

**DEVELOPING A MULTI-FACTOR AUTHENTICATION PROTOTYPE FOR
IMPROVED SECURITY OF ENTERPRISE RESOURCE PLANNING SYSTEMS
FOR KENYAN UNIVERSITIES**

Carolyne Wanjiru Kimani

**A Research Project submitted in partial fulfilment of the requirements
for the award of the degree of Master of Science in Applied Information Technology
in the Department of Computer and Information Technology and the School of
Science and Technology
of Africa Nazarene University**

February 2022

DECLARATION

I declare that this document and the research that it describes are my original work and that they have not been presented in any other university for academic work.

Name: Carolyne Wanjiru Kimani

REG NO: 19M03DMIT021



Student signature

24/02/2022

Date (dd/mm/yyyy)

This research was conducted under our supervision and is submitted with our approval as university supervisors.

Supervisor name: Dr. James Obuhuma



University supervisor signature

28/02/2022

Date (dd/mm/yyyy)

Supervisor name: Dr. Emily Roche



University supervisor signature

28/02/2022

Date (dd/mm/yyyy)

Africa Nazarene University

Nairobi, Kenya

DEDICATION

I dedicate this Research Project to my entire family for their immense support, inspiration and encouragement throughout my studies. May God bless you.

ACKNOWLEDGEMENTS

I thank the Almighty God for this opportunity and for seeing me through this research. Secondly, I extend my appreciation to my supervisors Dr. James Obuhuma and Dr. Emily Roche for their guidance, unwavering support, insights, and mentorship during this research. I also thank all those that I worked with, in the course of this research. Finally, I am grateful to my family and classmates for their support and encouragement.

TABLE OF CONTENTS

DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	viii
ABSTRACT	ix
DEFINITION OF OPERATIONAL TERMS	x
ABBREVIATIONS AND ACRONYMS	xi
CHAPTER ONE	1
INTRODUCTION	1
1.1 Introduction	1
1.2 Background of the Study	1
1.3 Statement of the Problem	4
1.4 Purpose of the Study	5
1.5 Objectives of the Study	6
1.5.1 Main Objective	6
1.5.2 Specific Objectives	6
1.6 Research Questions	6
1.7 Significance of the Study	7
1.8 Scope of the Study	7
1.9 Delimitation of the Study	8
1.10 Limitations of the Study	8
1.11 Assumptions of the Study	8
1.12 Theoretical Framework	9
1.13 Conceptual Framework	13
CHAPTER TWO	16
LITERATURE REVIEW	16
2.1 Introduction	16
2.2 Review of Literature	16
2.2.1 Authentication Mechanisms	16
2.2.2 ERP Authentication and its Vulnerabilities	18

2.2.3 Related Work on Multi-Factor Authentication.....	24
2.3 Summary of Review of Literature and Research Gap.....	30
CHAPTER THREE.....	33
RESEARCH METHODOLOGY	33
3.1 Introduction.....	33
3.2 Research Design	33
3.3 Research Site	34
3.4 Target Population	34
3.5 Study Sample.....	34
3.5.1 Sampling Procedure.....	34
3.5.2 Study Sample Size	35
3.6 Data Collection	37
3.6.1 Data Collection Instruments	37
3.6.2 Pilot Testing of Research Instruments	37
3.6.3 Instrument Reliability.....	38
3.6.4 Instrument Validity.....	38
3.6.5 Data Collection Procedures.....	39
3.7 Data Processing and Analysis	39
3.8 Legal and Ethical Considerations.....	48
3.9 Chapter Summary.....	49
CHAPTER FOUR.....	50
DATA ANALYSIS AND FINDINGS.....	50
4.1 Introduction.....	50
4.2 Characteristics of the Respondents	51
4.3 Analysis, Findings and Interpretation.....	54
4.3.1 Authentication Methods used in ERP Systems for Kenyan Universities.....	54
4.3.2 Vulnerabilities of existing ERP systems' authentication methods for Kenyan Universities	57
4.3.3 A Multi-Factor Authentication Framework Prototype	59
4.3.4 Validation of the Multi-Factor Authentication Framework Prototype	67
4.4 Chapter Summary.....	69
CHAPTER FIVE	70
DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS	70
5.1 Introduction.....	70
5.2 Discussion.....	70

5.2.1 ERP Systems Authentication Methods for Kenyan Universities	70
5.2.2 Vulnerabilities of Existing ERP Systems' Authentication Methods for Kenyan Universities	71
5.2.3 A Multi-Factor Authentication Framework Prototype	72
5.2.4 Validation of the developed Multi-Factor Authentication Prototype.....	73
5.3 Summary of the Main Findings	73
5.4 Conclusion.....	74
5.5 Recommendations	75
5.6 Areas of Further Research	75
REFERENCES.....	76
APPENDICES.....	78
Appendix 1 – Chartered Universities in Kenya.....	78
Appendix 2 – Questionnaire.....	80
Appendix 3 – NACOSTI Research Permit	85
Appendix 4 – Reliability Test Output	87
Appendix 5 – Digital Persona 4500 Fingerprint Reader Technical Specifications	88
Appendix 6 – Multi-Factor Authentication Prototype Screenshots	90
Appendix 7 – Multi-Factor Authentication Prototype Source Code.....	99

LIST OF TABLES

Table 2.1: Authentication Mechanisms Comparison	26
Table 2.2: Biometrics Comparison	27
Table 3.1: Reliability Statistics	38
Table 3.2: Summary of Data Analysis Techniques.....	40
Table 4.1: Current ERP Authentication Method Adequacy and Security Rating	56
Table 4.2: Security Attributes of Current ERP Authentication Methods.....	56
Table 4.3: ICT Policy Effectiveness and Level of User Training	61
Table 4.4: Correlations.....	63
Table 4.5: Model Summary	64
Table 4.6: Analysis of Variance (ANOVA).....	64
Table 4.7: Coefficients.....	65
Table 4.8: Test Cases	68
Table 5.1: Summary of Findings.....	74

LIST OF FIGURES

Figure 1.1: Technology Acceptance Model.....	11
Figure 1.2: Conceptual Framework	14
Figure 2.1: Evolution of Authentication Methods	18
Figure 2.2: Most Desired Authentication Methods among Consumers.....	27
Figure 3.1: Process Models for Prototyping	42
Figure 3.2: System Flow Chart	45
Figure 3.3: Database Schema:	48
Figure 4.1: Age Bracket of the Respondents	51
Figure 4.2: Respondents Role in ICT Department.....	52
Figure 4.3: Years of Experience in Systems Administration Roles.....	53
Figure 4.4: Education Level of the Respondents	53
Figure 4.5: ERPs used in Kenyan Universities.....	54
Figure 4.6: Current ERP Authentication Methods.....	55
Figure 4.7: Need for Improving Current Authentication Method.....	57
Figure 4.8: Vulnerabilities of Current Authentication Methods	58
Figure 4.9: Possible Attacks to the Current Authentication Methods Vulnerabilities	59
Figure 4.10: Infrastructure Available to support improved ERP Systems Security	60
Figure 4.11: Authentication Improvement.....	62
Figure 4.12: Proposed Multi-Factor Authentication Framework Prototype	67

ABSTRACT

Automated systems are crucial for organizations to maintain records and transactions effectively. Universities have increasingly adopted Enterprise Resource Planning (ERP) systems, a software that provides integrated management of processes and transactions in real-time. ERP systems contain lots of information and are accessed by multiple users, commonly through usernames and password authentication mechanisms. However, there have been security and privacy concerns about ERP systems' security, where only the traditional authentication method of a username and password is commonly used. Passwords have weaknesses that can be easily compromised. Thus, this research aimed at establishing authentication methods used for ERPs in chartered Kenyan Universities and their vulnerabilities. The study further aimed at developing and validating a multi-factor authentication prototype to improve ERP systems security. Multi-factor authentication which combines several authentication factors such as something the user has, knows, or is, is a new state-of-the-art technology that is being adopted to strengthen systems' authentication security. This research used an exploratory sequential design and a survey for chartered Kenyan Universities. Data collection was done through document analysis, issuing questionnaires online to the universities' system administrators to establish ERP authentication methods and vulnerabilities. The questionnaires were validated by carrying out a pre-study that assessed whether the required data was captured and helped identify areas of improvement. The data collected was analyzed using descriptive statistics, correlation and regression, whose outcome was used as input for the development of a multi-factor authentication prototype. The key vulnerabilities established from the survey were password guessing, password reuse and social engineering hence the proposed multi-factor authentication prototype to counter them. The independent variable factors found to have a positive significant relationship with ERP systems security according to the correlation were; attack tolerance, level of user training and ICT Security policy. The regression analysis model revealed that user training was the most significant variable on improved ERP systems security. This research hence proposed and developed a multi-factor authentication prototype factoring in these variables, to contribute towards the improvement of security of ERP systems for universities in Kenya. The final outcome of the research was a multi-factor authentication prototype combining passwords and biometric authentication, that requires to be coupled with effective user training and enforcement of ICT security policies, to improve ERP systems security for Kenyan universities. As a recommendation for further research, alternative biometric authentication methods, integration of authentication applications and addressing other systems security issues can be explored to further improve ERP systems security.

DEFINITION OF OPERATIONAL TERMS

Authentication: The process of verifying a user's identity, process, or device, as a prerequisite to allowing access to a system's resources.

Authorize: A decision to grant access to a system, commonly automated by evaluating an entity's attributes.

Enterprise Resource Planning: A unified, programmed application software that helps organizations to maintain multiple transactions in one place.

Multifactor Authentication: An authentication mechanism that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authentication factor or by a combination of different authentication factors.

ABBREVIATIONS AND ACRONYMS

CIA:	Confidentiality, Integrity, Availability
ERP:	Enterprise Resource Planning
InfoSec:	Information Security
ISMS:	Information Security Management System
IT:	Information Technology
MFA:	Multi-Factor Authentication
NIST:	National Institute of Standards and Technology
PIN:	Personal Identification Number
SFA:	Single-Factor Authentication
SSO:	Single Sign-On
TAM :	Technology Acceptance Model
TFA:	Two Factor Authentication

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Enterprise Resource Planning (ERP) systems have become valuable information assets in improving service delivery, hence their adoption by Kenyan universities. Authentication is a significant area of ERP system security, influenced by the authentication methods, vulnerabilities, technological infrastructure, information security policies and user training. The main objective of this study was, therefore, to establish authentication methods used in ERP systems in Kenyan universities, identify their vulnerabilities, develop and validate a multi-factor authentication prototype for improved ERP system security for universities in Kenya.

This chapter discusses the background to the study, statement of the problem, the purpose of the study, objectives and research questions. It also discusses the significance of the study, scope, delimitations, limitations, assumptions, theoretical and conceptual framework of the research.

1.2 Background of the Study

Information technology has developed at a high-speed rate and has seen the world rapidly moving towards computing technologies in their operations. Computing has numerous benefits such as real-time transactions, electronic records saving on space, costs and efficiency. This has steered organizations and even individuals to move from manual records and transactions to the use of systems and other digital services. An ERP system is a software consisting of a suite of integrated applications that organizations can use to collect, process, manage, store, and interpret data from business activities. It is an information system that integrates management of all aspects of a business or institutional

processes. It consists of various modules of the operational areas such as student management, student academics, human resources, finance, procurement among others. This integration allows the business units to share, process and communicate information with each other. Benefits of ERP systems include; easier access to accurate information, centralized management, real-time transaction processing, seamless operation, improved service delivery, reduction of costs and redundancy in institutions (Bett, 2018). ERPs have been instrumental in automating organizations with a wide range of operational areas and users.

Universities have not been left behind in adopting ERP systems due to the large population they serve, large amounts of information they keep, and transactions processed. They have invested heavily in these systems both globally and locally to improve their service delivery, efficiency and availability of information (Bett, 2018). These systems contain information, which is one of the most valuable assets to organizations and their stakeholders. Therefore, the systems should be protected as much as possible. However, like all other IT assets, systems have risks and vulnerabilities that come with their use both internally and externally for organizations. Ziani and Al-muwayshir (2017), identified privacy and security as the two major system security concerns. Little investment is made to address these concerns. It is worth noting that attackers are always working tirelessly to exploit these systems for their gains. Unfortunately, gaining illegitimate access to these systems enables attackers to access valuable information for their benefit, to the disadvantage or loss of the owner.

Globally, digital identities have become necessary for organizations and users to access systems, services or resources. Once users register and enroll for digital identity, it

is upon the system to verify the users' identity by authenticating them based on the user authentication information that they have (Grassi et al., 2017). Authentication is the first point of contact for users in a system, and it can be easily compromised through loss or theft of credentials, eavesdropping, shoulder surfing, malware or social engineering (Serianu, 2020). In the recent decade, organizations have indeed realized that authentication by a single factor, which is the most common method, is also one of the weakest methods that need to be improved (First Identity Online Alliance, 2019). This has led to research on ways of strengthening authentication mechanisms.

Authentication factors are categorized based on three metrics, namely, something that the user has, something that the user knows or something that the user is. Multi-factor authentication, a sophisticated authentication method that requires two or more authentication factors to verify an entity's identity, granting system access when they are correct, has been identified as one of the mechanisms of improving system security. It provides enhancements in dealing with the password menace and improving confidentiality, integrity and availability of systems. According to Serianu's Africa Cyber Security Report 2020, identity management is an area of priority, prone to cybersecurity issues that Africa needs to focus on, and can be mitigated through multi-factor authentication (Serianu, 2020).

Across the world, various leading technology companies have moved fast in adopting and implementing optional multi-factor authentication such as Google, Apple, Facebook, Twitter, Visa, Paypal, among others. This aims at securing the large amounts of personal, transactional, sensitive information contained in their systems and mitigating the ever-rising cyber threats (First Identity Online Alliance, 2019). In Africa, multi-factor

authentication is increasingly being adopted in the financial and government digital services systems in various African countries and regional entities such as banks. In Kenya, it is also being adopted in government agency systems such as eCitizen, National Transport and Safety Authority, National Health Insurance Fund (NHIF), mobile money services and banks which have implemented multi-factor authentication to provide secure banking services to their clients. Universities in Kenya use single-factor authentication, commonly username and passwords. Cyber threats towards universities and student hacktivism have been on the rise and thus require secure solutions to be developed (Mayieka, 2019). This research therefore, aimed at exploring the use of multi-factor authentication towards the improvement of the security of ERP systems for Universities in Kenya. This will in return ensure that they maintain confidentiality, integrity and availability of their information.

1.3 Statement of the Problem

Most Universities in Kenya have implemented ERP systems. In an ideal case, these systems should ensure confidentiality, integrity, availability of their data, records and information at all times. However, using these systems presents security risks and vulnerabilities due to the large amounts of valuable and sensitive information they contain, which, is of interest to different parties. Authentication is a common risk area since it is the entry point for an ERP system, which, if compromised, attackers gain access to lots of information, transactions and operations. Mayieka (2019), highlights that institutions of higher learning in Kenya, Africa and globally, are facing a high rate of increase of cyber-threats and underscores the importance of reinforcing responsible cybersecurity measures and investing in cybersecurity technologies. According to First Identity Online Alliance, (2019), the use of passwords alone is considered the most vulnerable authentication

method, thus, needs to be done away with or improved. Passwords can be easily cracked, guessed or attacked since most passwords are based on users' personal information. Student hacktivism to interfere with school information systems to alter students' grades, fee balances have also been on the rise and therefore requires proper solutions to be developed (Mayieka, 2019). Single-factor authentication, that is, username and password, is commonly used for ERP systems authentication in Kenyan Universities. The Ministry of Foreign Affairs of the Kenyan Government has been a victim of hacking where attackers stole user passwords and used them to steal sensitive data from the ministry's communication system. This attack was suspected of having involved Kenyan University IT students, exploiting user password vulnerabilities (Mutambo, 2016).

Wanjala (2020), highlights a report suggesting hackers were sharing Mount Kenya University students' data online, such as names, addresses and phone numbers. This was after hackers discovered vulnerabilities on their websites and databases, as well as that of three Nigerian universities. One of the Nigerian universities stored usernames and passwords online in plain text. The sharing of this data left the students vulnerable to online attacks. The increase in cybersecurity threats, therefore, calls for the improvement of ERP authentication to ensure systems security. This research, therefore, proposed to address this gap by developing and validating a multi-factor authentication prototype to improve ERP systems security for Kenyan Universities.

1.4 Purpose of the Study

The purpose of this study was to develop a multi-factor authentication prototype to improve ERP system security for universities in Kenya.

1.5 Objectives of the Study

1.5.1 Main Objective

The overall objective of the study was to develop and validate a multi-factor authentication prototype for improved Enterprise Resource Planning(ERP) system security for universities in Kenya.

1.5.2 Specific Objectives

1. To identify the current authentication methods used in ERP systems for Kenyan Universities.
2. To establish vulnerabilities of existing ERP systems' authentication methods for Kenyan Universities.
3. To develop a multi-factor authentication framework prototype for improving ERP system security.
4. To validate the multi-factor authentication framework prototype for effectiveness in improving ERP system security.

1.6 Research Questions

1. What authentication methods are used for ERPs in Kenyan Universities?
2. What are the vulnerabilities of the current ERP system authentication methods in Kenyan Universities?
3. How can multi-factor authentication be used to improve ERP security?
4. How effective is the proposed multi-factor authentication approach to improving ERP systems security?

1.7 Significance of the Study

ERP systems are a key investment by institutions of higher learning which have enabled them to improve their services by providing information in real-time, with accuracy and efficiency. These systems contain lots of valuable information that is of interest to many parties. ERP systems have provided Universities with a central means of coordinating and controlling their operations through a unified information structure (Muiruri, 2015). However, security measures in place need to be improved, to secure the ERP systems, which are often targeted by attackers within and outside the organization (Serianu, 2020). It was, therefore, necessary to conduct this study to identify ERP authentication methods in Kenyan universities, their vulnerabilities and ways of enhancing secure authentication. This research sought to develop a multi-factor authentication prototype to improve the ERP system's security. It gives insights into the security vulnerabilities facing ERP systems and authentication methods. It will also be beneficial to universities and other government agencies to enhance the security of their systems.

1.8 Scope of the Study

There is a wide range of security issues affecting ERP systems in universities in Kenya. However, this study focused on authentication since it is the entry point of a system. Authentication is the most commonly exploited vulnerability both internally and externally for organizations. Universities have a high population of students and other stakeholders, therefore, containing large amounts of data that attackers may target. This study surveyed chartered Kenyan universities only, as published by the Commission for University Education (CUE). It targeted ICT personnel carrying out ERP systems administration roles in each university since they are directly involved in ERP authentication and systems

security. This research identified current ERP system authentication methods in Kenyan universities, established their vulnerabilities, developed and validated a multi-factor authentication prototype to improve ERP system security for Kenyan Universities.

1.9 Delimitation of the Study

The main delimitation of this study was that it was confined to ERP systems authentication methods, their vulnerabilities, developing and validating a multi-factor authentication prototype to improve ERP system security for Kenyan universities. The study focused on authentication and did not cover other security issues of the ERP systems. Another delimitation of this study was that participants only included ICT personnel carrying out system administration roles and not other system users in Kenyan Universities.

1.10 Limitations of the Study

This study was carried out against the following limitations:

1. Universities are geographically diversely located in Kenya, hence creating a challenge in physical access during data gathering. This was moderated by using an electronic survey to reach the universities.
2. During the study, the COVID-19 pandemic led to the closure of universities, new ways of carrying out tasks online and social distancing. This was moderated by using an electronic survey to ensure the data is collected while observing the new measures.
3. Universities vary in size, infrastructure, population, among other factors, which influence the systems they use and systems security challenges. This was moderated by conducting the survey based on their current systems and infrastructure.

