components and data meet the requirements.

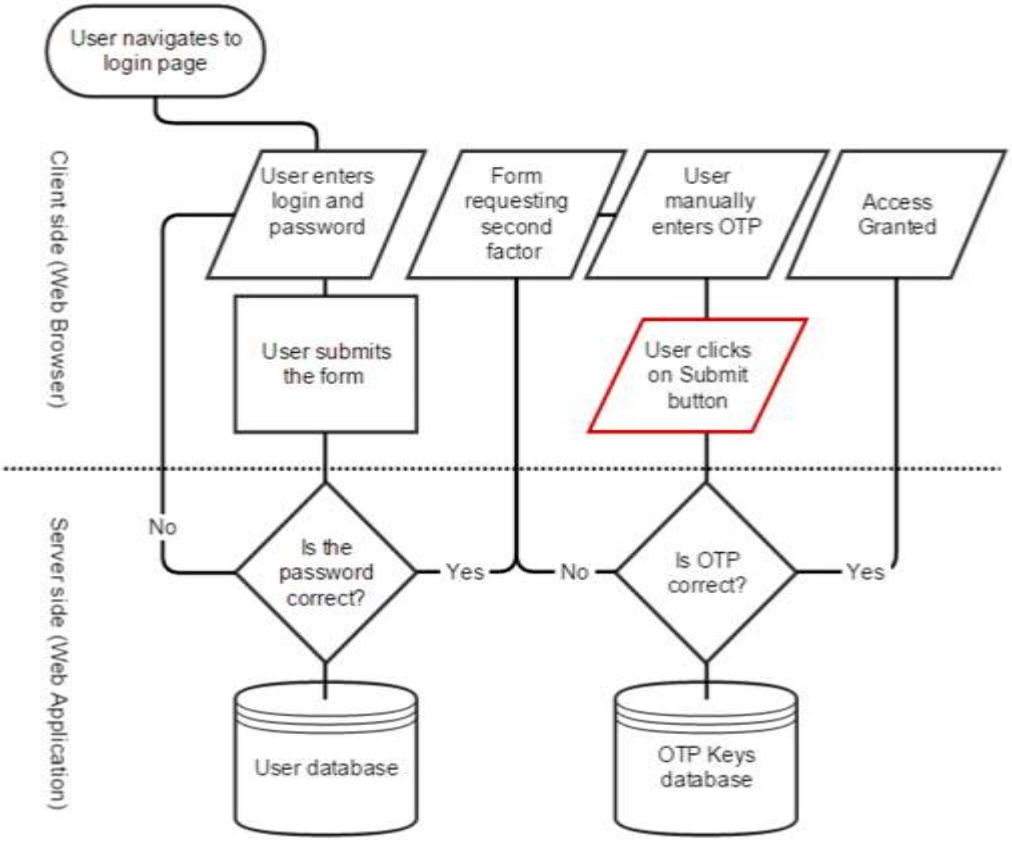
3.4.1 Dataflow Diagrams

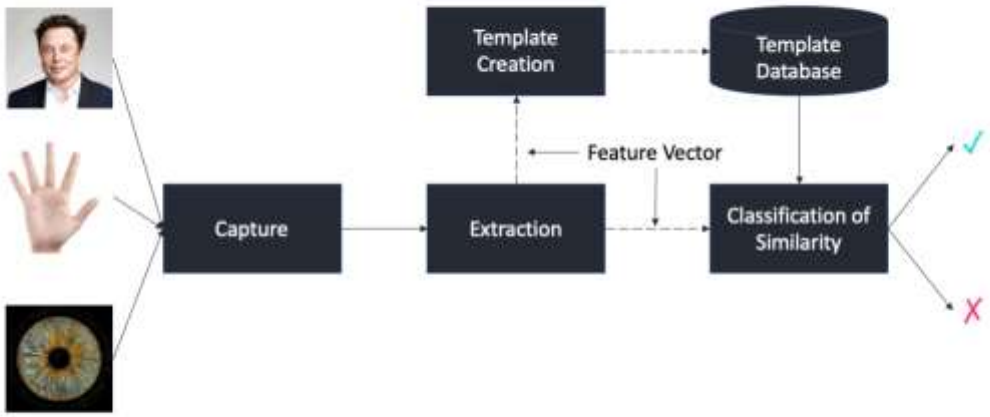
DFDs (data flow diagrams) depict the relationships between and among various system components. A dataflow diagram is a useful visual representation of high-level information in a system that explains how input data is transformed into output outcomes through a series of functional transformations. The name of the data flow indicates the type of data used in a DFD. DFDs are a type of information development that can assist you in comprehending how data is transformed as it moves through a system and how the result is displayed.