1.11 Assumptions of the Study

This research was conducted under the following assumptions:

1. The respondents provided truthful, accurate and reliable information to the best of their knowledge.
2. Information Technology experts are best placed to provide information on authentication of ERP systems in Kenyan universities, and therefore, the survey only covered system administrators or persons designated to carry out these roles.
3. Literacy levels of users in these institutions are adequate for implementing the anticipated secure ERP systems' authentication.
4. The respondents provided data for the study while adhering to privacy policies and the sensitive nature of information systems security. The survey conducted allowed for anonymous responses and was in line with the organizational privacy policies.

1.12 Theoretical Framework

There exist various security theories, frameworks and guidelines for information systems security as discussed below:

a) Socio-Technical Systems Theory

This theory views an organization system as a set of interdependent sub-systems comprised of goals, people, processes/procedures, technology, physical infrastructure and culture. The core of this theory is that systems design should factor both social and technical aspects, allowing people to work with technology in ways that enable the achievement of organizational goals and societal benefit. Changes in any component of socio-technical systems affect the others. Information security is considered to be a continuous socio-technical practice. Technological, people and organization attributes, and interactions of these sub-systems contribute to the preservation of information security. Security controls such as authentication, are a crucial component of socio-technical

systems that protect or mitigate an organization and its assets against threats and vulnerabilities (Zaini et al., 2018).

The socio-technical systems theory views the holistic, unified role of technology and people to operate and interact with systems. It enables the design of systems that are adaptable and contribute to effective work in changing environments. This model has been applied in large technology companies and platforms such as Facebook, Twitter, LinkedIn and Apple.

The Socio-Technical Systems Theory was applied in this study by assessing and factoring its various components when carrying out the research, prototype design and development. These components were; system users, technology, infrastructure, organizational processes of ERP systems authentication and security controls. This contributed towards developing the multi-factor authentication prototype for improving ERP systems security for Kenyan Universities.

b) Technology Acceptance Model (TAM)

TAM is a common theory applied to evaluate the acceptance level and usage of technology by users. It is based on two related aspects namely: perceived usefulness and perceived ease of use, which evaluate the user's intention to use a certain system or technology. Perceived ease of use refers to the perception of the technology from a users's perspective while perceived usefulness is the degree to which users feel they will benefit from using a certain system or technology (Opoku & Enu-Kwesi, 2020).

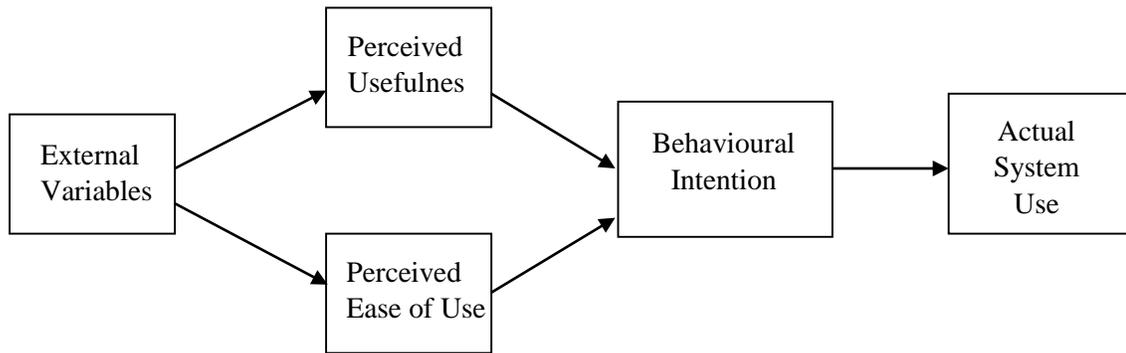


Figure 1.1: Technology Acceptance Model

The Technology Acceptance Model was applied by identifying the current ERP authentication methods, rating their effectiveness, adequacy, usability and vulnerabilities, and developing the multi-factor authentication prototype for improved ERP systems security for Kenyan Universities.

c) National Institute of Standards and Technology - Digital Identity Guidelines SP 800-63-3

NIST provides these guidelines for the technical specification for the implementation of digital identity services. It involves identity proofing and authentication of users such as staff, contractors and other parties interacting with government systems through open networks. These guidelines define the technical specification for identity proofing, registration, authenticators, management processes, and authentication protocol. Digital identity is the online persona of an entity. Users have digital identities for various systems such as email, to identify them as the owners of a particular record and to grant them access to certain services. It is difficult to prove someone is indeed whom they claim to be online, and impersonation is possible hence the guidelines to mitigate against such vulnerabilities. They require users to be represented uniquely and to prove they are the represented entity. Identity proofing verifies that a subject or entity is who they claim to

be. This is done by subjecting them to digital authentication, where the system is in control of verifying their identity by requiring them to provide authenticators associated with the subject. This has been challenging due to multiple opportunities for impersonation and other attacks (Fenton et al., 2017).

SP 800-63-3 categorizes the guidelines into; enrollment and identity proofing, authentication process and federation assurance level processes, to enable ease of management and flexibility in implementing solutions for digital systems. Their roles are;

1. SP 800-63-3A Enrollment and Identity Proofing addresses how applicants are uniquely identified, enrolled and can prove their identities as valid subscribers within a system. It provides specifications and ways in which users can enroll and prove identity for both physically present and remote scenarios of system access.
2. SP 800-63-3B Authentication and Lifecycle Management provide a reasonable risk-based assurance of the user's identity for systems they visit often or a set of digital services and the process of binding authenticators to subjects. Authenticators are classified based on three factors of authentication: something that the user knows, has or is. A combination of more than one authentication factor is referred to as Multi-factor authentication. The number of factors used determines the strength of the authentication systems. The more the factors are, the more robust the system is considered to be. However, two factors are considered to adequately meet high-security requirements.
3. SP 800-63-3C Federation and Assertions are used to relay the results of the authentication processes and relevant attribute information to involved parties (Grassi et al., 2017).

The NIST Digital Identity guidelines were applied in the authentication of ERP users and the basis upon which the multi-factor authentication prototype was developed with enrollment and identity proofing, authentication and lifecycle management and federation and assertions functionalities.

1.13 Conceptual Framework

The conceptual framework in Figure 1.1 below illustrates the independent and dependent variables for the study. The socio-technical systems theory was applied in this study by the inclusion of the following variables in its subsystems;

- Goals - ERP systems security and attack tolerance.
- Processes/procedures - Systems authentication, ICT policy and vulnerabilities.
- Culture – ICT policies.
- People – User training and usability.
- Infrastructure – Infrastructure.
- Technology – authentication mechanisms and vulnerabilities.

The Technology Acceptance Model theory was applied in the usability and improved ERP systems security variables of this study.

Systems authentication influences ERP systems security. The independent variable, system authentication, is based on vulnerabilities, authentication methods, infrastructure, information security policies and user training. The dependent variable improved ERP system security, is based on the CIA triad model that addresses information system security concerning confidentiality, integrity, availability, and system-related factors on usability and attack tolerance.

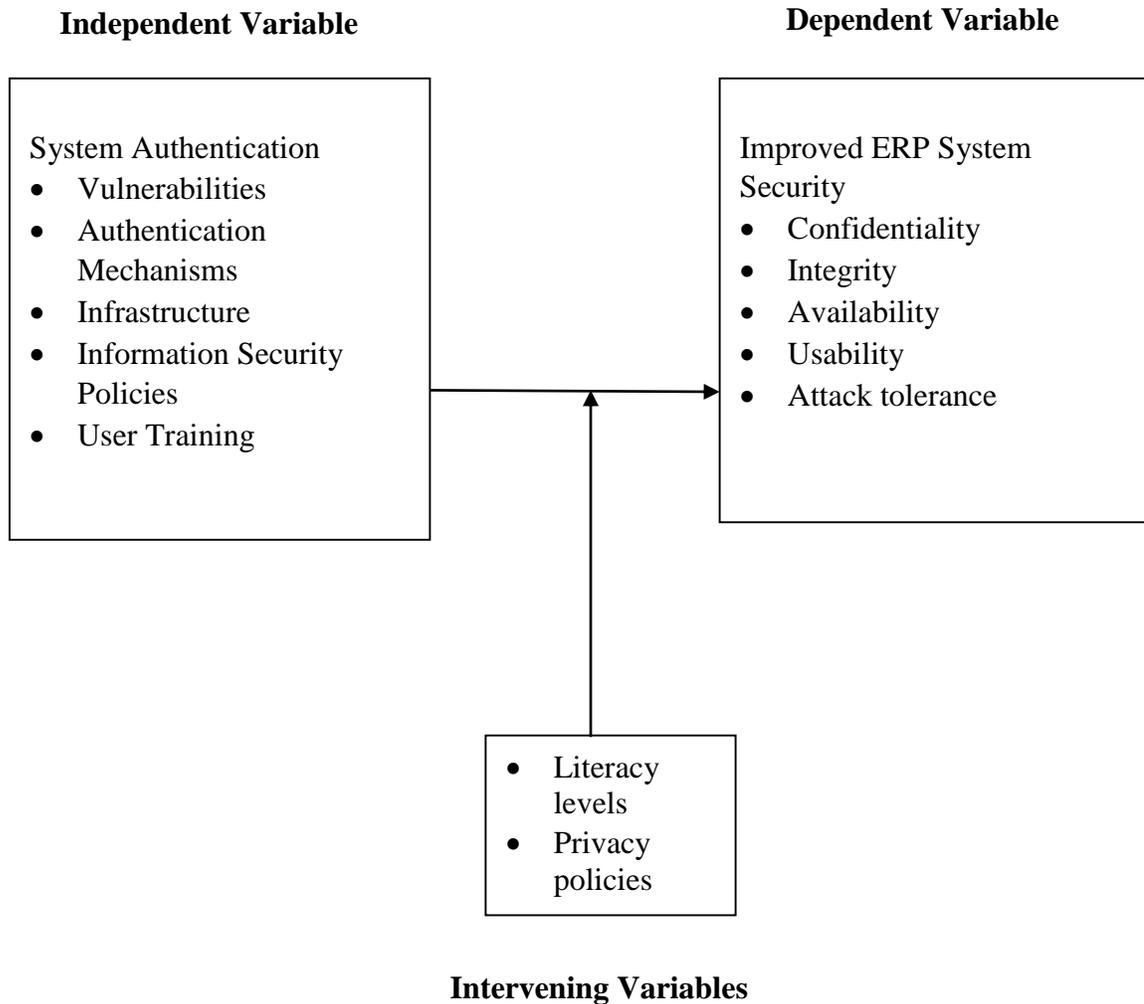


Figure 1.2: Conceptual Framework

Relationship between the independent and dependent variable:

The independent variable system authentication is centered on the following aspects which influence ERP system security;

- Vulnerabilities - establishing risks and security issues enables the implementation of appropriate authentication and countermeasures, therefore, ensuring system security.
- Authentication mechanisms – there are various types of authentication mechanisms, with each having its pros and cons. The use of more secure authentication methods

improves system security. The authentication methods should be effective and user-friendly.

- Infrastructure – Use of authentication methods with readily available hardware/software and at a reasonable cost, enables improvement of ERP system security.
- Information Security Policies - organizations that have information security policies can integrate them into their system authentication methods, therefore ensuring all-round system security.
- User Training - users are one of the most vulnerable components of attacks in systems because they are assigned rights and privileges. Training users on secure system authentication, enables them to effectively use secure authentication methods, makes them less prone to attacks and vulnerabilities hence improving ERP system security.
- However, improving ERP system security requires user literacy and compliance with privacy policies by users, which are the intervening variables of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews related literature categorized into sections derived from the research objectives. The purpose of this study was to establish ERP authentication methods for Kenyan universities, their vulnerabilities and how their security can be improved using multi-factor authentication. The literature review is organized into the following sections; authentication mechanisms, enterprise resource planning systems authentication and its vulnerabilities, related research and a summary of the research gap.

2.2 Review of Literature

2.2.1 Authentication Mechanisms

Authentication is the verification of the user's, process or device's identity to allow access to the system's resources. A secure authentication scheme should adhere to the ISMS requirements of confidentiality, integrity and availability. Authentication can be categorized into three, based on authentication factors: something that the user knows, something that the user has and something that the user is. The use of at least two or three factors for verification is considered to provide a positive, secure authentication.

1. Knowledge Factors: Something that the user knows such as; password, Personal Identification Number (PIN), passphrase, security question or challenge-response.
2. Ownership Factors: Something the user has like an identification card, security token, device token or Quick Response (QR) code (Akif, 2017).

3. Biometric Factors – Something the user is or does like a fingerprint, iris, retinal pattern, face, voice, DNA, signature or any other biometric identifiers. They are also known as inheritance factors (Ometov et al., 2018).

Additionally, location-based factors are an emerging authentication factor, which is somewhere the user is and can be in the form of a connection-specific network or Geographical Positioning System (GPS) location identification (Akif, 2017).

Single-Factor Authentication

Uses only a single factor from one of the three categories of authentication factors above to verify the identity of an entity. It is considered the most common method due to usability and familiarity, however, it is the weakest level of authentication, that can easily be guessed, stolen, memorized, reset or bypassed.

Multi-Factor Authentication

This is a sophisticated authentication method that requires two or more authentication factors from the different categories of authentication factors to verify an entity's identity, and therefore, grant system access when they are correct. It is done by a combination of elements from these factors as follows:

- Two-Factor Authentication is a type of multi-factor authentication, where users confirm they are indeed who they claim to be by providing a combination of two different authentication factors. Typically providing correct login plus another additional verification factor. For example, to withdraw money from an Automated Teller Machine(ATM), a user is required to provide an ATM card and enter a correct PIN for them to be granted access to carry out their transactions. A One-Time Password (OTP) can be used to supplement user passwords or code-generated security tokens.

Two Factor Authentication confirms a user's identity by use of something they know, mostly a password, and an additional second factor of something they have such as a code sent to them or something that they are.

- MFA has been known to be a better security option; however it has implementation complexities, requires deployment and integration of additional software for them to work. This will change with time as firms explore unified multi-factor technologies and standards to improve on passwords and at the same time provide usable and practical methods (Velasquez et al., 2019).
- Biometrics has also been a standard security solution; however, it is quite costly and has its challenges hence it has still not been adopted much (Grassi et al., 2017).

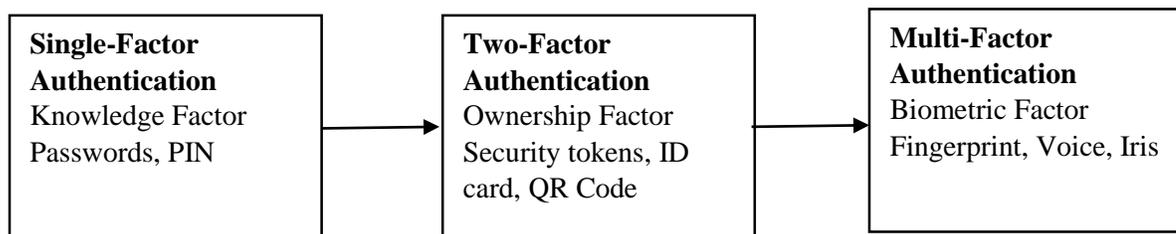


Figure 2.1: Evolution of Authentication Methods

2.2.2 ERP Authentication and its Vulnerabilities

Enterprise Resource Planning involves the integrated management of main organizational processes, often in real-time done using software and technology. An ERP system is a business management software consisting of a suite of integrated applications that enable organizations to collect, process, store, manage and interpret data from several business activities. ERPs have become one of the latest technologies universities in Kenya are investing in, in terms of financial and human resources (Bett, 2018). ERPs help institutions achieve several functionalities, but one area still proves difficult – Security and

Controls (Rathore & Gupta, 2017). These systems require secure authentication, which is the process of verifying an entity's or device's identity, to allow them access to specific resources upon request. This is crucial for managing these ERP systems, which have a large number of users, and secure authentication is still a significant challenge.

Rathore and Gupta (2017), identify some areas in which ERP security fails due to vulnerabilities in the enterprise environment, authentication and authorization. Vulnerabilities are system weaknesses that can be exploited and include: Standard Query Language(SQL) injection, information disclosure, impersonation, denial of service, switchable authorization, directory traversal, clickjacking, among others. This study discusses the ERP security solutions in physical, transmission, storage, access, data and application security. User authentication through a password and username needs robust checks, which imply the use of mechanisms such as one-time passwords. It also identifies continuous monitoring as the solution once built-in controls are handled in the system.

Ziani and Al-muwayshir (2017), review Cloud ERP security challenges, their existing solutions and propose an effective approach to cloud ERP security management. This research identifies measures to improve ERP security and privacy in the following areas; data storage, virtualization, improved access control and two-factor authentication. A descriptive survey research on the *Challenges and Prospects of Enterprise Resource Planning (ERP) Systems in the Newly Chartered Public Universities in Kenya* identified top management support as the major challenge of ERP systems. It however does not highlight the critical aspect of the system's security (Bett, 2018).

In 2019, the United States Department of Education released a security alert on the Ellucian ERP systems vulnerabilities targeted by hackers. The attack targeted

authentication mechanism vulnerabilities, where they would intercept students' sessions and get authentication details to create fake accounts. Within 24 hours, over 600 fake accounts had been created, causing a denial of service to legitimate users. The affected institutions were advised to put in place adequate security measures to prevent unauthorized system access. One of the best practices recommended in this case was to enable multiple authentication methods and continuous activity monitoring (TrendMicro, 2019).

Mayieka (2019), evaluates emerging issues in cybersecurity for higher learning institutions in a descriptive survey from secondary data. This survey established that cyber-attacks have become common to institutions of higher learning and cannot be underestimated as they evolve with emerging technologies (Communications Authority of Kenya: Kenya National Bureau of Statistics, 2016). The attacks are considered as data exfiltration, cyberstalking, data interception, identity theft, denial of service attack, network interference, data theft, cybercrime-related data/information access such as unauthorized and unauthenticated data/information access, virus distribution, among others. This has resulted in these institutions incurring substantial economic costs, services mislay and even legal action against modification of data such as school fees balance, student's grades among other breaches both by internal parties such as students, staff and external parties such as competitors and malicious attackers. It reviews ways in which institutions are attacked and recommends improvements on their defence mechanisms against cyber-attacks. This study underscores the importance of reinforcing and investing in their security measures. Among the proposed solutions to these challenges is the implementation of secure authentication techniques, cybersecurity awareness among all

stakeholders, enforcement of InfoSec policies, investing in up-to-date technologies, research, frequent cybersecurity training, conferences and training students on cyberethics (Mayieka, 2019).

The Ministry of Foreign Affairs of the Kenyan Government has been a victim of hacking where attackers stole user passwords and used them to steal data from the ministry's communication system. The attackers did this by sending phishing emails to junior staff advising them to change their passwords, where some users fell victim. The victims' credentials captured were used to access government documents and correspondences, which mainly were classified as open. In a consequent attack, the hackers gained access to confidential documents with correspondence on sensitive communication on security issues and international agreements. This attack was suspected of involving Kenyan University IT students, working closely with other hackers around Africa. This attack exploited user password vulnerabilities (Mutambo, 2016).

The Kenyan Government has been a victim of hacking where official websites such as the Integrated Financial Management Information Systems (IFMIS) website was defaced and functionality disabled by a team calling itself Kurd Electronic Team. Other websites that were hacked were the National Youth Service and Judicial Service Commission. The ICT Authority managed to recover the websites after the attacks (Kimuyu, 2019).

An empirical study targeted at providing a roadmap for a holistic examination of the efficiency of integrating ERPs assesses hurdles faced by universities that have implemented ERP (Singoro et al., 2018). Data collection for this study was done through questionnaires, interview schedules and content analysis. One of the challenges identified

is the provision of security of examination data. Findings include; the use of ERP systems for solving the missing marks challenge, security of examination data by training users and securing authorized access (Singoro et al., 2018). This study leaves a gap in securing the authentication process, which has been the vulnerability attacked in some cases, to access student marks and make unauthorized changes.

Alaca (2018), reviews common vulnerabilities and attacks on user authentication which may arise internally or externally in an organization, which are as follows:

1. Password Discovery Attack

This can be done through various means such as dictionary attacks, brute force attacks, weak password recovery validation, video recording, stolen verifier attack and shoulder surfing.

- Dictionary attack – vulnerability where programs have built-in dictionaries, and attackers attempt all dictionary words to find the correct passwords assuming users may have used the dictionary words.
- Brute Force attack – attackers, use trial and error to guess all possible passwords users may have used as their password until they find the correct password.
- Weak password recovery – attackers take advantage of password recovery schemes, posing as the user attempting to recover their account password and reset it, locking the legitimate user out. If additional information is required by the password recovery scheme, they use a brute force attack to guess the correct information such as the security questions or change recovery phone number or email to theirs.
- Video recording – attackers may record a video capturing users entering their login credentials, they later review it and use it to log in, using recorded credentials.

- Stolen verifier attack – attackers access password tables stored by a verifier and then attempts offline guessing attacks by running scripts until they manage to get correct login details.
 - Shoulder surfing – uses social engineering to monitor users entering their login credentials, such as observing keystrokes as the user types their password and then uses the observed credentials to log in (Garrett, 2016).
2. Leaks from other verifiers – use of authentication details from other websites, applications and platforms by attackers to impersonate users.
 3. Phishing – deceiving users by redirecting them to an illegitimate application or website, which is usually similar to the legitimate one, and gaining their login details without their knowledge and permission.
 4. Man-in-the-middle attack - In this method, attackers secretly intercept and may even alter communication between two parties in communication during the authentication process. It takes various forms; flooding attacks, eavesdropping, impersonation attacks, browser attacks, session high-jacking and Secure Socket Layer attacks.
 5. Replay Attack – attackers intercept messages with credentials of a legitimate user and once they log off, the attacker replays the message with login credentials to gain system or server access.
 6. Targeted impersonation – attackers use personal information linked to a user to gain access, such as ID number, date of birth, phone number or relative's names.
 7. Physical theft – stealing of user credentials from where they are stored.

8. Internal observation – monitoring user credentials through malware installed on their devices or by interception of credentials between the user’s device and the verifying agent.
9. Denial of Service Attack – this is an attack that occurs when attackers overload authenticating servers with fake authentication requests to overwhelm them and as a result, prevent legitimate users from accessing systems or services (Miessler, 2021).

2.2.3 Related Work on Multi-Factor Authentication

Numerous research has been done on improving systems authentication techniques using multi-factor authentication. Various studies were reviewed during this research and are discussed in this section.

According to Alaca (2018), user authentication is one of the critical tools that safeguards user accounts from unauthorized access. Password is the most common user authentication method. It has well-documented usability and security drawbacks. This study identified, developed and evaluated fingerprinting options for use with passwords and offered direction on their use to enhance web authentication security. A comprehensive methodology is recommended for evaluation of the mimicry resistance and guides on combining multiple authentication schemes alongside passwords, to improve security. It enforces comprehensive analysis and evaluation of a variety of Single-Sign-On (SSO) schemes that allow users to access many services online through a single master password, is carried out using a proposed evaluation framework revealing the benefits and drawbacks of different designs. SSO requires users to authenticate to an Identity Provider to establish an authentication session, providing proof of identity to authenticate users without requiring any additional authentication tasks.

This research identifies a gap in the need for improving the password authentication mechanism with minimal impact on usability and without necessarily supplementing it since users are well familiar with it. The proposed Single-Sign-On (SSO) authentication system using a master password has the risk of loss or theft and leaves users' multiple accounts vulnerable. It also has a cost implication and risk of involving a third party to provide these services.

A research carried out by Ting et al., (2016), reviews methods to secure resources using a multi-factor authentication policy consisting of various access control methods. Combining physical and logical access control requires all these systems to be integrated to use a standard protocol for information exchange among various components or devices. Multi-factor authentication can also be problematic where multiple systems are being managed as separate entities. It is based on rules and policies for the users and access to resources requests. Securing authentication per request for resources can also be applied. Various levels of authentication factors are considered, before granting a user access to increase assurance that the user is indeed authorized to access a secure system. This study reviews ERP security and proposes a new model for secure cloud ERP environments. One of the solutions proposed is the use of dynamic credentials based on the user's location or data packets and digital signatures to improve data security. The gap in this research is that not all universities in Kenya are using cloud-based ERP systems. Dynamic location-based credentials would therefore be a challenge to users and requires them to have a secure internet connection like a virtual private network anytime they need to access the system.

Ali et al., (2020), recommend biometrics as a powerful method to counter vulnerabilities and attacks. Biometrics provides a unique physical or behavioural

characteristic to verify a user's identity, offering security against shoulder surfing, identity theft, replay attacks and impersonation. Biometrics is considered an accurate authentication mechanism as shown in Table 2.1 below:

Table 2.1: Authentication Mechanisms Comparison

Authentication Mechanisms	Accuracy	Cost	Devices Required	Social Acceptability
Biometrics	High	Medium	Biometric Devices	High
PIN	Medium-low	Low	Keypad	High
Password	Medium-low	Low	Keypad	High
Pattern	Medium-low	Low	Scanner	Low
Smartcard	Medium	Medium	Card Reader	High

Source: Dahea & Fadewar, 2018.

Velasquez et al., (2019) recommend a combination of authentication techniques to increase systems security and proposed a multi-factor authentication methods framework for comparison and selection. The various biometrics types are compared as shown in Table 2.2, based on the seven criteria for an effective biometric system which are:

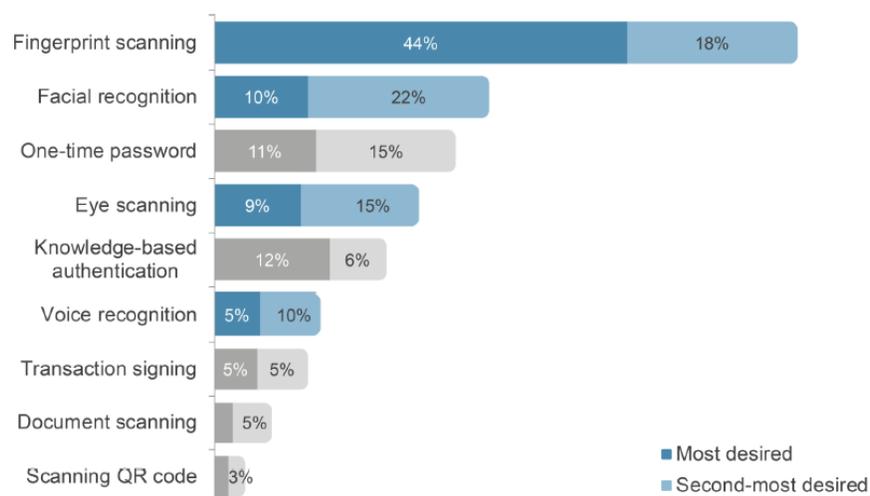
1. Universality – should use a common trait among users.
2. Distinctiveness – provides unique user recognition and cannot be the same among different users.
3. Permanence – can be sufficiently constant, stored for some time without changing.
4. Collectability – can be easily obtained from individuals without any inconvenience.
5. Performance – should provide speed, accuracy and efficiency of the technology.
6. Acceptability – should be easy to use and user-friendly.
7. Circumvention – cannot be reproduced or deceived.

Table 2.2:Biometrics Comparison

Biometric Identifier	Finger	Facial	Iris	Head	Retina	Signature
Characteristics						
Universality	high	high	high	mid	high	low
Distinctiveness	high	low	high	mid	high	low
Permanence	high	mid	high	mid	mid	low
Collectability	mid	high	mid	high	low	high
Performance	high	low	high	mid	high	low
Acceptability	high	high	low	mid	low	high
Circumvention	mid	high	low	mid	low	high

Source: Dahea & Fadewar, 2018.

According to First Identity Online Alliance, (2019), fingerprint scanning was the most desired authentication feature among consumers as shown in Fig. 2.2.

**Figure 2.2:** Most Desired Authentication Methods among Consumers

Source: Javelin Strategy & Research, 2018.

Multi-factor authentication is commonly being adopted in the banking, mobile money, healthcare sectors in the African region and Kenya. In other sectors, it has been adopted in the email systems provided by third parties such as Gmail, Microsoft Outlook, where it can be set as optional. Serianu, (2020) recommends the implementation of multi-factor

authentication and biometrics to improve systems identity and access management in Africa. Below is a review of multi-factor authentication-related work in Kenya.

According to Ntonja et al., (2020), Cloud Health Information systems have become popular to enable data sharing, real-time access to critical information and coordination of clinical services in the health sector. They are however faced with privacy and security concerns due to the sensitive nature of medical information. This descriptive, experimental study focused on the enhanced security of cloud health information systems through multi-factor authentication. The study was carried out in Maua Methodist Hospital in Meru county, Kenya, surveying middle and senior-level managers who understand the technology in the hospital's operations. Thirty-one online questionnaires were issued to assess cloud computing threats and opportunities in healthcare. The survey established privacy, cost and availability as some of the factors affecting cloud computing use in healthcare. The study proposed an attribute-based authentication model for robust data privacy models. The proposed model uses the legacy password system, adds multiple authentication mechanisms of random six-character one-time passwords and incorporates encryption for data transmission, shown in a prototype. This study recommended exploring how confidentiality and data privacy is being implemented in other sectors. Similar strategies can be replicated in other systems.

E-commerce is the modern way of carrying out business transactions where electronic payment systems are used. This has created opportunities, risks and vulnerabilities for the e-commerce platforms. E-commerce security is essential, this study aimed at addressing security issues associated with password-based authentication mechanisms in e-commerce websites. The study used a design science approach, focus group discussions of 7 security

experts from Jphiego Corporation were used to collect data on password-based authentication challenges, ways of enhancing security using passphrases and its implementation on e-commerce websites. It sought to enhance security by designing a module that incorporates passphrases to mitigate password guessing and brute force attacks. A prototype was developed following passphrase guidelines. Upon entry of correct passphrases, users were able to update or modify their shopping carts. The prototype validity was tested by a team of experts, with results demonstrating that passphrases can enhance e-commerce security (Odera, 2016).

Mpesa is a convenient mobile money transfer service in Kenya that has grown phenomenally, expanding to an international platform. One of the challenges it faces is, increased fraud cases to swindle subscribers. Chetalam, 2018, carried out research aimed to improve the Mpesa authentication process by incorporating voice biometrics for better user control and efficiency. The objectives of this research were; to establish mobile money services authentication mechanisms, investigate primary Mpesa fraud techniques, to implement and analyze an effective, secure mobile-based multi-factor authentication scheme using device ID, voice biometrics and a PIN to secure Mpesa transactions. The study sample was thirty-two Mpesa subscribers in Mirema area selected using purposive sampling. The data was collected using questionnaires on google forms and analysed using quantitative techniques. The study indicated that the common mpesa authentication scheme was a four-digit mpesa PIN, with 75% finding it insufficient for mpesa security. The majority of the respondents felt that incorporating biometrics will improve mpesa security. The primary mpesa fraud techniques used in Kenya were transaction reversal, unauthorized SIM card swapping, identity theft, scam messages. The study modelled VMPESA to

implement a secure mobile-based multi-factor authentication method using device ID, voice biometrics and a PIN to secure Mpesa transactions due to the weaknesses of using single-factor authentication. It recommends the incorporation of multi-factor authentication by mobile money service providers to improve security, reduce fraud cases and subscriber money losses (Chetalam, 2018).

Fingerprint biometrics have advantages of high-security assurance, usability, privacy, non-transferability and are difficult to circumvent. The National Hospital Insurance Fund (NHIF), a Kenyan government medical insurance scheme, recently introduced the use of fingerprint biometrics to identify members and their dependents, as a move to tackle fraud and speed up the medical claims payment process. NHIF is migrating from the use of physical NHIF and national identity cards, as the identification mode of members and their dependents, due to the loopholes faced of fraudulent claims as a result of fake identities seeking medical care and hospitals processing false claims. Adoption of the new system requires biometric registration and identity verification of members and dependents, which will allow for the electronic processing of claims. This aims to improve efficiency, identity verification and reduce fraudulent claims arising from impersonation (Alushula, 2021).

2.3 Summary of Review of Literature and Research Gap

Several studies have been conducted in this area and reveal ERP systems are prone to a wide range of vulnerabilities (Alaca (2018), (Bett, 2018), (Miessler, 2021), (Mayieka, 2019), (Rathore & Gupta, 2017), (TrendMicro, 2019) and (Ziani & Al-muwayshir, 2017)). It is difficult to address each of these vulnerabilities, and continuous monitoring is necessary for all of them. The literature review identified the following gaps:

1. A general overview of Security Hurdles and Proposed Security Measures for the ERP systems in the management of academic affairs is carried out, identifying secure system access as one of the hurdles, however leaving a gap on how secure systems access and authentication can be achieved (Singoro et al., 2018).
2. According to Bett (2018), ERP system implementation success is majorly based on top management support factors, which is still a challenge. This study leaves a gap in the critical security factor contributing to ERP system success.
3. Password is the most common user authentication method, with well-documented usability and security drawbacks burdening users to secure their accounts through their passwords (Alaca, 2018). It is necessary for the password authentication method to be reinforced, to improve systems security.
4. Authentication is a prominent ERP security area of concern since the traditional authentication method of passwords is the most commonly used due to its usability and familiarity. It is, however the weakest authentication method and requires to be improved, if not done away with (First Identity Online Alliance, 2019).
5. Learning institutions are highly prone to cyber-attacks, underscoring the importance of reinforcing and investing in security measures. Among the proposed solutions to their security challenges is implementing secure authentication techniques (Mayieka, 2019).
6. Most of the multi-factor authentication schemes in Kenya identified in the literature review are for improved systems security in the banking, mobile money and health sectors. This shows the need for enhanced systems security in the education sector systems.

7. A study by Islam, (2015) recommends the incorporation of multi-factor authentication to secure ERP systems but also highlights the complexity and additional costs that come with it hence its slow adoption.

From the identified gaps, this research aimed to address the ERP authentication security challenges by proposing a multi-factor authentication prototype to enhance the security of ERP systems used in Kenyan Universities.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology used in this study, outlined in the following sections: research design, research site, target population, study sample, data collection instruments, procedures, processing, analysis and the legal and ethical considerations of the research.

3.2 Research Design

The study used an exploratory sequential research design. Exploratory sequential design is an approach that combines qualitative and quantitative data collection in a sequence of phases. It starts with the first phase collecting qualitative data, analyzing it, the results of the first phase, then directs the next quantitative phase (Cresswell, 2018). The research aimed to survey authentication methods for ERP systems in Kenyan universities, their related vulnerabilities, to develop and validate a multi-factor authentication framework prototype for improving ERP authentication security.

The research design was guided by the objectives of the study and combined several approaches, which include qualitative, quantitative and mixed methods as follows. Document review and analysis were carried out on ERP authentication methods and their vulnerabilities. After the document analysis, questionnaires were designed in Google Forms, validated through a pre-study, issued for data collection by sharing the Google Form link to participants whose responses were captured in a Microsoft Excel downloadable file. The survey was conducted using questionnaires to identify ERP authentication methods used in chartered universities in Kenya to achieve the first objective.

The data collected from the survey was analyzed and the results were used to guide the development of a multi-factor authentication prototype for ERP systems for universities in Kenya.

3.3 Research Site

The research was conducted in Kenya by involving Kenyan universities as listed in section 3.5.2.

3.4 Target Population

The target population for this study was the forty-nine (49) chartered universities in Kenya, as listed in Appendix 1.

3.5 Study Sample

3.5.1 Sampling Procedure

This study combined stratified and random sampling. Stratified sampling was used to categorize the universities into two categories; public and private universities for subsequent analysis. The universities involved in the survey from these two strata, public and private universities were then selected randomly. Purposive sampling, which involves the selection of respondents that represent the population, was employed in the next phase to determine the respondents for the survey. This involved a conscious selection of the participants, who, for this study were ICT personnel from each university to be sampled.

Universities that use ERP systems by the same developer, customized to suit their requirements, were considered in one stratum during analysis. Data analysis focused on those that have ERP systems in place and in use.

3.5.2 Study Sample Size

The study sample size was from a target population of forty-nine(49) chartered universities in Kenya. The universities are categorized into public and private respectively, as listed in Appendix 1. Slovin's formula was applied to compute the sample size as shown below;

$$n = \frac{N}{(1 + Ne^2)}$$

Where:

n = Number of samples

N = Total population

e = error tolerance level

Public Universities: $n=31/(1+31(0.21)^2) = 13$

Private Universities: $n=18/(1+18(0.25)^2) = 8$

The sample size was a total of twenty-one (21) universities; thirteen (13) public and eight (8) private universities were selected for the study using stratified and random sampling, which were as follows:

Public Universities

1. Chuka University
2. Dedan Kimathi University of Technology
3. Egerton University
4. Karatina University
5. Kibabii University
6. Laikipia University

7. Maasai Mara University
8. Meru University of Science and Technology
9. Muranga University of Technology
10. Pwani University
11. University of Embu
12. University of Eldoret
13. University of Nairobi

Private Universities

1. Africa Nazarene University
2. Kabarak University
3. KCA University
4. Kenya Highlands University
5. Kenya Methodist University
6. Mount Kenya University
7. St. Paul's University
8. Strathmore University

The research topic was on a technical aspect and was, therefore, best addressed by Information Communication and Technology (ICT) Departments/ Directorates staff. The targeted participants were ICT personnel because they understand ERP systems authentication methods, vulnerabilities, infrastructure and technology and were best suited to provide the information required for this study. The actual number of participants was one person per ICT Department of the respective institution since the same ERP system

was in use. Therefore, the sample size for this study was twenty-one(21) ICT personnel carrying out ERP systems administration roles in the sampled universities.

3.6 Data Collection

3.6.1 Data Collection Instruments

To achieve the objectives of the study, the following instruments were used to collect data:

Document Analysis/Desk review was used to collect theoretical information, already existing, documented data, the literature on ERP systems authentication methods, their vulnerabilities and proposed improvements. The documents that were analyzed or reviewed included; technical reports, papers, journals, books and publications. This data was used to guide the development of the questionnaire and the development of the prototype.

Questionnaires consisting of several questions on ERP authentication methods and related vulnerabilities were designed, tested and administered online through sharing or emailing the online questionnaire link to collect the data. Respondents were assured of confidentiality for their feedback.

3.6.2 Pilot Testing of Research Instruments

The data collection began by designing the questionnaire. Appendix 2 shows the questionnaire used for this research. The sample size for a pilot study should be at least 10% of the sample size to be used in the study (William et al., 2013). Therefore, the pilot sample size was 10% of the study's sample size. The questionnaire was reviewed by conducting a pre-study with a sample of three(3) representative universities before conducting the actual survey. This was issued well in advance before the actual data

collection and contained sample questions of the data to be collected. It was filled by the pre-study sample and collected data evaluated to assess whether it met the objectives of the study. A few gaps were identified from the pre-study and improvements were made to the questionnaire to ensure it captured the data required for this study while ensuring data reliability and validity.

3.6.3 Instrument Reliability

Instrument reliability was tested through pilot testing as outlined in section 3.6.2. The pre-study results were organized, coded in Microsoft Excel, entered in Statistical Package for Social Science (SPSS) and the Cronbach's alpha correlation coefficient computed to measure the reliability of the data collected using the questionnaire. This was done by correlating the scores of various variables in the questionnaire. The computation yielded a correlation coefficient of 0.745 as shown in Table 3.1 below and appendix 4, according to this score the instrument was deemed reliable.

Table 3.1: Reliability Statistics

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of items
.745	.576	11

3.6.4 Instrument Validity

The instrument validity was tested by conducting pilot testing as outlined in section 3.6.2 to ensure the questionnaire for the survey captured the expected data. It assessed if the questions were well understood, well interpreted by all participants and captured expected data. The pre-study addressed the objectives of the study adequately and

answered the research questions. The objectives and research questions, therefore, remained the same for this study. The pre-study also captured the variables of the study as identified in the conceptual framework, which were well factored in the data collected and analyzed, they therefore remained the same for the main study.