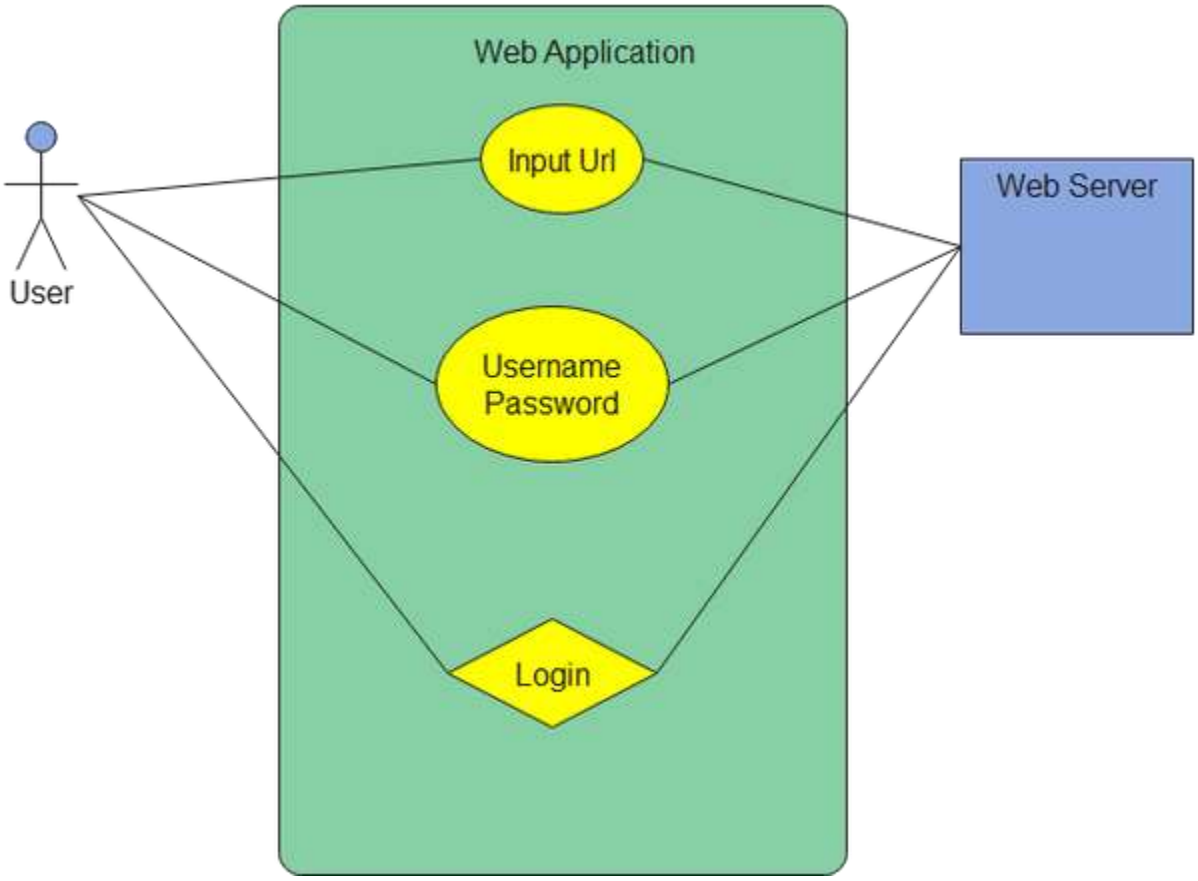


3.4.2 Proposed System flow chart

Flowcharts are an effective technique to bridge the gap between programmers and end users in terms of communication. They're flowcharts that specialize in condensing a large quantity of information into a small number of symbols and connectors.







3.5 Data collection methods

The author collected data through observation. The author ran multiple cycles, subjecting the system to various scenarios and observing how it responded. The observation allowed the researcher to assess the system's accuracy and the solution's response time.

3.6 Implementation

The system now is able to perform a three-tier login authentication.