The validity of the questionnaire was also achieved by peer debriefing and scrutiny by supervisors. During the pre-study, improvements of the survey questions were made by including additional questions to assess the need for improving the current ERP systems authentication method.

3.6.5 Data Collection Procedures

The data was collected through a survey using a questionnaire designed in Google forms, whose link was shared with the participants to fill online and their responses captured in a file downloadable in Microsoft Excel format.

3.7 Data Processing and Analysis

The collected data was analyzed using the Microsoft Excel analysis tools and Statistical Package for Social Science (SPSS) package. Descriptive statistics and correlation analysis was used to analyze the data and the findings presented using tables and charts. The findings informed the development of the multi-factor authentication prototype. Table 3.2 summarizes the data analysis techniques per objective.

Table 3.2: Summary of Data Analysis Techniques

Objective	Independent Variable	Dependent Variable	Statistical Tests
1. To identify ERP systems authentication methods for Kenyan Universities.	System Authentication <ul style="list-style-type: none"> • Authentication mechanisms • Infrastructure • InfoSec Policies 	Improved ERP System Security – attack tolerance	Percentages, mean,
2. To establish vulnerabilities of existing ERP systems authentication methods for Kenyan Universities.	System Authentication <ul style="list-style-type: none"> • Vulnerabilities • Authentication mechanisms • Infrastructure • InfoSec Policies • User Training 	Improved ERP System Security - confidentiality, usability, availability and attack tolerance	Frequencies, mean, median, standard deviation
3. To develop a multi-factor authentication framework prototype for improving ERP system security.	System Authentication <ul style="list-style-type: none"> • Vulnerabilities • Authentication mechanisms • Infrastructure • InfoSec Policies • User Training 	Improved ERP System Security – confidentiality, integrity, usability, availability and attack tolerance	Correlation analysis
4. To validate the developed multi-factor authentication prototype for effectiveness in improving ERP system security.	System Authentication <ul style="list-style-type: none"> • Vulnerabilities • Authentication mechanisms • Infrastructure • InfoSec Policies 	Improved ERP System Security – confidentiality, integrity, usability, availability and attack tolerance	Regression analysis

Data collected from the survey and document analysis was used as the basis on which a multi-factor authentication prototype for improved security of ERP systems was developed. Pearson Correlation was computed from the data collected to determine the dependent and independent variables relationship, so as to develop the prototype based on

significant variable factors. A multiple linear regression model was applied to show the dependence between the variables of the study and to identify the key variables in the prototype development. This model was fit between the dependent variable, improved ERP system security and the independent variable, system authentication. The regression equation was as follows:

$$Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \beta_6X_6 + \beta_7X_7 + e$$

Where Y is the dependent variable (improved ERP security), β_0 is the constant, $\beta_1 - \beta_7$ are the regression coefficients, X is the independent variable factors below and e is the error term.

X_1 = Adequacy of Security (Vulnerabilities)

X_2 = Authentication Type

X_3 = Infrastructure Present

X_4 = ICT Policy Adequacy

X_5 = Attack Tolerance

X_6 = Authentication Improvement

X_7 = Level of User Training

Prototyping

A prototype is an early version of software that demonstrates concepts, designs and can be used to find out more about the problem and possible solutions. Prototypes are useful in modelling or simulation of proposed systems (Sommerville, 2016). Rapid prototyping was used in this study to meet the objectives of developing and validating a multi-factor authentication prototype for improved ERP security for Kenyan Universities.

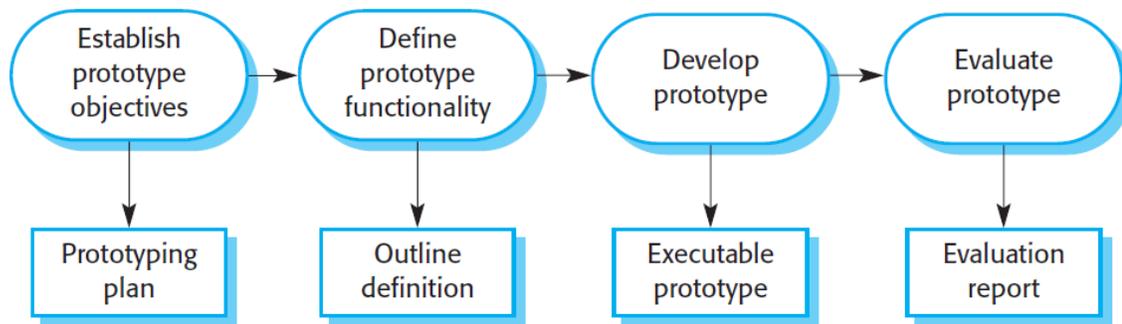


Figure 3.1: Process Models for Prototyping

Source: (Sommerville, 2016)

The prototyping involved the following steps:

1. Establish objectives of the prototype

This step involved coming up with a prototyping plan detailing the objectives of developing the prototype. The main objective was to develop and validate a multi-factor authentication prototype for improved ERP systems security in Kenyan Universities. This was done by:

- a) Developing a user interface for registering/enrolling and managing users.
- b) Developing a user interface to authenticate users using multi-factor authentication.
- c) Developing a user interface that logs the outcome of the authentication process.
- d) Testing the prototype.

2. Define Prototype functionality

This involved describing the required prototype functionality. These are categorized into functional and non-functional requirements.

Functional Requirements – the services and features the system should provide given specific inputs and scenarios. It is based on the function the system is intended to deliver.

It describes the system functions, inputs, outputs and exceptions.

The functional requirements for this prototype were:

- i. User enrollment/ registration – the system provides a means by which users are registered and prove their identity using authentication attributes to access system resources. Systems must be able to register users.
- ii. User Authentication and lifecycle management – the system provides mechanisms to verify users' identity, that they are indeed who they claim to be through the provision of valid authentication credentials. It assures users' identities for them to access system resources. The system must be able to identify users from their unique user identity, verify their matching password and biometrics to grant them system access or otherwise deny them system access.
- iii. Activity logs - the system shall provide records of the authentication process outcome through user log-in logs.

Non-functional requirements – refer to requirements that are indirectly concerned with the explicit function or services of the system, but are expected general characteristics as a whole. The non-functional requirements of this prototype were:

- i. Usability – user-friendly and ease of use.
- ii. Security – systems ensure security against most vulnerabilities. This is provided for by authentication method settings, encryption of passwords stored in the database and user biometrics.
- iii. Confidentiality of user credentials. It was provided by enforcing secure password policy requirements and matching users' fingerprints.
- iv. Availability and reliability for users.
- v. Response time – responds in a reasonable amount of time.

- vi. Accuracy, allowing only authorized users access.
 - vii. Scalable - allows for expansion, changes and further customization.
 - viii. Display appropriate information and error messages to users.
 - ix. Validation, error and exception handling.
3. Develop prototype – executable prototype

This step involved the development of an executable prototype using the following tools:

- Hardware: Computer Intel core i5, Digital Persona Biometric Reader, technical specifications are shown in Appendix 5.
- Operating system: Windows 10
- Software Development Tools: FlexCode SDK, CodeIgnitor
- Relational Database: MySQL
- Web server: Apache
- Programming Languages: PHP

System Process Modelling

This is the process of developing representative models of a system, with each presenting different views and perspectives.

Process Flow

1. User is registered by the system administrator, an account created for them, password set and their fingerprints captured.
2. The user accesses the system and lands on the log-in page. They log in by submitting the correct username and password. Once username and password are successfully authenticated, the user enters their fingerprint for the final authentication factor. The system carries out verification, and if successful, the user is granted access to the ERP

dashboard. In case of incorrect credentials, the system gives an appropriate error message and returns the user to the login screen. In case of 3 unsuccessful log-in attempts, the system temporarily disables the user and can only be enabled by the systems administrator.

3. The user is authenticated/not authenticated, and the transaction is successful/fails.

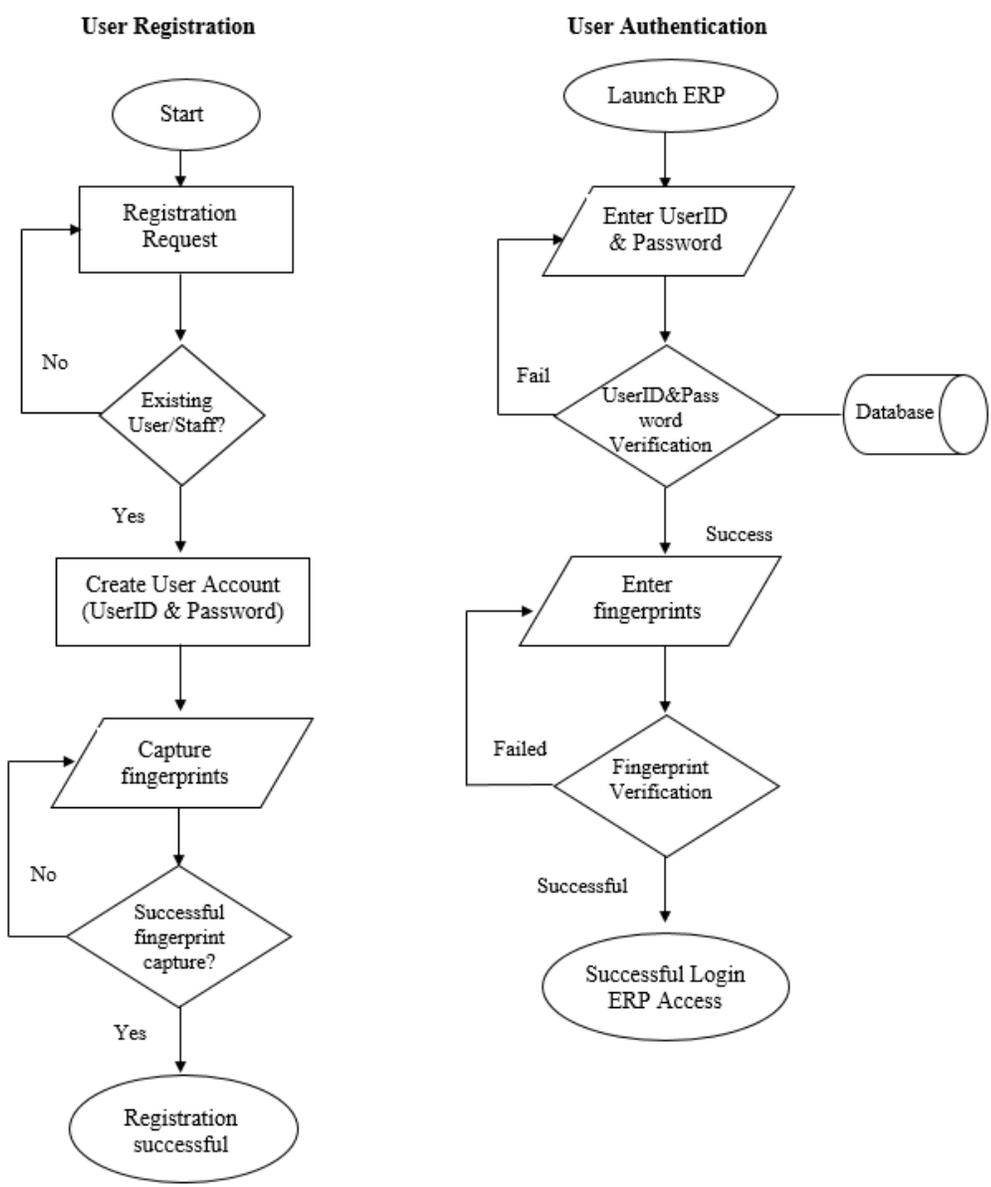


Figure 3.2: System Flow Chart

Source: Author, 2021

Use Case Diagram - It shows the interaction between a system and its environment, which includes users who are referred to as actors.

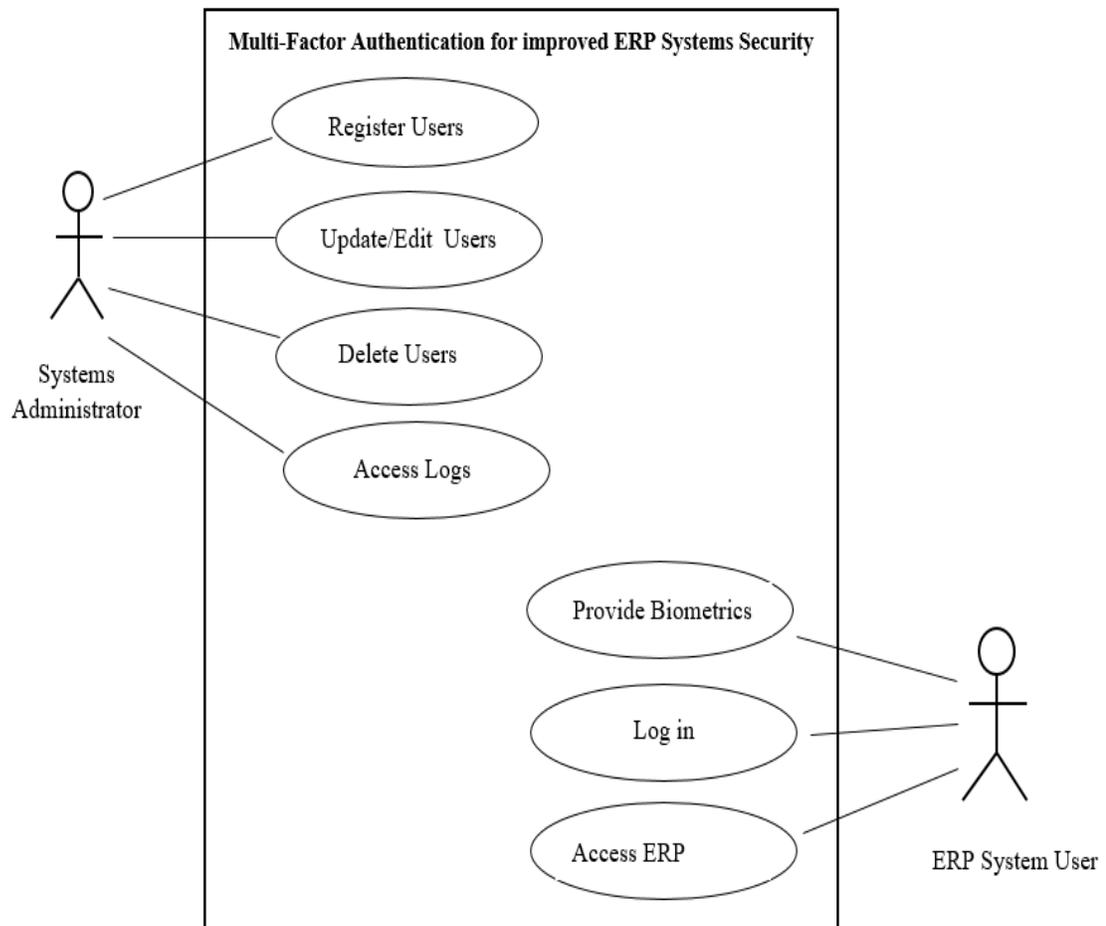


Figure 3.3: Use Case Diagram

Source: Author, 2021

Sequence Diagram – this process modelling diagram shows the interaction between actors and system components.

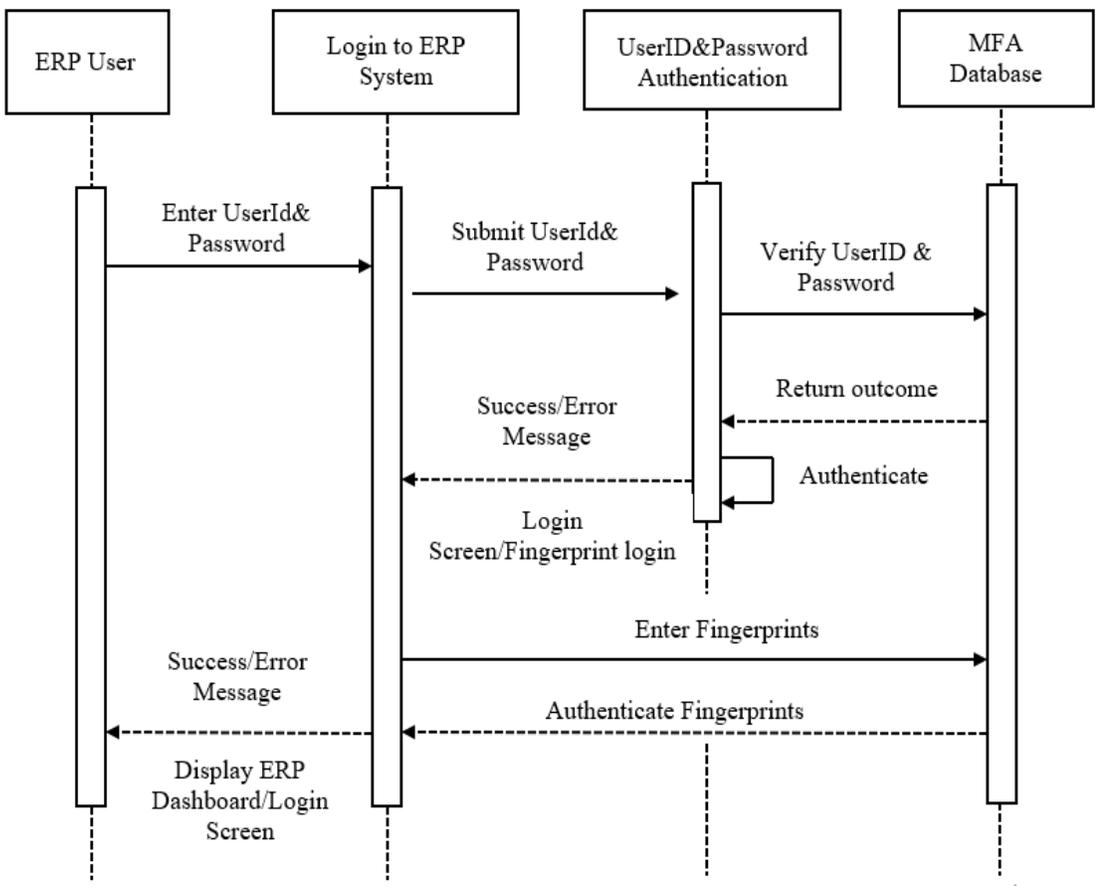


Figure 3.4: Sequence Diagram

Source: Author, 2021

Database Schema – shows the database tables and structure.

The image shows a screenshot of a database schema with three tables:

- mfa_db mfa_user**:
 - user_id : int(11) unsigned
 - user_name : varchar(50)
 - user_fname : varchar(255)
 - user_lname : varchar(255)
 - user_email : varchar(255)
 - user_tel : varchar(15)
 - user_empno : int(10)
 - user_role : varchar(255)
 - user_pass : text
 - user_status : tinyint(1)
 - user_auth : varchar(20)
 - plain_pass : text
 - user_logincodeexpiry : datetime
 - user_smscode : int(6)
 - user_loginurl : varchar(255)
 - user_trials : int(2)
- mfa_db mfa_finger**:
 - user_id : int(11) unsigned
 - finger_id : int(11) unsigned
 - finger_data : text
- mfa_db mfa_log**:
 - log_id : int(11)
 - log_time : timestamp
 - user_empno : varchar(50)
 - data : text
 - ip : varchar(30)

Figure 3.3: Database Schema:

Source: Author, 2021

After the prototype was developed, it was tested against its functionalities, some of the identified vulnerabilities and the dependent variable factors for improved ERP system security. This was done by carrying out functional testing.

3.8 Legal and Ethical Considerations

The data collection questionnaires for this research included a section with all the information the participants needed to know about the study and allowed participants to voluntarily consent to participate in the research. The research was on systems security which is a sensitive topic that requires high levels of confidentiality and ethics. Thus, participants were informed that their data remains confidential and allowed for responses that do not have personally-identifying information.

A National Commission for Science, Technology and Innovation (NACOSTI) research permit was sought, as a legal research authorization document. This is as shown in Appendix 3.

3.9 Chapter Summary

This chapter detailed the methodology, approaches and techniques used to achieve the objectives of this study.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter presents the analysis of the collected data and a summary of the findings based on the study's objectives. Data analysis refers to operations performed on collected data to summarize and organize it so that it addresses set out objectives. It involves the computation of specific measures and searching for patterns of relationship in a group of data (Cresswell, 2018). This chapter presents the general demographic information and characteristics of the respondents. The study had the following four objectives: to identify ERP systems authentication methods for Kenyan Universities, to establish vulnerabilities of existing ERP systems authentication methods for Kenyan Universities, to develop and validate a multi-factor authentication prototype for improving ERP systems security in Kenyan Universities.

The data was collected for twenty-one universities in Kenya, which was the sample size of the study. Three universities were involved in the pre-study, namely; Chuka, Laikipia and Kabarak University. The three universities were not included in the final data collection, since their data had already been collected. ICT personnel carrying out systems administration-related roles in the twenty-one universities participated in the survey. The data was collected using a questionnaire designed in Google forms, whose link was shared with the participants to fill online and the responses captured in a file downloadable in Microsoft Excel format. Analysis was carried out using Microsoft Excel and SPSS analysis tools. The analyzed data is presented using charts, graphs and tables.

The targeted number of respondents was twenty-one ICT staff in the sampled universities. A total of nineteen participants (13 public and 6 private universities) filled in the questionnaire, while two were non-responsive, resulting in a response rate of 90%.

4.2 Characteristics of the Respondents

This section analyzes the demographics of the respondents, which were captured by collecting general information about the respondents, that is, age, role in the ICT Department, years of experience in systems administration roles and education level. The demographic information shows the respondents' appropriateness to provide the data that was required for this study. This data was collected and analyzed as follows:

Age Bracket

The study collected data on the respondents' age brackets to gain an understanding of the age brackets of the staff who are involved in ERP systems security. The findings are as shown in Fig 4.1.

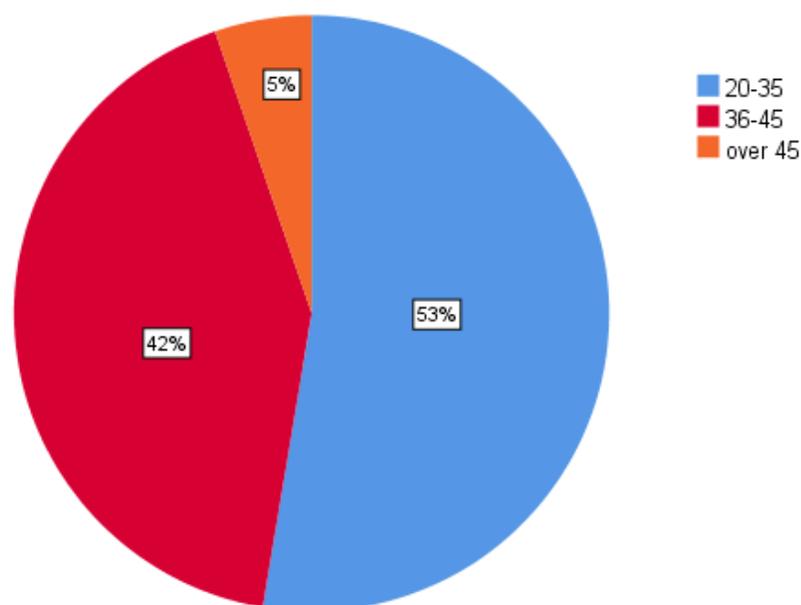


Figure 4.1: Age Bracket of the Respondents

Fig 4.1 shows that the respondents' age bracket was 53% in the 20 – 35 years age bracket, 42% in the 36-45 years age bracket and 5% were over 45 years. The findings revealed that the majority of the respondents, representing ICT Systems Administrators in Kenyan Universities, were in the 20-35 years age bracket.

Respondents role in ICT Department

The study sought to identify the respondents' role in the ICT Department. The findings are as shown in Fig 4.2.

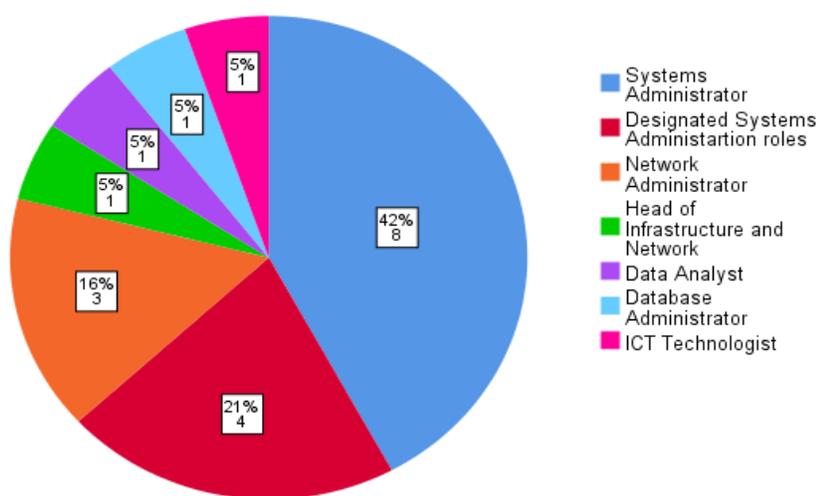


Figure 4.2: Respondents Role in ICT Department

The findings revealed that the respondents' roles in their ICT Departments were 42% Systems Administrators, 21% Designated System Administration Roles, 37% in other roles of; Network Administrator, Head of Infrastructure and Network, Database Administrator, Data Analyst and ICT Technologist. This revealed that the respondents were in roles related to ERP authentication and therefore had an adequate understanding of ERP authentication and systems security. This showed that they were suitable candidates for providing reliable information for this study.

Years of Experience in Systems Administration Roles

The respondents were asked to specify their years of experience in systems administration roles. Fig. 4.3 below shows the findings.

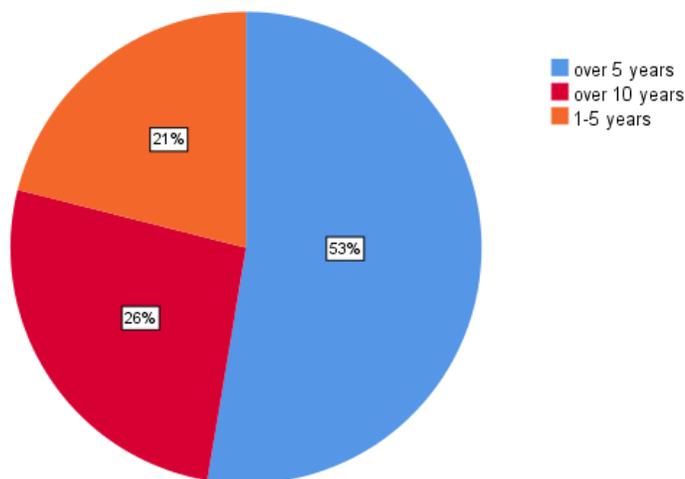


Figure 4.3: Years of Experience in Systems Administration Roles

The study findings revealed that the respondents' years of experience in systems administration-related roles was a majority of 53 % with over 5 years, 26% with over 10 years and 21% with 1-5 years. This implied the respondents had adequate work experience in systems administration roles required for the data collected in this study.

Education Level of Respondents

The study also required respondents to provide their education level. The findings are shown in Fig. 4.4.

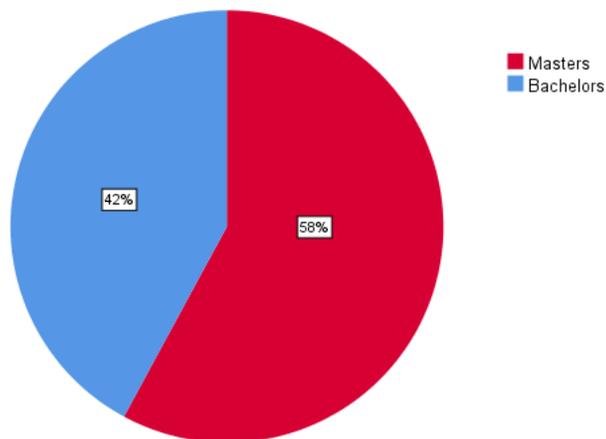


Figure 4.4: Education Level of the Respondents

According to the data collected and analyzed in Fig 4.4, the highest education level of the respondents was 58% Master's degree and 42 % Bachelor's degree, indicating that majority of the Universities ICT staff have at least a Bachelor's degree, were qualified and therefore had an understanding of ERP systems authentication security.

4.3 Analysis, Findings and Interpretation

The first objective of the study was to identify current authentication methods used for ERPs in Kenyan universities. All the universities in this study had ERP systems, which have been in use for an average period of 6 years, therefore, providing adequate data for this study. The ERP systems in use were Microsoft Navision, ABN Unisol, Sage Accpac, and others used multiple systems as shown in Fig. 4.5. Microsoft Navision and ABN Unisol were at the top with the rest featuring at an equal level of 5% usage.

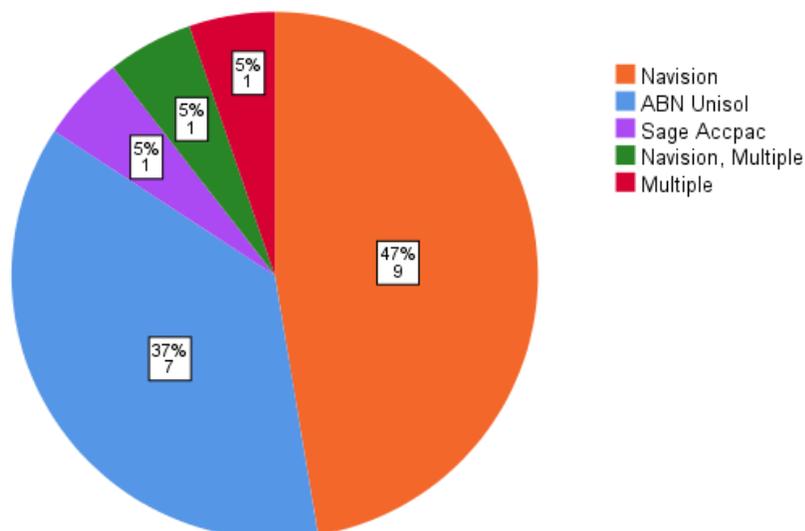


Figure 4.5: ERPs used in Kenyan Universities

4.3.1 Authentication Methods used in ERP Systems for Kenyan Universities

The study sought to identify the ERP systems authentication methods used for Kenyan Universities. The findings revealed that a majority, of 58% of the sampled universities

currently use passwords only, 26% passwords with email verification, 5% passwords with Windows Domain Authentication, 5% biometrics that was card-based and 5% passwords with optional biometrics, for ERP system authentication as shown in Fig. 4.6 below:

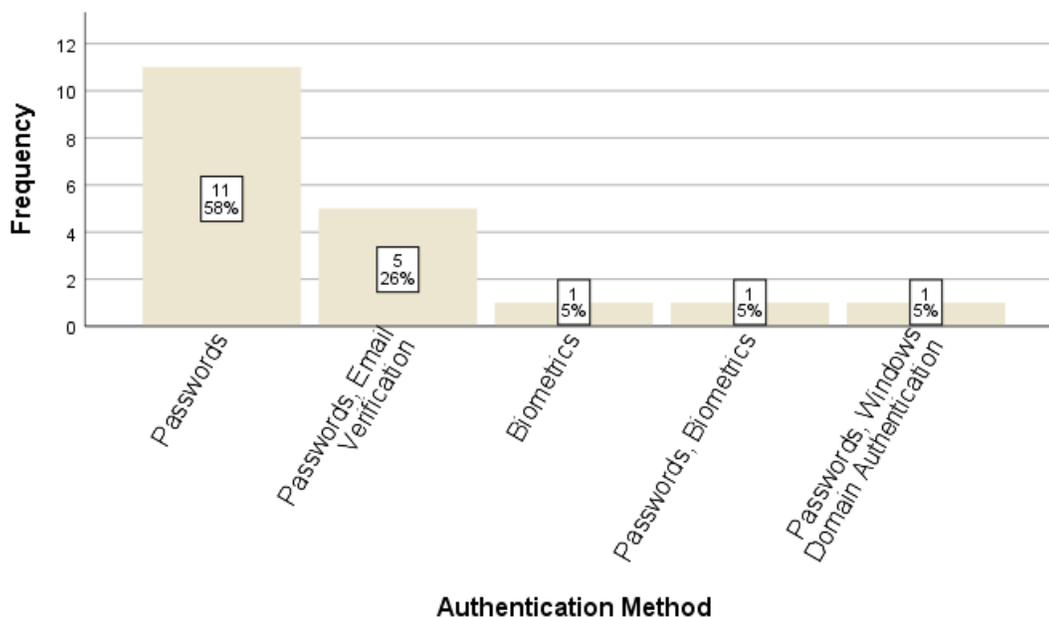


Figure 4.6: Current ERP Authentication Methods

The Universities using passwords with optional biometrics authentication methods had set use of biometrics authentication mostly at the transaction approval level. This authentication method used either passwords or biometrics authentication, only one at a time and not a combination of both.

The study further sought to understand whether the authentication method in use was considered to offer adequate security. The respondents were requested to give a rating for the adequacy and security of the authentication method. This was done through a Likert scale going from 1 (Very Weak) to 5 (Very Strong). The findings were as shown in Table 4.1:

Table 4.1: Current ERP Authentication Method Adequacy and Security Rating

Authentication Method	Mean	Standard Deviation
Adequacy for ERP Security	3.79	0.787
Security Rating	3.74	0.653

The findings revealed that the current authentication method was considered moderate in offering adequate security and was rated to offer neutral security for their ERP systems.

The study further required respondents to rate the authentication method based on security attributes. The findings were as shown in Table 4.2

Table 4.2: Security Attributes of Current ERP Authentication Methods

Security Attribute	Very High	High	Moderate	Weak	Very Weak	Mean	Standard Deviation
Ease of Use	9	9	1	0	0	4.42	0.607
Confidentiality	2	8	8	1	0	3.58	0.769
Integrity	3	6	9	1	0	3.58	0.838
Availability	9	7	3	0	0	4.32	0.749
Attack Tolerance	1	8	7	1	1	3.32	0.946

System security attributes in Table 4.2, as identified in the conceptual framework, were assessed using a Likert scale to determine the strength of the current authentication method of passwords. The Likert scale was denoted as follows; 5 = Very Strong, 4 = Strong, 3 = Moderate, 2 = Weak and 1 = Very Weak. From the findings in Table 4.2, the authentication methods were considered strong in ease of use and availability, at a mean of

4.42 and 4.32 respectively. They were, however, rated moderate in confidentiality (3.58 mean), integrity (3.58 mean) and attack tolerance (3.32 mean).

The study also required respondents to answer whether there was a need to improve the current authentication method. The respondents all agreed on a need for improving the current authentication method for ERP security, as shown in Fig 4.7 below:

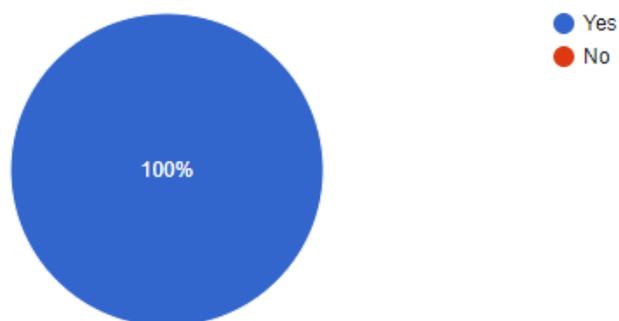


Figure 4.7: Need for Improving Current Authentication Method

4.3.2 Vulnerabilities of existing ERP systems' authentication methods for Kenyan Universities

The second objective of the study was to establish vulnerabilities of existing ERP systems authentication methods for Kenyan Universities. Vulnerability, in this case, refers to gaps or weaknesses of IT security controls that can be exploited by threat agents resulting in harm or loss. The study sought to identify the vulnerabilities and if there were cases of compromised ERP user accounts. The findings were as shown in Fig. 4.8.

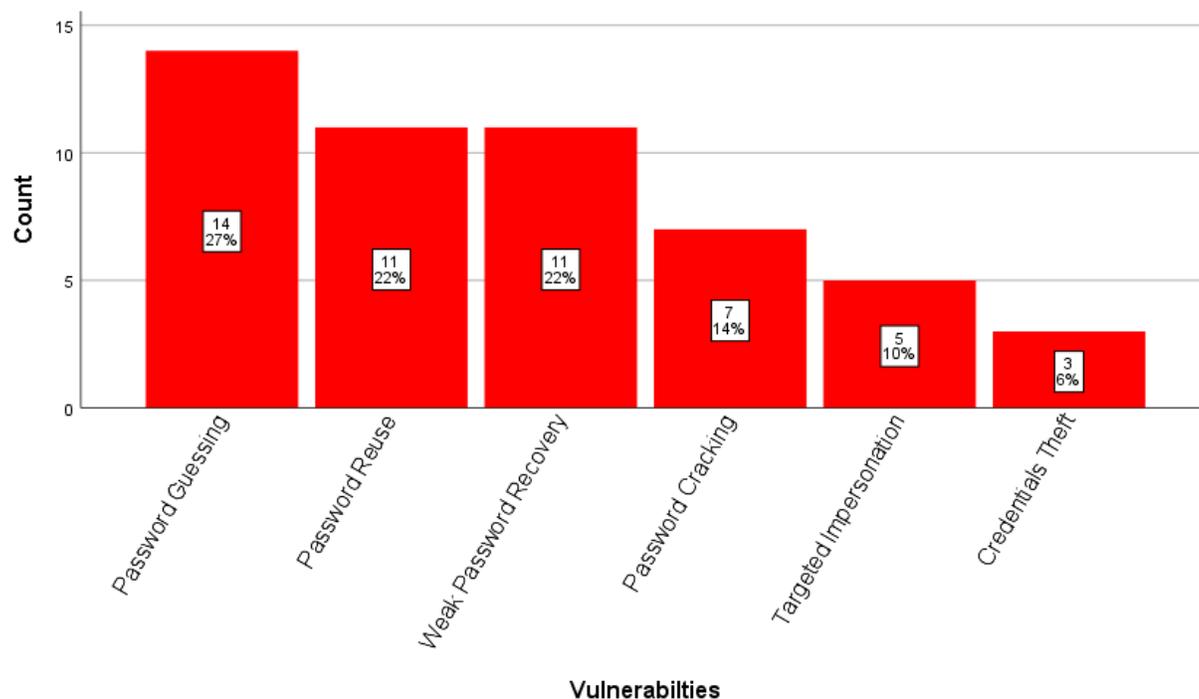


Figure 4.8: Vulnerabilities of Current Authentication Methods

The findings revealed that the responses captured included both vulnerabilities and attacks. These were therefore analyzed separately in two categories; vulnerabilities and possible attacks to the vulnerabilities of the current authentication methods. The vulnerabilities of the current authentication methods were identified as; password guessing, password reuse, weak password recovery, password cracking, targeted impersonation and credentials theft, as shown in Fig. 4.8.

Other vulnerabilities include password complexity, password encryption, default credentials, password masking, hardcoded passwords and code recompilation. These should be addressed by having control measures in place for the systems.

These vulnerabilities in the current systems authentication methods may be exploited through various attacks resulting in loss or harm. Attacks are potential incidents

that may cause unauthorized access or transactions. These attacks included; social engineering, malware, brute force attacks, denial of service attacks and replay attacks, as summarized in Fig. 4.9. These vulnerabilities and attacks were comparable to those identified by Njoroge et al., (2019) in a study on information security risks facing Kenyan public universities. The respondents indicated that there might have been ERP user accounts authentication compromises in the last three years.