Figure 6 Screenshots of the landing page of the system

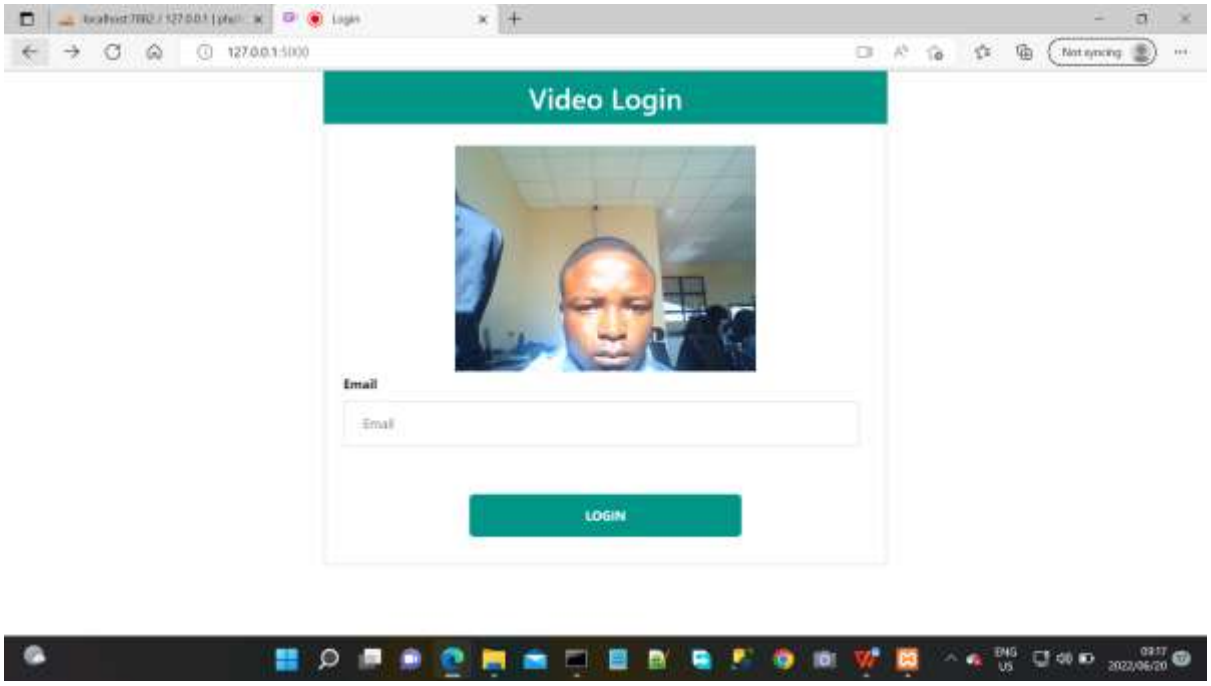
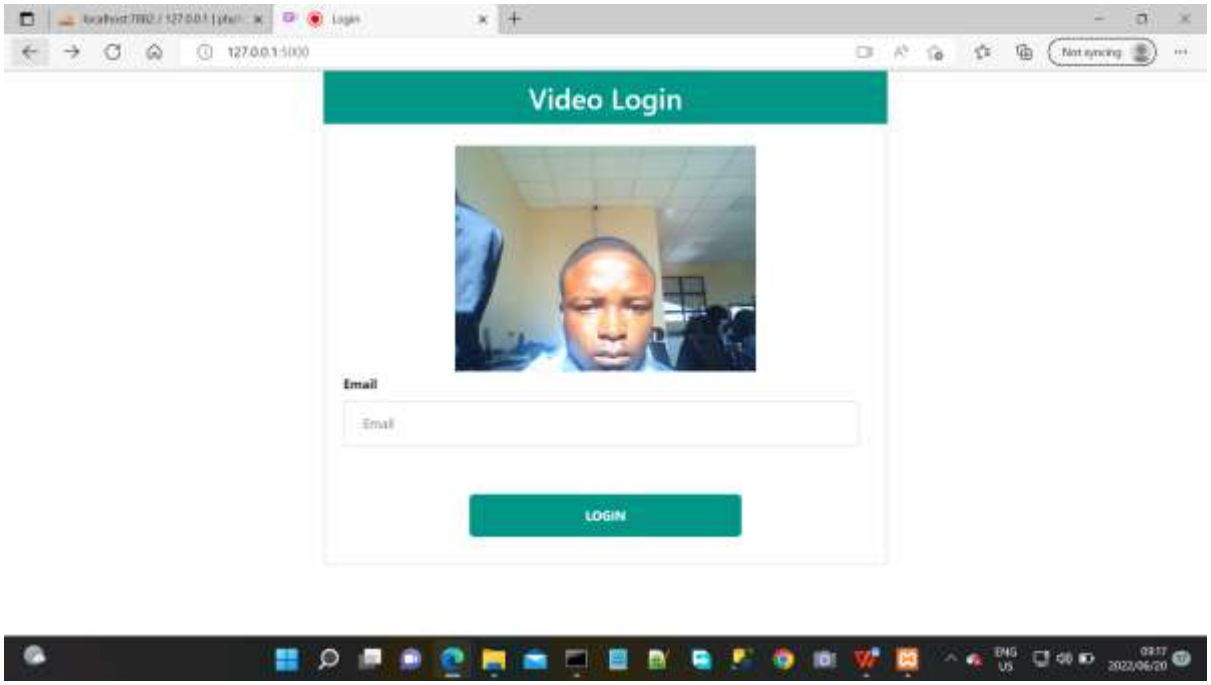
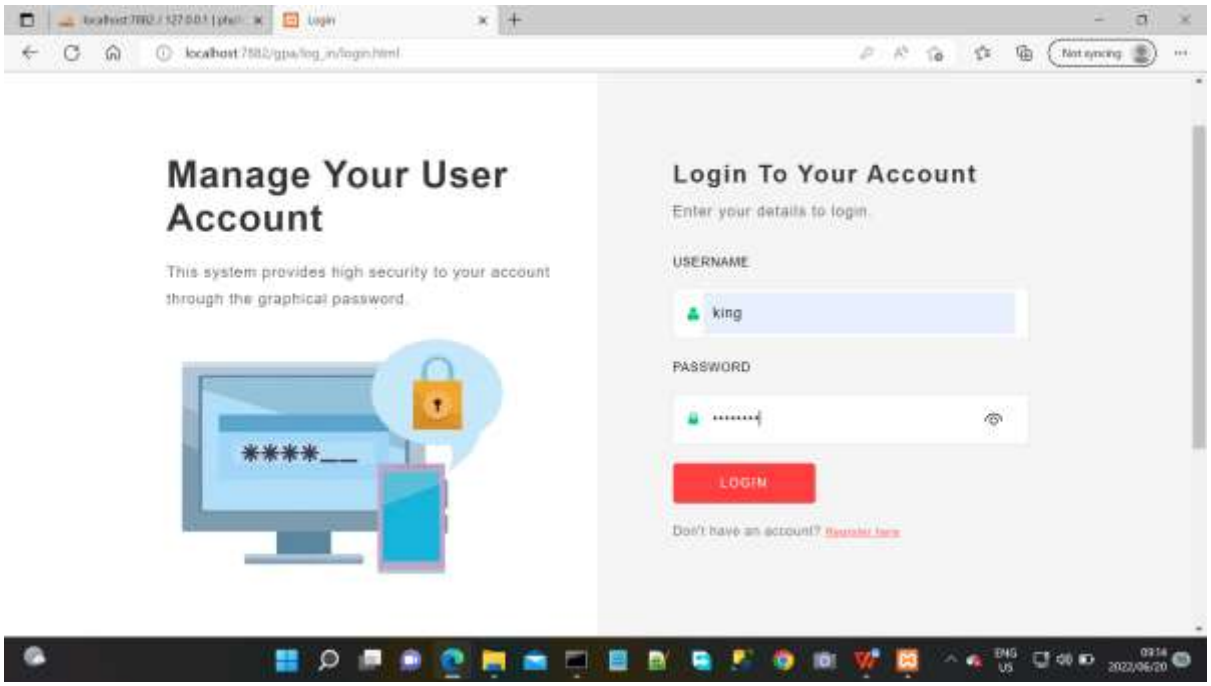