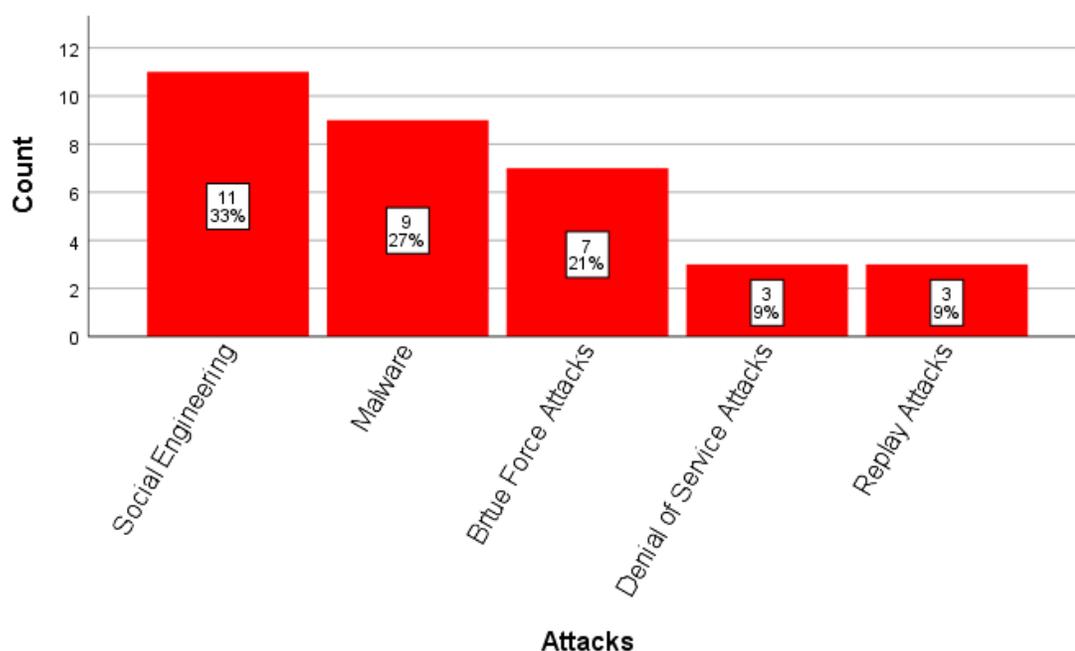


Figure 4.9: Possible Attacks to the Current Authentication Methods Vulnerabilities

Other attacks that may face authentication methods include; Data Language Libraries(DLL) hijacking, SQL injections and man-in-the-middle attacks.

4.3.3 A Multi-Factor Authentication Framework Prototype

Objective 3 was to develop a multi-factor authentication framework prototype for improving ERP system security. To achieve this objective, the study collected data on the

independent variables for secure system authentication, which were covered as follows: availability of infrastructure, infrastructure openness to integration, ICT Security policy existence, ICT Security policy effectiveness on secure system authentication and user training on ERP authentication security. The findings for these independent variables for secure ERP authentication are discussed below.

Study findings established that universities have the infrastructure to support improved ERP system authentication, as shown in Fig 4.10. Infrastructure available was as follows: Email (18), Biometrics (10) and SMS (10). They indicated that the infrastructure could be open to integration with their institutional ERP systems.

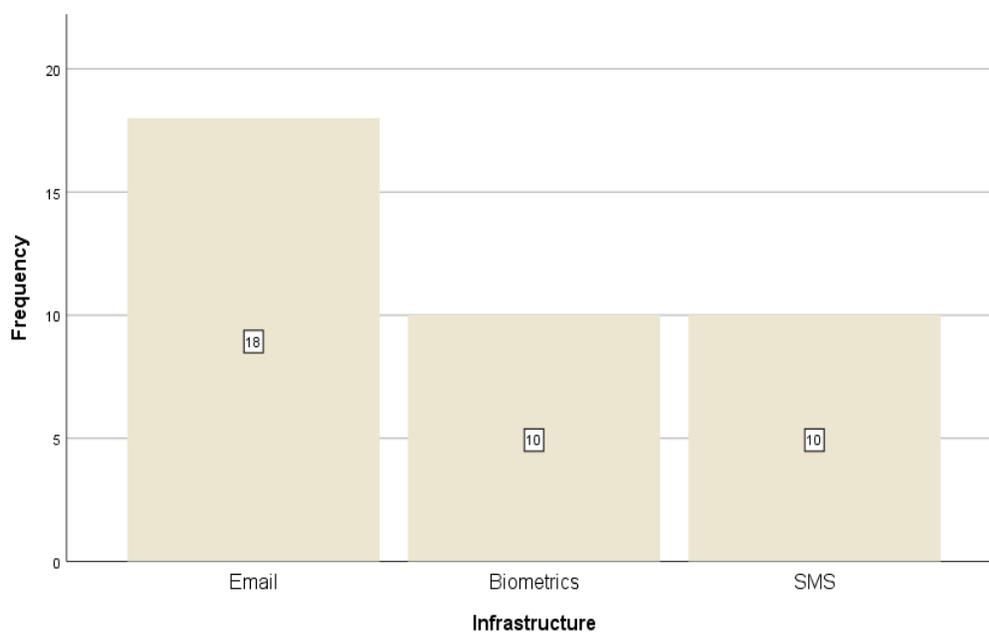


Figure 4.10: Infrastructure Available to support improved ERP Systems Security

Respondents were asked to provide data on whether they have ICT Security Policies in place, the ICT Security policy effectiveness on secure system authentication and the level

of user training on ERP authentication security. The findings were as summarized in Table 4.3.

Table 4.3: ICT Policy Effectiveness and Level of User Training

Authentication Method	Mean	Standard Deviation
ICT Policy Adequacy	3.42	0.507
Level of User Training	3.63	0.684

The majority of the universities (95%) in this study had ICT Security Policies, which offered guidance on secure authentication and privacy policies. These findings concurred with Njoroge et al., (2019), who established that security is a vital requirement for universities, and the majority have implemented Information Security Policies. The effectiveness of the ICT Security Policy on secure systems authentication was rated as moderate using the Likert scale provided in the questionnaire where 5 = Very Strong, 4 = Strong, 3 = Moderate, 2 = Weak and 1 = Very Weak. User training on ERP Secure Authentication was conducted 50% once during system implementation and 50% often. The level of user training on secure ERP Authentication was scored as moderate using a Likert scale as summarized in Table 4.3. This differed slightly with Bett, (2018), who found that universities carry out user training and information security awareness but were not as effective, hence it was identified as a hurdle facing the implementation of ERP systems in Kenya.

The study finally sought to find out how ERP systems security can be improved in line with Mayieka, (2019), who recommended that institutions of higher learning take a proactive approach to minimize cyber security challenges. The respondents suggested the following measures in Fig. 4.11.

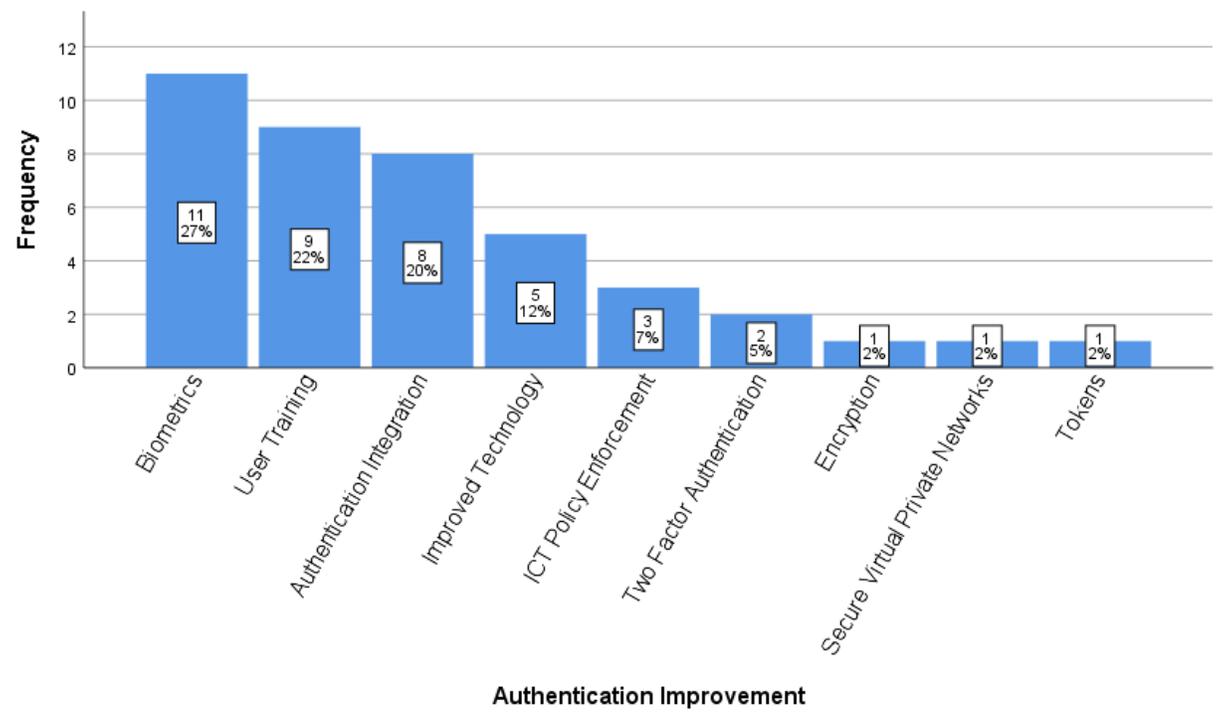


Figure 4.11: Authentication Improvement

Correlation

Pearson Correlation was computed to establish the relationship between the dependent and independent variables. There was a strong positive relationship between ERP system security and vulnerabilities (attack tolerance) of $r=.681$, $p=0.001$, ICT Policy adequacy at $r=0.521$ and $p=0.022$, and level of user training at $r=0.890$ with a p-value of 0.000 as shown in the table below. The prototype framework therefore, factored in attack tolerance, level of user training and ICT policy components such as password management and user identity to ensure ERP systems authentication security.

Table 4.4: Correlations

Variable		Security Rating	Adequacy of Security	Authentication Type	Infrastructure Present	ICT Policy Adequacy	Attack Tolerance	Level of User Training
Security Rating	Pearson Correlation	1	.426	.308	.330	.521*	.681**	.890**
	Sig (2-tailed)		0.69	.200	.168	.022	.001	.000
	N	19	19	19	19	19	19	19
Adequacy of Security	Pearson Correlation	.426	1	.372	-.021	-.373	.542*	.467*
	Sig (2-tailed)	0.69		.117	.932	.115	.017	.044
	N	19	19	19	19	19	19	19
Authentication Type	Pearson Correlation	.308	.372	1	.271	.147	.184	.301
	Sig (2-tailed)	.200	.117		.261	.548	.451	.210
	N	19	19	19	19	19	19	19
Infrastructure Present	Pearson Correlation	.330	-.021	.217	1	.221	.026	.303
	Sig (2-tailed)	.168	.932	.261		.364	.915	.207
	N	19	19	19	19	19	19	19
ICT Policy Adequacy	Pearson Correlation	.521**	.373	.147	.221	1	.518*	.632**
	Sig (2-tailed)	.022	.115	.548	.364		.023	.004
	N	19	19	19	19	19	19	19
Attack Tolerance	Pearson Correlation	.681**	.542*	.184	.026	.518*	1	.705**
	Sig (2-tailed)	.001	.017	.451	.915	.023		.001
	N	19	19	19	19	19	19	19
Level of User Training	Pearson Correlation	.890**	.467*	.301	.303	.632**	.705**	1
	Sig (2-tailed)	.000	.044	.210	.207	.004	.001	
	N	19	19	19	19	19	19	19

** . Correlation is significant at the level of the 0.01 level (2-tailed).

* . Correlation is significant at the level of the 0.05 level (2-tailed).

Regression Analysis

Regression analysis was conducted using SPSS to establish the relationship between the dependent variable ERP security and the independent variables; Level of user training, ICT Policy adequacy, authentication type, infrastructure present, authentication improvement, adequacy of security and attack tolerance. The regression analysis model yielded an R square value of .817 at a significance of $F(7,11) = .894, p=0.03$, which shows a good fit to the model. This implies that the independent variables, particularly the level of user training, have a significant effect on the dependent variable, as shown in the coefficients table below.

Table 4.5: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.904 ^a	.817	.701	.357

- a. Predictors: (Constant), Level of User Training, ICT Policy Adequacy, AuthenticationType, InfrastructurePresent, AuthImprove, Adequacy of Security, Attack Tolerance

Table 4.6: Analysis of Variance (ANOVA)

Model		Sum of Squares	df	Mean Square	F	Sig
1	Regression	6.259	7	.894	6.903	.003 ^b
	Residual	1.425	11	.130		
	Total	7.684	18			

- b. Dependent Variable: Security Rating
 c. Predictors: (Constant), Level of User Training, ICT Policy Adequacy, AuthenticationType, InfrastructurePresent, AuthImprove, Attack Tolerance, Adequacy of Security

Table 4.7: Coefficients

Model	Unstanda rdized B	Coefficients Std. Error	Standard ized Coeffici ents Beta	t	Sig
1 (Constant)	.126	1.632		.077	.940
Adequacy of Security	-0.70	.172	-.084	-.407	.692
AuthenticationType	.166	.251	.128	.662	.521
InfrastructurePresent	.113	.173	.122	.652	.528
ICT Policy Adequacy	-.069	.157	-.071	-.441	.668
Attack Tolerance	.066	.157	.095	.417	.685
AuthImprove	.010	.207	.009	.047	.963
Level of UserTraining	.768	.201	.804	3.829	.003

a. Dependent Variable: Security Rating

In the regression model, the coefficients of the independent variables show that Authentication type, infrastructure present, attack tolerance, and authentication improvement had positive beta coefficients and therefore have a positive effect on ERP security. The results show that the level of user training contributed most significantly to the model (B = .768, $p < .003$) having the highest beta coefficient. Adequacy of security and ICT Policy adequacy, which had positive correlation coefficients but resulted in negative beta coefficients, which could be as a result of suppression by the other independent variables. The final predictive model using the forward variable selection regression technique shows the measure of the influence of the variables on the model was as follows:

$$Y = .126 + 0.768 * \text{Level of User Training}$$

This implies that user training has a positive and the highest effect on improved ERP system security.

From the data collected, the biometrics technology available was fingerprint-based and smart-card-based biometrics. The use of biometrics was the leading method to improve ERP security proposed by the respondents, as shown in Fig. 4.11. According to First Identity Online Alliance, (2019), fingerprint scanning was the most desired authentication feature among consumers. Fingerprint biometrics has the advantages of providing high-security assurance, usability, privacy, non-transferability and are difficult to circumvent.

The multi-factor authentication prototype will therefore use a combination of passwords and fingerprint-based biometrics to improve ERP systems security for Universities in Kenya. Security, usability, reliability and cost were the criteria applied in this study for comparison and selection. This authentication method has been selected based on authentication mechanisms evaluation, infrastructure available to improve ERP systems security, as shown in Fig 4.10, where most universities had biometrics in place.

The proposed multi-factor authentication framework prototype for improved ERP systems security, therefore, is as shown in Fig. 4.12:

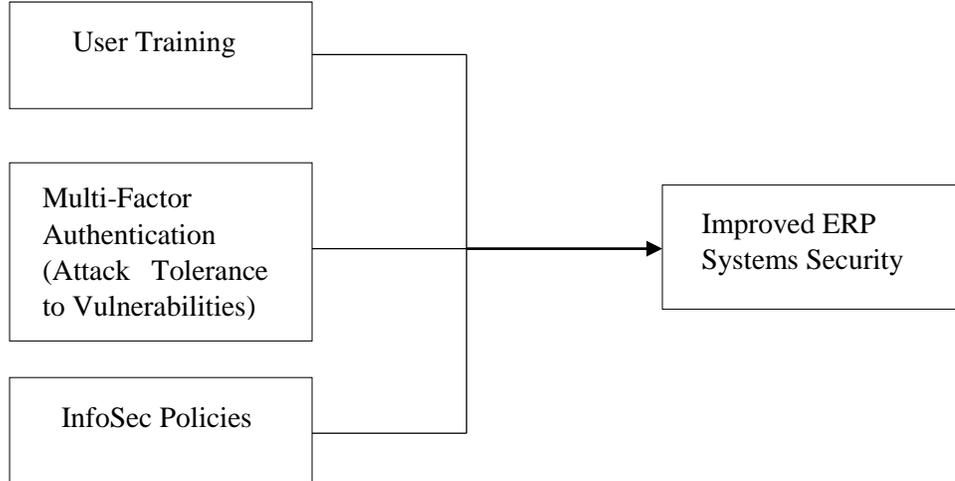


Figure 4.12: Proposed Multi-Factor Authentication Framework Prototype

Source: Author, 2021

Multi-Factor Authentication Prototype User Interface

The prototype was developed and the user interface is as shown in the prototype screenshots in Appendix 6.

4.3.4 Validation of the Multi-Factor Authentication Framework Prototype

Validation is done after an application is developed to ensure it functions as expected while meeting the requirements. The multi-factor authentication prototype was tested by use of test cases and through peer review. Testing was done continuously during the development process as well as after completion which involved unit testing, integration testing and system testing. Test cases were designed to validate the prototype as follows:

Table 4.8: Test Cases

Test Case ID	Test Scenario	Test Steps	Expected Results	Actual Results	Pass/Fail
1	Creating New User with valid data	<ol style="list-style-type: none"> 1. System Administrator Logs in 2. Click on Create New User 3. Enter all Valid Details 4. Capture Fingerprints 5. Submit 	New User Successfully added	As expected	Pass
2	User Login with valid data(userid, password and fingerprint)	<ol style="list-style-type: none"> 1. Open log in page 2. Enter UserID and password 3. Click submit 4. Correctly verified 5. Enter fingerprint 6. Submit 	User is logged in to the ERP system	As expected	Pass
3	User Login with invalid data	<ol style="list-style-type: none"> 1. Open log in page 2. Enter UserID and password 3. Click submit 4. Not verified 	User not logged in	As expected	Pass
5	Required/Compulsory fields	<ol style="list-style-type: none"> 1. Open log in page 2. Enter details leaving out any required field 	Error Message	As expected	Pass
6	Password strength	<ol style="list-style-type: none"> 1. Enter weak password 	Error Message	As expected	Pass
7	User Logs	<ol style="list-style-type: none"> 1. System Administrator Logs in 2. Click on Logs 	Error Message	As expected	Pass

Validation screenshots are shown in Appendix 6.

4.4 Chapter Summary

This chapter summarized the data analysis and findings of the current ERP authentication methods in use for Kenyan Universities and their vulnerabilities. Based on the findings, a multi-factor authentication prototype was developed and validated to improve ERP systems security for the universities.

CHAPTER FIVE

DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This final chapter summarizes the purpose of the research, the discussions, summary, conclusions, recommendations and suggestions for further research, based on the objectives of the study.

5.2 Discussion

The purpose of this research was to develop a multi-factor authentication prototype for improved ERP systems security for Universities in Kenya. The study was driven by the following four objectives; identifying ERP systems authentication methods for Kenyan Universities, establishing vulnerabilities of existing ERP systems authentication methods for Kenyan Universities, developing and validating a multi-factor authentication prototype for improving ERP systems security in Kenyan Universities.

Data on current ERP system authentication methods and their vulnerabilities was collected using an online questionnaire, from ICT personnel carrying out systems administration roles in the sampled universities. The collected data was analyzed, and the findings guided the development of the prototype. The outcome per objective is summarized as follows;

5.2.1 ERP Systems Authentication Methods for Kenyan Universities

The study found that the use of passwords is the leading ERP systems authentication method for Kenyan Universities. A majority of 58% of the sampled universities were using passwords only, 26% passwords with email verification, 5% passwords with Windows

Domain Authentication, 5% biometrics that was card-based and 5% passwords with optional biometrics for ERP system authentication.

The universities using passwords with optional biometrics authentication methods had set use of biometrics authentication mostly at the transaction approval level. This authentication method used either passwords or biometrics authentication, only one at a time and not a combination of both.

The respondents all agreed there was a need for improving the current authentication method for ERP security, which concurs with First Identity Online Alliance, (2019).

5.2.2 Vulnerabilities of Existing ERP Systems' Authentication Methods for Kenyan Universities

The study established current authentication methods to be vulnerable to; password guessing, password reuse, weak password recovery, password cracking, targeted impersonation and credentials theft. Other vulnerabilities that may arise include password complexity, password encryption, default credentials, password masking, hardcoded passwords and code recompilation.

These vulnerabilities in the current systems authentication methods may be exploited through various attacks resulting in loss or harm. These attacks included; social engineering, malware, brute force attacks, denial of service attacks and replay attacks. These vulnerabilities and attacks were similar to those identified by Njoroge et al., (2019) in a study on information security risks facing Kenyan public universities. Other attacks that may face authentication methods include; Data Language Libraries (DLL) hijacking, SQL injections and man-in-the-middle attacks.

These vulnerabilities and attacks guided the study on selecting an appropriate multi-factor authentication framework for the prototype to improve ERP systems security.

5.2.3 A Multi-Factor Authentication Framework Prototype

The third objective was to develop a multi-factor authentication framework prototype to improve ERP systems security for Kenyan universities. This was based on the findings of the authentication methods, vulnerabilities and infrastructure from the data collected. The research findings revealed that the majority were using passwords only. Respondents agreed there was a need to improve the ERP authentication.

The majority of the universities (95%) in this study had ICT Policies in place, which offered guidance on secure authentication and privacy policies. These findings concurred with Njoroge et al., (2019), who established that security is a vital requirement for universities and the majority have implemented Information Security Policies. User training on ERP Secure Authentication was conducted 50% once during system implementation and 50% often. The level of user training on secure ERP Authentication was found to be moderate. These findings slightly differed with Bett, (2018), who found that universities carry out user training and information security awareness but were not as effective; hence it was identified as a hurdle facing universities implementing ERP systems in Kenya. Improved ERP security requires user training and improved authentication methods.

The study developed a multi-factor authentication prototype with user registration, authentication and capturing user activity logs functionalities. It has two authentication methods; a combination of username, password and SMS code and a combination of username, password and fingerprint. It consists of two login steps, with the first requiring

username and password, while the second requires identity verification through fingerprint or a randomly generated code sent via SMS to the user registered phone number. Once a user submits login credentials in both steps and if successfully verified, they are granted access to the ERP system. Based on the systems defined user role, standard users can access their respective modules of the ERP and change their password, whereas system administrators can create new, edit, delete users and access user activity logs.

5.2.4 Validation of the developed Multi-Factor Authentication Prototype

The multi-factor authentication prototype was validated through testing and peer review. Testing was done using test cases, unit, functional and system testing where the outcome showed that the prototype was functioning well and improved ERP systems security.

5.3 Summary of the Main Findings

This study was carried out to identify current ERP authentication methods for universities in Kenya and their vulnerabilities, to develop and validate a multi-factor authentication prototype to improve ERP systems security for Kenyan Universities. The findings were as outlined in Table 5.1:

Table 5.1: Summary of Findings

Objective	Findings
1. To identify ERP systems authentication methods for Kenyan Universities.	The majority of the universities (58%) were using passwords only and had a high-security risk. There is a need to enhance this authentication method to improve ERP systems security.
2. To establish vulnerabilities of existing ERP systems authentication methods for Kenyan Universities.	Vulnerabilities were mainly; password guessing, password reuse, weak password recovery, password cracking, targeted impersonation and credentials theft. There are attacks likely to result from the vulnerabilities: social engineering, malware, brute force, denial of service and replay attacks.
3. To develop a multi-factor authentication framework prototype for improving ERP system security.	A Multi-factor authentication prototype using a combination of Password and SMS or Password and Biometrics was developed to improve ERP systems security for Kenyan Universities.
4. To validate the developed multi-factor authentication prototype for effectiveness in improving ERP system security.	The prototype was tested by use of test cases, unit, functional and system testing, which showed it was effective in improving ERP system security.

5.4 Conclusion

Authentication is a crucial area of systems security with risks that should be mitigated. Passwords are the common authentication method for ERP systems in Kenyan Universities and should be improved, as it has vulnerabilities such as password guessing, password reuse, weak password recovery, and this may be prone to various forms of attacks which include; brute force attacks, replay attacks, social engineering, malware and denial of service attacks. The results of this study show that ERP system authentication can be improved by enhancing user authentication through multi-factor authentication. User

training is essential to achieve improved ERP systems security coupled with attack tolerance mechanisms.

5.5 Recommendations

The study, therefore, puts forth the following recommendations:

- Multi-factor authentication can be implemented to improve ERP systems security for Kenyan Universities and other organizations.
- Effective user training is critical in achieving ERP systems security.
- Universities and organizations must ensure effective implementation of ICT security policies and enforcement of its use.
- Universities and other organizations must invest in systems security.

5.6 Areas of Further Research

The study found the following for further research:

- Implementation of phone integrated authentication such as google authenticator; can be explored to improve ERP systems security.
- Measures to mitigate the risk of taking someone's phone and using it during authentication.
- Addressing other systems security issues that go beyond authentication.
- More research can be carried out on the implementation of other biometrics authentication for improved ERP systems security.
- Study of ERP systems in Universities by efficiency and location.

REFERENCES

- Akif, O. Z. (2017). *Secure Authentication Procedures Based on Timed Passwords, Honey Pots, Honeywords and Multi-Factor Techniques*.
- Alaca, F. (2018). *Strengthening Password-Based Web Authentication through Multiple Supplementary Mechanisms*.
- Alushula, P. (2021). *NHIF goes for Fingerprint Identity in War on Fraud*.
<https://www.businessdailyafrica.com/bd/corporate/companies/nhif-goes-for-fingerprint-identity-in-war-on-fraud>
- Bett, A. K. (2018). Challenges and Prospects of Enterprise Resource Planning (ERP) Systems in the Newly Chartered Public Universities in Kenya. *International Journal of Scientific Research and Management (IJSRM)*, 06(02).
<https://doi.org/10.18535/ijssrm/v6i2.em01>
- Chetalam, L. (2018). *Enhancing Security of M-Pesa Transactions by use of Voice Biometrics*.
- Communications Authority of Kenya : Kenya National Bureau of Statistics. (2016). *Public Sector ICT Survey Report*.
- Cresswell, J. W. (2018). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (Third Edit).
- First Identity Online Alliance. (2019). *The-State-of-Strong-Authentication-2019-Report.pdf*. <https://media.fidoalliance.org/wp-content/uploads/2019/01/The-State-of-Strong-Authentication-2019-Report.pdf>
- Garrett, K. (2016). *Vulnerability Analysis of Multi-Factor Authentication Protocols*.
- Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Authentication Guideline*. NIST, National Institute of Standards and Technology.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- Islam, S. K. H. (2015). Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system. *Journal of King Saud University - Computer and Information Sciences*, 27(2), 211–221.
<https://doi.org/10.1016/j.jksuci.2014.03.018>
- Kimuyu, H. (2019). *Kenyan Government Websites Hacked*.
<https://nairobi.news.nation.co.ke/news/kenyan-government-websites-hacked>
- Mayieka, J. M. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. *International Journal of Computer Science and Network*, 8(4).
- Miessler, D. (2021). *The Consumer Authentication Strength Maturity Model (CASMM) v5*. <https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model/>
- Muiruri, K. J. (2015). *Threats Mitigation Measures and Security of Cloud-Based Enterprise Resource Planning Systems in Kenya*.
[http://erepository.uonbi.ac.ke/bitstream/handle/11295/93156/Kinyanjui_Threats mitigation measures and security of cloud-based enterprise resource planning systems in Kenya.pdf?sequence=1](http://erepository.uonbi.ac.ke/bitstream/handle/11295/93156/Kinyanjui_Threats%20mitigation%20measures%20and%20security%20of%20cloud-based%20enterprise%20resource%20planning%20systems%20in%20Kenya.pdf?sequence=1)
- Mutambo, A. (2016). *State admits hackers stole data from Ministry of Foreign Affairs*.
<https://nairobi.news.nation.co.ke/news/state-admits-hackers-stole-data-foreign-affairs-ministry>
- Njoroge, P. M., Ogalo, J., & Ratemo, C. M. (2019). A Framework for Effective Information Security Risk Management in Kenyan Public Universities. *International*

- Journal of Social Sciences and Information Technology*, October, 0–19.
- Ntonja, K. G., Muketha, G. M., & Kamau, G. N. (2020). Cloud Data Privacy Preserving Model for Health Information Systems Based on Multi-Factor Authentication. *International Journal of Recent Technology and Engineering (IJRTE)*, 3, 360–367. <https://doi.org/10.35940/ijrte.C4458.099320>
- Odera, S. (2016). *Integrating Passphrases as an Authentication Mechanism in E-Commerce*.
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication : A Survey †. *Cryptography*, 2(1), 1–31. <https://doi.org/10.3390/cryptography2010001>
- Opoku, M. O., & Enu-Kwesi, F. (2020). Relevance of the technology acceptance model (TAM) in information management research: a review of selected empirical evidence. *Pressacademia*, 7(1), 34–44. <https://doi.org/10.17261/pressacademia.2020.1186>
- Rathore, T. S., & Gupta, A. (2017). Security Issues and Their Countermeasures in the ERP. *International Journal of Advances in Electronics and Computer Science*, ISSN: 2393-2835, 4, 39–43.
- Serianu. (2020). *Africa Cyber Security Report 2019/2020*. 1–104. <https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf>
- Singoro, B., Achoka, J. S. K., & Ndiku, J. M. (2018). The Hurdles encountered with the Implementation of ERP in the management of academic affairs in Public Universities in Kenya. *International Journal of Advanced Educational Research*, 3(4), 1–10.
- Ting, D. M. T., Hussain, O., & LaRoche, G. (2016). *Systems and Methods for Multi-Factor Authentication* (Patent No. US 9,118,656 B2).
- TrendMicro. (2019). *Hackers Exploit ERP App Flaw for Fraudulent Accounts in 62 Colleges, Universities*. <https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/hackers-exploit-erp-app-flaw-for-fraudulent-accounts-in-62-colleges-universities>
- Velasquez, I., Caro, A., & Rodiruez, A. (2019). Multifactor Authentication Methods : A Framework for Their Comparison and Selection. *InTech Open Computer Network and Security*. doi: <http://dx.doi.org/10.5772/intechopen.89876>
- Wanjala, A. (2020). *Data of Thousands of Mount Kenya University Students Leaked Online*. <https://techtrendske.co.ke/data-of-thousands-of-mount-kenya-universitys-students-leaked-online/>
- William, G. Z., Carr, J. C., Babin, B., & Griffin, M. (2013). *Business Research Methods*.
- Zaini, M. K., Masrek, M. N., Sani, M. K. J. A., & Anwar, N. (2018). Theoretical Modeling of Information Security: Organizational Agility Model based on Integrated System Theory and Resource-Based View. *International Journal of Academic Research in Progressive Education and Development*, 7(3), 390–400. <https://doi.org/10.6007/ijarped/v7-i3/4379>
- Ziani, D., & Al-muwayshir, R. (2017). *Improving Privacy and Security in Multi-Tenant Cloud ERP Systems*. 8(5), 1–15. <https://doi.org/10.5121/acij.2017.8501>

APPENDICES

Appendix 1 – Chartered Universities in Kenya

NO	UNIVERSITY	YEAR OF ESTABLISHMENT	YEAR OF AWARD OF CHARTER	COUNTY
PUBLIC CHARTERED UNIVERSITIES				
1.	University of Nairobi	1970	2013	Nairobi
2.	Moi University	1984	2013	Uasin Gishu
3.	Kenyatta University	1985	2013	Nairobi
4.	Egerton University	1987	2013	Nakuru
5.	Jomo Kenyatta University of Agriculture and Technology	1994	2013	Kiambu
6.	Maseno University	2001	2013	Kisumu
7.	Chuka University	2007	2013	Meru
8.	Dedan Kimathi University of Technology	2007	2013	Nyeri
9.	Kisii University	2007	2013	Kisii
10.	Masinde Muliro University of Science and Technology	2007	2013	Kakamega
11.	Pwani University	2007	2013	Kilifi
12.	Technical University of Kenya	2007	2013	Nairobi
13.	Technical University of Mombasa	2007	2013	Mombasa
14.	Maasai Mara University	2008	2013	Narok
15.	Meru University of Science and Technology	2008	2013	Meru
16.	Multimedia University of Kenya	2008	2013	Nairobi
17.	South Eastern University	2008	2013	Kitui
18.	Jaramogi Oginga Odinga University of Science and Technology	2009	2013	Siaya
19.	Laikipia University	2009	2013	Laikipia
20.	University of Kabianga	2009	2013	Kericho
21.	Karatina University	2010	2013	Nyeri
22.	University of Eldoret	2010	2013	Uasin Gishu
23.	Kibabii University	2011	2015	Bungoma
24.	Kirinyaga University	2011	2016	Kirinyaga
25.	Machakos University	2011	2016	Machakos
26.	Murang'a University of Technology	2011	2016	Murang'a
27.	Rongo University	2011	2016	Migori

28.	Taita Taveta University	2011	2016	Taita-Taveta
29.	The Co-operative University of Kenya	2011	2016	Nairobi
30.	University of Embu	2011	2016	Embu
31.	Garissa University	2011	2017	Garissa
TOTAL 31				
PRIVATE CHARTERED UNIVERSITIES				
1.	University of Eastern Africa, Baraton	1989	1991	Nandi
2.	Catholic University of Eastern Africa	1989	1992	Nairobi
3.	Daystar University	1989	1994	Machakos
4.	Scott Christian University	1989	1997	Nairobi
5.	United States International University	1989	1999	Nairobi
6.	Africa Nazarene University	1993	2002	Kajiado
7.	Kenya Methodist University	1997	2006	Meru
8.	St. Paul's University	1989	2007	Kiambu
9.	Pan Africa Christian University	1989	2008	Nairobi
10.	Kabarak University	2002	2008	Nakuru
11.	Strathmore University	2002	2008	Nairobi
12.	Africa International University	1989	2011	Nairobi
13.	Kenya Highlands Evangelical University	1989	2011	Kericho
14.	Mount Kenya University	2008	2011	Kiambu
15.	Great Lakes University of Kisumu	2005	2012	Kisumu
16.	Adventist University	2005	2013	Kajiado
17.	KCA University	2007	2013	Nairobi
18.	KAG – EAST University	1989	2016	Kajiado
TOTAL 18				

Appendix 2 – Questionnaire

Developing a Multi-Factor Authentication Prototype for Improved Security of Enterprise Resource Planning Systems in Kenyan Universities

Dear Sir/Madam,

I am a Master of Science in Applied Information Technology student at Africa Nazarene University researching on Developing a Multi-Factor Authentication Prototype for improved security of ERP systems in Kenyan Universities. I am kindly seeking your assistance with information on this topic to enable me to achieve the objective of this research.

Your assistance will be highly appreciated.

Please be assured that the information you provide will be treated as confidential and used for this research only.

You are kindly requested to answer **all** the following questions.

NB: Do not include your name.

PART I: GENERAL INFORMATION

University

Click or tap here to enter text.

1. What is your gender?

2. What is your age bracket?

3. What role do you play in the ICT Department?

Click or tap here to enter text.

4. Highest level of education?

5. Years of Experience in systems administration roles

PART II: ERP SYSTEMS AND AUTHENTICATION METHODS

6. Does your University have an ERP system?

7. How long has the ERP system been in use?

Click or tap here to enter text.

8. Type of ERP used?

SAP

Navision

ABN Unisol

Multiple

Other Click or tap here to enter text.

9. What User Authentication Method is used for the ERP system in your University (you can select more than one if applicable)?

- Tokens
- QR Codes
- Biometrics
- Email Verification
- SMS Verification
- Passwords
- Other Click or tap here to enter text.

10. Do you consider the authentication method to offer adequate ERP security?
5= Strongly Agree, 4= Agree, 3= Neutral, 2= Disagree, 1= Strongly Disagree

11. How would you rate the security of your current ERP authentication method(s)?
5=Very Strong, 4=Strong, 3=Moderate, 2= Weak, 1= Very Weak

12. Which level of the following security attributes does the current ERP authentication method offer?

5=Very Strong, 4=Strong, 3=Moderate, 2= Weak, 1= Very Weak

	Very Strong	Strong	Moderate	Weak	Very Weak
Ease of use	<input type="radio"/>				
Confidentiality	<input type="radio"/>				
Integrity	<input type="radio"/>				
Availability	<input type="radio"/>				
Attack tolerance	<input type="radio"/>				

13. Do you feel there is a need for authentication methods to be improved?

PART III: VULNERABILITIES OF CURRENT ERP AUTHENTICATION METHODS

14. What vulnerabilities is the current ERP authentication method(s) prone to? (select all that may apply)

- Password Guessing
- Brute Force Attacks
- Shoulder Surfing
- Password Cracking
- Weak Password Recovery
- Internal Observation
- Targeted impersonation
- Physical Theft
- Denial of Service Attacks
- Replay Attacks
- Password Reuse
- Other [Click or tap here to enter text.](#)

15. Have any ERP user accounts authentication been compromised in the last three years?

-
-
-
-

16. Does your University have any of the following infrastructure to support improved ERP system authentication security?

- Email
- SMS
- Biometrics
- Other [Click or tap here to enter text.](#)

17. Is the infrastructure in 16 above open for integration with the ERP system?

-
-
-
-

18. Does your University have an ICT Security Policy in place?

-

19. If yes in 18, does the policy offer guidance on secure authentication and privacy policies?

-

20. If yes in 19, how would you rate the effectiveness of the ICT Security Policy on secure systems authentication?

5=Very High, 4=High, 3=Moderate, 2= Low, 1= Very Low

-

21. How often are users trained on ERP authentication security?

-

22. Level of user training on ERP authentication security?

5=Very High, 4=High, 3=Moderate, 2= Low, 1= Very Low

-

23. In your opinion how can ERP systems security in Kenyan Universities be improved?

Type text here

Thank you for taking the time to fill out this questionnaire.

Appendix 3 – NACOSTI Research Permit

755952

RESEARCH LICENSE



This is to Certify that Ms. CAROLYNE WANJIRU KIMANI of Africa Nazarene University, has been licensed to conduct research in Embu, Kakamega, Kericho, Kiambu, Kilifi, Kirinyaga, Kisii, Lailipia, Machakos, Meru, Muranga, Nairobi, Nakuru, Narok, Nyeri on the topic: Developing a Multi-Factor Authentication Prototype for Improved Enterprise Resource Planning Systems Security for Universities in Kenya for the period ending : 06/January/2022.

License No: NACOSTIP/21/8383

Applicant Identification Number
755952

Director General
NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code



NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013

The Grant of Research Licenses is Guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014

CONDITIONS

1. The License is valid for the proposed research, location and specified period
2. The License any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearance from relevant Government Agencies
5. The License does not give authority to transfer research materials
6. NACOSTI may monitor and evaluate the licensed research project
7. The Licensee shall submit one hard copy and upload a soft copy of their final report (thesis) within one year of completion of the research
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice

National Commission for Science, Technology and Innovation
off Waiyaki Way, Upper Kabete,
P. O. Box 30623, 00100 Nairobi, KENYA
Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077
Mobile: 0713 788 787 / 0735 404 245
E-mail: dg@nacosti.go.ke / registry@nacosti.go.ke
Website: www.nacosti.go.ke

Appendix 4 – Reliability Test Output

RELIABILITY

/VARIABLES=WorkExperience SecurityAdequacy EaseOfUse ICTPolicyEffectiveness
Confidentiality

Integrity Availability AttackTolerance SecurityRating UserTrainingLevel ERPUsagePeriod

/SCALE('ALL VARIABLES') ALL

/MODEL=ALPHA

/STATISTICS=DESCRIPTIVE SCALE

/SUMMARY=TOTAL CORR.