Figure 7 Screenshots of the system describing the process


Video Login
Email
Email
LOGIN


Manage Your User Account
This system provides high security to your account through the graphical password.
Login To Your Account
Enter your details to login.
USERNAME
king
PASSWORD
LOGIN
Don't have an account?

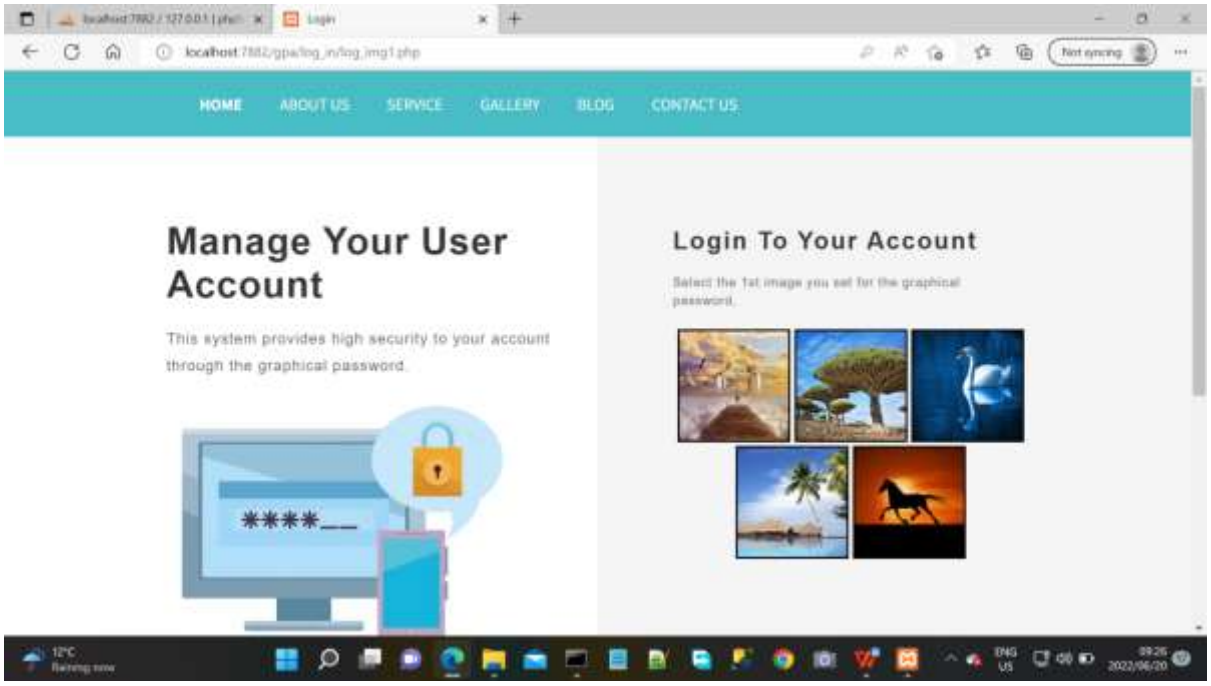


Figure 8 Screenshots of the system on graphical login authentication phase

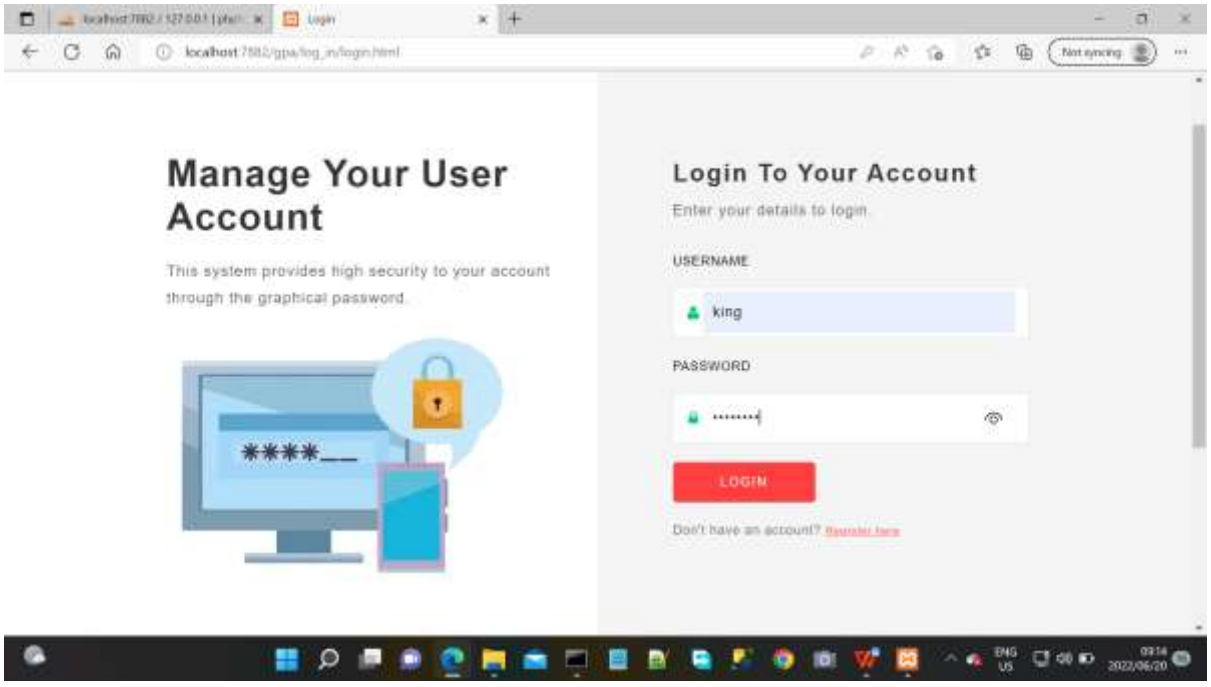
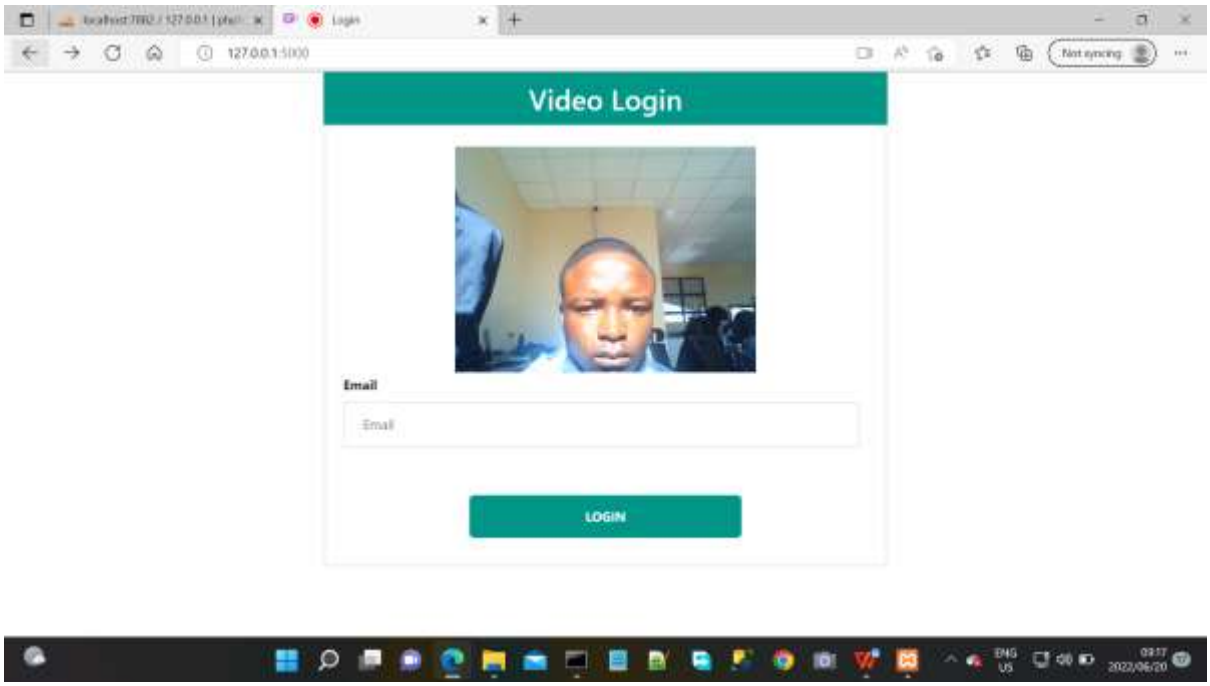


Figure 9 Screenshots of the system in detection mode



3.7 Summary

This chapter discusses each aspect of the project's design, including how each project outcome was created. It concentrated on the system design, which included PHP, Python, MySQL, and JavaScript, with each component detailed and how they work together to create this functional system. In order to meet the research's objectives, every component of the research that was specified in the scope of the study was covered. The results will be presented in.

Chapter 4 Results

4.0 Introduction

Following the completion of the system, the effectiveness of the provided solution must be evaluated. The accuracy, performance, and response time matrices were used to determine the efficiency and efficacy of the produced solution. The information gathered in the previous chapter was examined to come up with useful results. The behavior of the constructed system was also observed under various settings, and the results were reported in a tabular format. White box, black box, and unit testing are all important in determining how a system behaves under different conditions.

4.1 Testing

Testing is an important element of the development process, and this chapter details the tests carried out and the results obtained. The testing is compared to the proposed solution's functional and non-functional requirements.

4.1.1 Black box Testing

Black box testing allows someone who is unfamiliar with the system's underlying structure to test it against functional and, in some cases, nonfunctional requirements. The system was black box tested by the supervisor and a few students, and the results are shown below.

Figure 10 running the system with no password

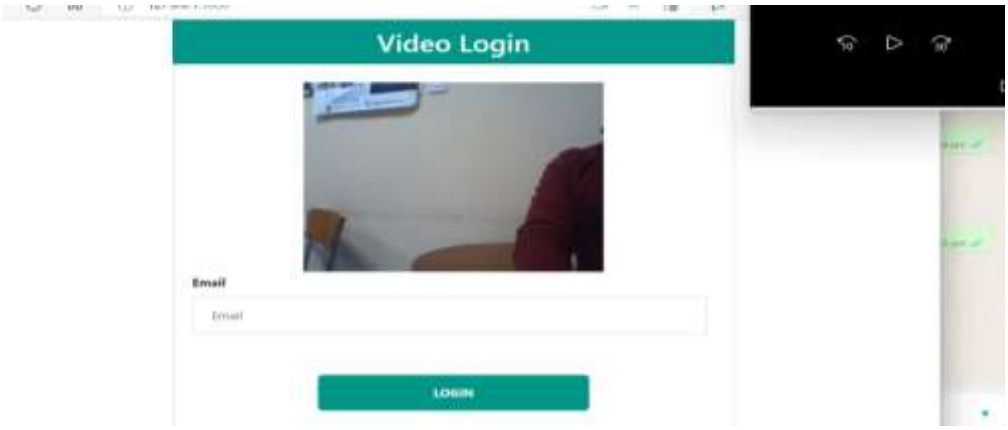
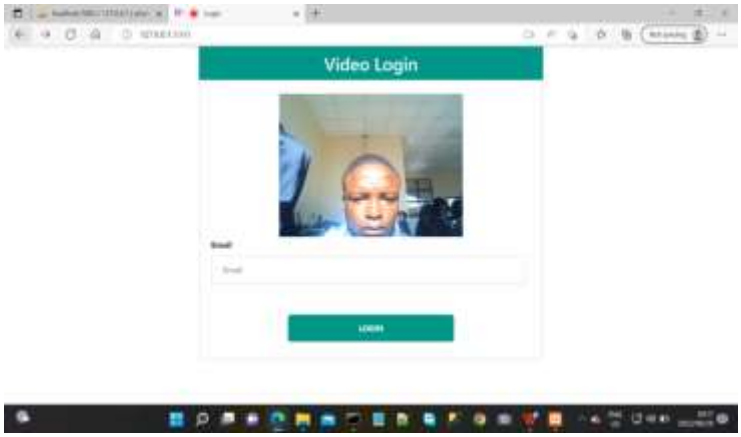


Figure 11 running the system with a face



4.1.2 White box Testing

White box testing allows developers and other stockholders to assess the internal structure of the system, such as error handling and other features. The author performed this test to see how the system handled situations such as running the system without the board and running the system without any prior detection knowledge (without training).

4.2 Evaluation Measures and results

Table 1 Confusion Matric

Type	Success Authentication	Failed Authentication
Success Authentication	True Positive	False Negative
Failed Authentication	False Positive	True Negative

For system observation, three scenes and a test environment were created. On each scene the system was observer on 40 occasions 20 correct details and 20 without correct details and the behavior of the system was observed. The three scenes were with wrong facial credential, wrong graphical text credentials and those with wrong text-based passwords. All of the analysis on the set was done to ensure that the answer was accurate and that there were no bogus credentials. The tables below indicate the outcomes of the tests that were conducted.

Table 2 Testing with Facial Credentials

Test cases	Correct Face	Number of tests	Correct readings	False Readings	Classification
1	Yes	20	18	2	True positive
2	No	20	16	4	True negative

Table 3 Graphical Text Credentials

Test cases	Correct Credentials	Number of tests	Correct readings	False Readings	Classification
1	Yes	20	20	0	True positive
2	No	20	20	0	True negative

Table 4 Testing with text-based passwords

Test cases	Correct Credentials	Number of tests	Correct readings	False Readings	Classification
1	Yes	20	20	0	True positive
2	No	20	20	0	True negative

4.2.1 Accuracy

Accuracy is equal to the number of correct predictions divided by the total number of forecasts in each category. After that, the percentage of correctness is calculated by multiplying it by 100. It is calculated using the following equation:

Equation 1: Accuracy calculation as adopted from Karl Pearson (1904)

Accuracy = (TP+TN)/ (TP+TN+FP+FN)*100

Accuracy on facial authentication= (18+16)/ (18+16+2+4)

=0.85

=0.85*100= 85%

Accuracy on the graphical authentication = (20+20)/(20+20+0+0) *100

= 100%

Accuracy on the text-based password = (20+20)/(20+20+0+0) *100

=1*100

=100%

Average Accuracy rate = Accuracy at (facial + graphical + text-based) /3

= (100+100+85)/3 *100 = 285/3 *100

=95 %

4.2.2 Response Time

Response time is the amount of time it takes for the system to detect and determine if there is a fire in the environment. It's a metric for determining a system's efficiency. When testing for system response time, the author used the average and peak response times to determine the overall performance of the system. The average reaction time is determined by taking a series of time readings to determine how long it takes the system to respond in order to complete the entire operation. The most valuable reading is taken at the peak time, which is also the worst-case response time. The author performed 20 readings and timed the system.

Table 5 System response times

Test	**Reading Time in Seconds**

1	3.0
2	0.6
3	2.0
4	0.4
5	0.7
6	0.9
7	2.0
8	0.5
9	0.4
10	1.0
11	0.8
12	0.9
13	1.3
14	1.9
15	1.0
16	2.3
17	1.0
18	0.6
19	0.5
20	0.5

All of the readings were rounded to one decimal place.

Average system response time = sum of all response time/ number of readings

= (0.5+0.6+0.5+0.4+0.7+0.9+1+0.5+0.4+0.6+0.8+0.9+1.3+1.9+2+2.3+1+1)/20

= 17.3/20 =0.865 = 0.8 second (1dp)

Figure 17 Summary of System Response Time against the Control Variables

The author arrived at the conclusion that the system has an average response time of 0.8 seconds and a 300 millisecond imposed delay. The author needed some time to observe the system, hence the wait was necessary. The system features a 50 millisecond enforced delay in real-time processing.

4.3 Conclusion

Since the solution had a high level of accuracy, the test results indicated that it was a good solution in 2 scenes it produced 100% rate accuracy which was a result of the analysis of the confusion matrix. However the solution had a ninety five (85%) percent accuracy on the facial authentication, this was due to the light intensity and insufficient training data and proper environment exposure. The high levels of accuracy of the system indicate a reduction security breaching into the system. The provided solution had a calculated average response time of 0.8 seconds, which is an appreciable response rate. Translating the rate of response, it implies that the provided solution can perform an operation on an average time of 0.8 seconds after it has been ignited. At this point the researcher saw seen it worthy to use Artificial Intelligence for environment learning/ automatic evaluation model generation and Bayes' rules in decision making thus using Artificial Intelligence, Bayesian rule and Sensor Fusion is a viable method for reducing breaching of system's security.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS OF RESEARCH

5.1 Introduction

In this chapter a conclusion of our research is presented. The chapter represents the summary of findings, conclusion drawn from the research and recommendations for further studies. In this chapter a conclusion of our research is presented. Also, suggestions for further research and our contribution to the subject are mentioned. The purpose of this study was to develop and implement a three tier authentication-based on biometric face recognition, text based and graphical based password.

5.2Aims & Objectives Realizations

- The first objective of this study was to design and implement a three tier authentication for universities web system and to asses the usefulness of diferent system development tools in developing an authentication system. The third objective was Evaluate the effectiveness and efficiency of three-tier login authentication towards the main aim.

The researcher developed a three tier authentication system. The gained results are significant and confirm the efficiency of the the waterfall model and experimental research design in developing this three tier authenticating process. In my chapter 4, the author presented results of the method in which the metrics were response time, accuracy and recall. The test results of the system performance indicated that the system had a high level of accuracy as it scored an accuracy of 100% in reading and authenticating all the users. The system also has a 100% accuracy in automatically recording all the users who register or logs into the system database. The system was also tested on whether it retains correct information relating to the user and it also achieved 100% accuracy. The author concluded that combined together face recognition, graphical and textbased password are effective in authenticating the user. This, therefore shows that the objectives mentioned in chapter 1 were achieved.

5.3 Major Conclusions Drawn

The research has proven that three tier authentication systems are potentially efficient in resolving core deficiencies of previously used single or two tier authentication systems in these domains, yet it a,lso face some few challenges as more data breaching techniques are being

produced. The system is designed to make the authentication of users of university web systems tronger more than before . It has proved to be very advantageous in providing security. In total, the complete system (including all the hardware components and software routines) is working as per the initial specifications and requirements of our project. So certain aspects of the system can be modified as operational experience is gained with it. As the users work with the system, they develop various new ideas for the development and enhancement of the project.

5.3 Recommendations & Future Work

The three tier authentication system has proved to be one of the most efficient method or mechanism of authenticating users who uses the web systems of universities so as to avoid hacking. However it has its own loop holes therfore those gaps call for future work to other future researchers as more data breaches and cyber crime rate is rapidly increasing. The researcher commends that there should be another application attached to the system that runns continuously so that even if the original user left the computer system loged in already another person who is unauthorized can not use the system as it will instantly lock after recognizing that the person is not the registered owner or user. More so the researcher recommends that a warning or notification message is required that is send to the account holder that someone is trying to break into your system and captures the image.

REFERENCES

Anoud Bani-Hani., Munir M., Aisha A., “Online Authentication methods used in banks and attacks against these methods”. 2019.

Mohanaad S., “USER AUTHENTICATION IN PUBLIC CLOUD COMPUTING THROUGH ADOPTION OF ELECTRONIC PERSONAL SYNTHESIS BEHAVIOR ”. 2020.

http://vote.msu.ac.zw/ . 2018.

J. Fagertun, 2005. Face Recognition. Master Thesis, Technical University of Denmark (DTU).

Bleumer, G., 2011, ’Anonymity’, in Van Tilborg H.C.A., Jajodia S. (ed.), Encyclopedia of Cryptography and Security, Springer, Boston, MA.

population using fingerprint, face and iris recognition." Applied Imagery and Pattern Recognition Workshop, 2005. Proceedings. 34th. IEEE, 2005.

Watanabe, M. (2008). Palm vein authentication. Advances in Biometrics (pp. 75–88). Springer. http://dx.doi.org/10.1007/978-1-84628-921-7_5

Eriksson, J., 2014, information och ärenden i e-förvaltningen, Öppna myndigheten. European Commission, 2011, Take your e-identity with you, everywhere in the EU, STORK, viewed 10 January 2019, from https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-youeverywhere-eu

Bekkers, V. & Homburg, V, 2007, The Myths of E-Government: Looking Beyond the Assumptions of a New and Better Government, The Information Society, 23:5, 373-382, viewed 15 January 2022, from https://doi.org/10.1080/01972240701572913

V. Bhatia, R. Gupta, " International Journal of Information Technology," Bharati

Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Dehli, 2014-2015

. A. R. Mohan and N. Sudha, 2009, "Fast Face Detection Using Boosted Eigenfaces", *Proc. 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009)*, pp.102-1006, Kuala Lumpur, Malaysia

Liu, G. Geng and X. Wang, 2010, "Automatically Face Detection Based On BP Neural Network And Bayesian Decision", *Proc. 2010 Sixth International Conference on Natural Computation (ICNC 2010)*, pp.1590-1594, Shandong, China