Reliability

Case Processing Summary

		N	%
Cases	Valid	3	100.0
	Excluded ^a	0	.0
	Total	3	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.745	.576	11

Appendix 5 – Digital Persona 4500 Fingerprint Reader Technical Specifications



U.are.U® 4500 Reader USB Fingerprint Reader

Target Applications

- Desktop PC security
- Mobile PCs
- Custom applications

Features

- Blue LED
- Small form factor
- Excellent image quality
- Superior ESD resistance
- Encrypted fingerprint data
- Latent print rejection
- Counterfeit finger rejection
- Rotation invariant
- Rugged
- Works well with dry, moist or rough fingerprints
- Compatible with Windows® Vista, XP Professional, 2000 and Windows Server 2000, 2003, 2008

Key Specifications

- Pixel resolution: 512 dpi (average x, y over the scan area)
- Scan capture area: 14.6 mm (nom. width at center) 18.1 mm (nom. length)
- 8-bit grayscale (256 levels of gray)
- Reader size (approximate): 65 mm x 36 mm x 15.56 mm
- Compatible with USB 1.0, 1.1 and 2.0 (Full Speed) specifications
- Indoor, home and office use



Product Description

The U.are.U 4500 Reader is an elegant, powerful fingerprint identity machine. With an executive-class look and feel, the U.are.U 4500 Reader is perfect for power users and shared environments. Its design is sleek and compact to conserve valuable desk space but it stays right where you put it because of its nice heft and special undercoating.

The U.are.U 4500 radiates an attractive blue glow that provides an unobtrusive presence in low light environments and also ensures that it does not compete with alarm colors in settings such as healthcare.

To use, you simply place your finger on the glowing window, and the reader quickly and automatically scans your fingerprint. For superior user feedback, a red "flash" indicates that a fingerprint image has been captured. On-board electronics calibrate the reader and encrypt the scanned data before sending it over the USB interface.

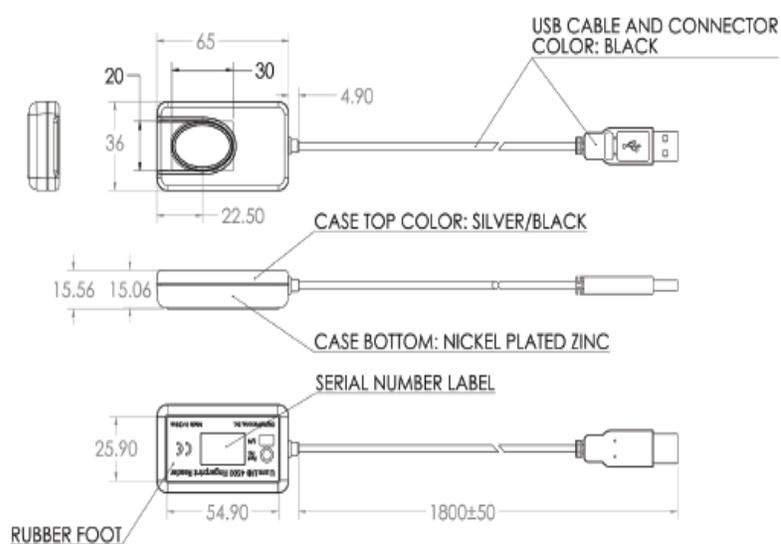
DigitalPersona readers utilize optical fingerprint scanning technology to achieve excellent image quality, a large capture area and superior reliability. The U.are.U 4500 Reader and DigitalPersona® Fingerprint Recognition Engine have an unmatched ability to authenticate even the most difficult fingerprints accurately and rapidly regardless of placement angle.

The U.are.U 4500 Reader can be purchased for use with DigitalPersona Pro Workstation, DigitalPersona Pro Kiosk, DigitalPersona Online, DigitalPersona Personal or any of the DigitalPersona SDK packages. Whether you are an enterprise customer, a system integrator or a home user, DigitalPersona's fingerprint authentication solutions provide a natural extension to your security system and applications.



Part Number	Packaging	Fingerprint Surface
88003-001-102	Single unit	Standard coating
88003-B01-102	2 or more units - packaged bulk	Standard coating
88004-001-102	Single unit	Heavy Duty coating
88004-B01-102	2 or more units - packaged bulk	Heavy Duty coating

Mechanical Specifications



Ratings

Supply Voltage	5.0V ±5% supplied by USB
Supply Current—scanning	190 mA (Typical)
Supply Current—idle mode	140 mA (Typical)
Supply Current—suspend mode	1.5 mA (Maximum)
ESD Susceptibility	>15 kV, mounted in case
Temperature, Operating	0 - 40 C
Humidity, Operating	20% - 80% non-condensing
Temperature, Storage	-10 - 60 C
Humidity, Storage	20% - 90% non-condensing
Scan Data	8-bit grayscale
Standards Compliance	FCC Class B, CE, ICES, BSMI, MIC, USB, WHQL

Appendix 6 – Multi-Factor Authentication Prototype Screenshots

User Registration

The screenshot shows the 'SYSTEM USERS' page in the ERP SYSTEM. A green notification banner at the top reads: "User Created Successfully. Navigate to fingerprint to register a finger." Below this is a table of system users with columns for EMP NO, FULL NAME, USERNAME, FINGERPRINT, TEL/EMAIL, ROLE, and ACTION. The table contains five rows of user data.

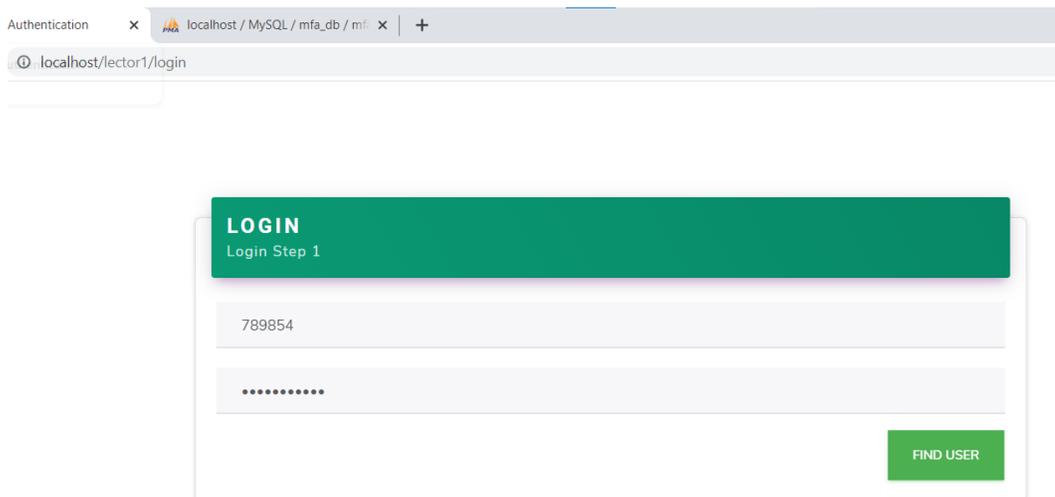
EMP NO	FULL NAME	USERNAME	FINGERPRINT	TEL/EMAIL	ROLE	ACTION
789855	Janet Wendo	Janet	.	7213305501 wendoj@gmail.com	Accountant	DEL EDIT
789855	Mercy Kemunto	Mercy	1.522545A0D1	254721311897 example@gmail.com	Accountant	DEL EDIT
789854	Carolyn Kimani	Carolyn	1.272532A5D7	254721311897 kimanicarolyn@gmail.com	Administrator	DEL EDIT
78956	Beatrice Wairimu	beatrice	.	254720279909 beatrice@gmail.com	Secretary	DEL EDIT
789852	Evans Maoncha	evans	1.58553C03A2	254721311897 evansmaoncha@gmail.com	Secretary	DEL EDIT

Fingerprint Capture

The screenshot shows the 'FINGERPRINT DATA' page in the ERP SYSTEM. A modal window is open for fingerprint capture, displaying a fingerprint image. Below the modal is a table for managing fingerprint data with columns for USER ID, EMP NO, FINGERPRINT, and ACTION. The table contains five rows of data.

USER ID	EMP NO	FINGERPRINT	ACTION
39	78956		REGISTER
38	789852		DEL FINGERPRINT
40	789854		DEL FINGERPRINT
41	789855	1	DEL FINGERPRINT
42	789855	0	REGISTER

Log in using Multi-Factor Authentication



Authentication x localhost / MySQL / mfa_db / mfa x +

localhost/lector1/login

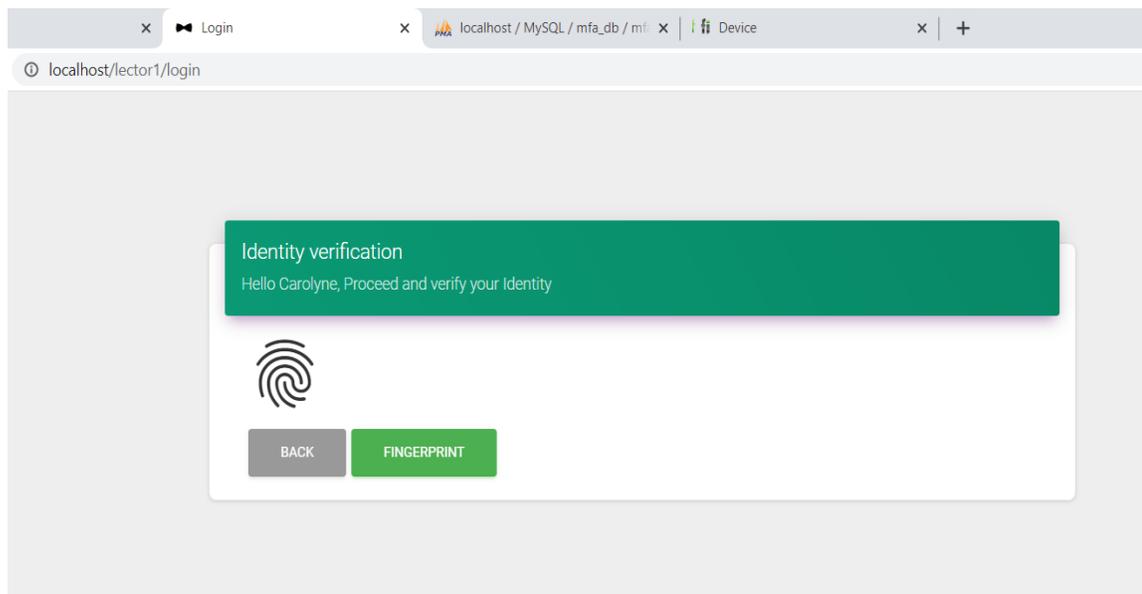
LOGIN
Login Step 1

789854

.....

FIND USER

MFA Prototype Login Step 1 for Password and Fingerprint Option



x Login x localhost / MySQL / mfa_db / mfa x Device x +

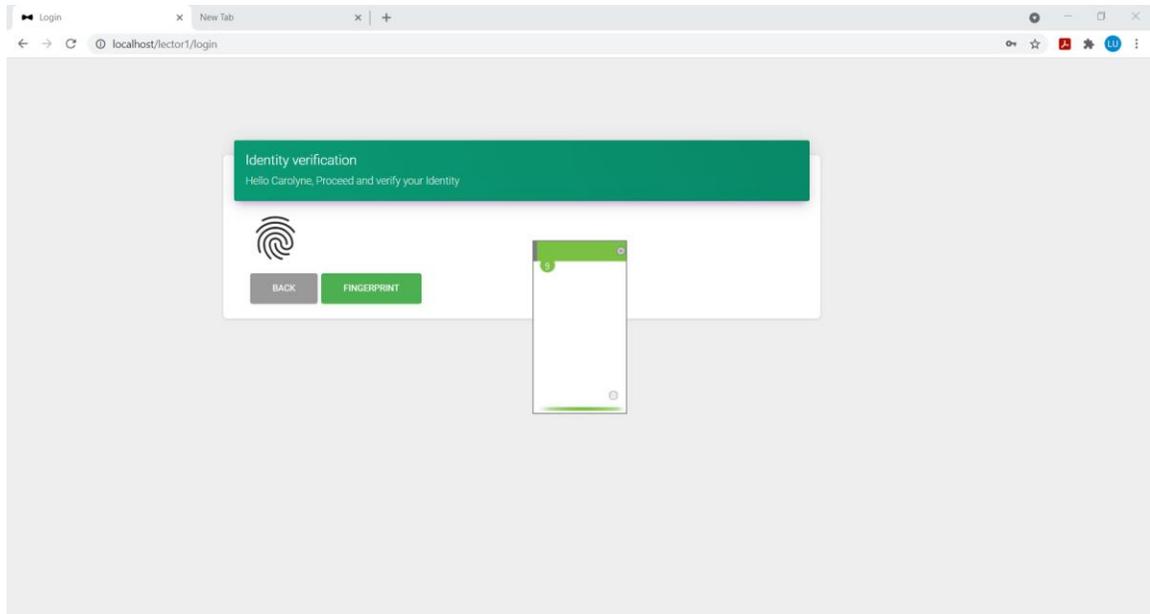
localhost/lector1/login

Identity verification
Hello Carolyne, Proceed and verify your Identity

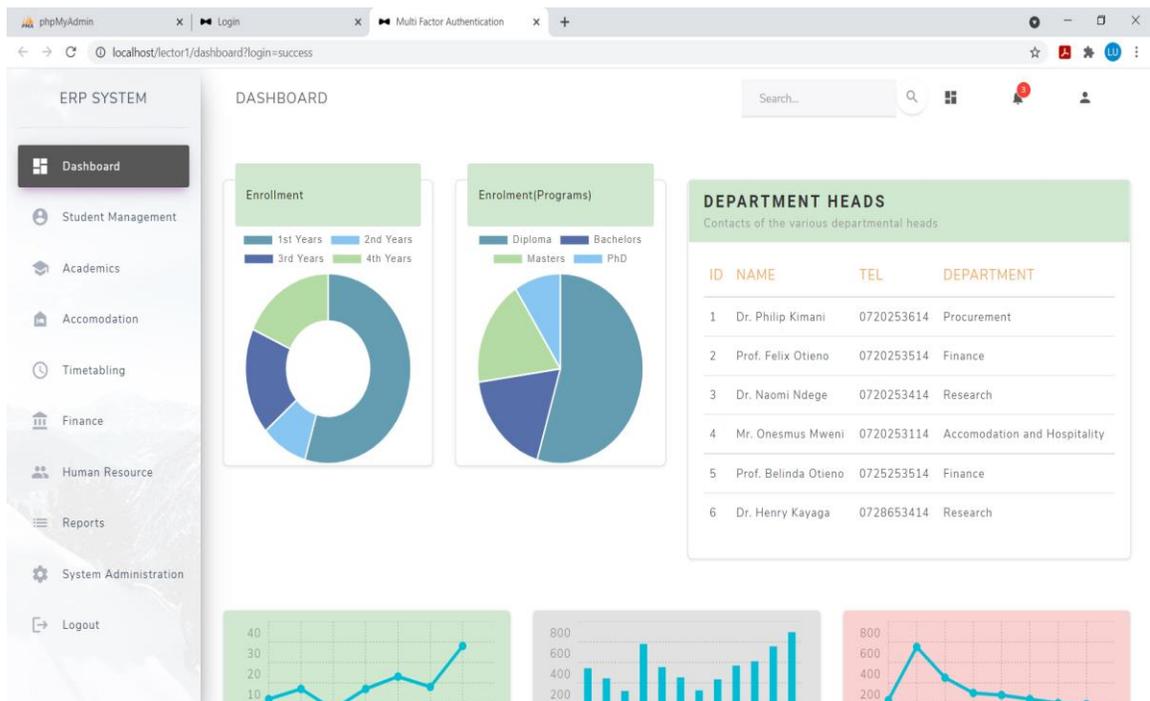


BACK FINGERPRINT

MFA Prototype Login Step 2 with Fingerprint Verification

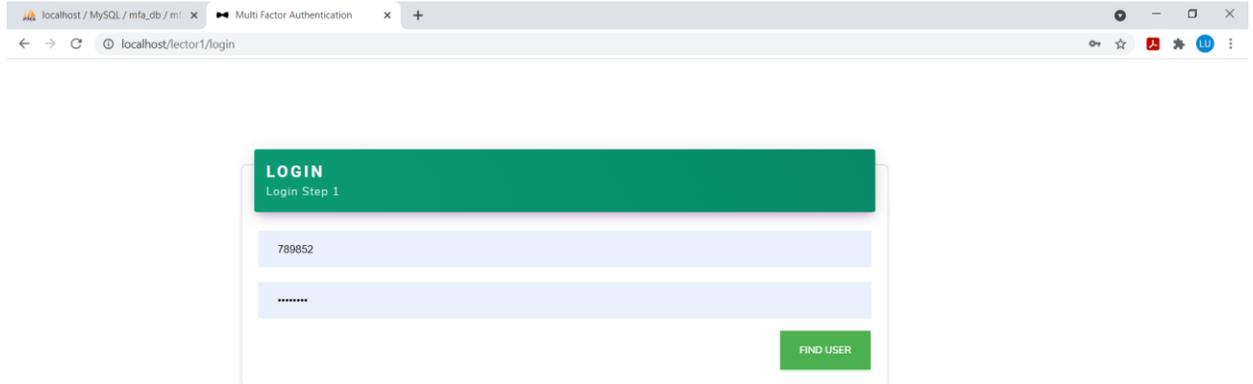


MFA Prototype Login Step 2 with Fingerprint Verification



MFA Prototype - ERP Dashboard

Username + Password and SMS option



localhost / MySQL / mfa_db / mi x Multi Factor Authentication x +

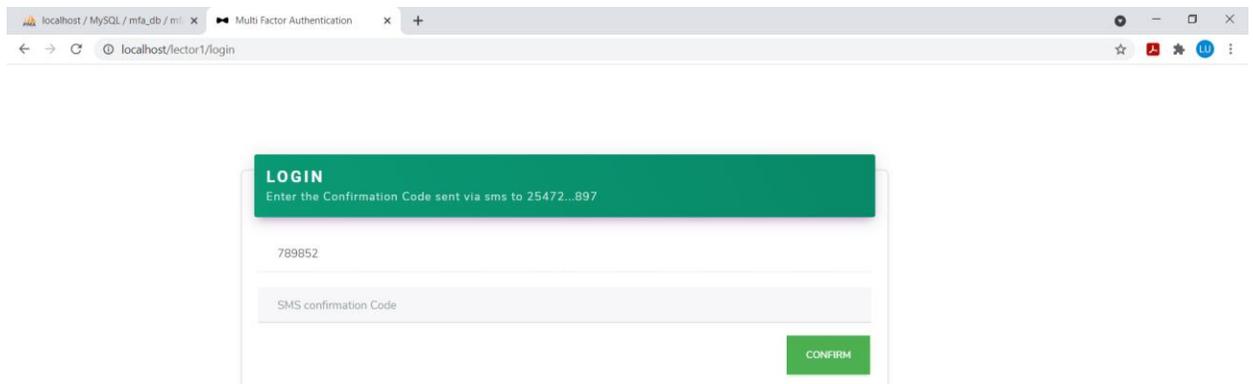
localhost/lector1/login

LOGIN
Login Step 1

789852

FIND USER

MFA Prototype Login Step 1 for Password and SMS Code



localhost / MySQL / mfa_db / mi x Multi Factor Authentication x +

localhost/lector1/login

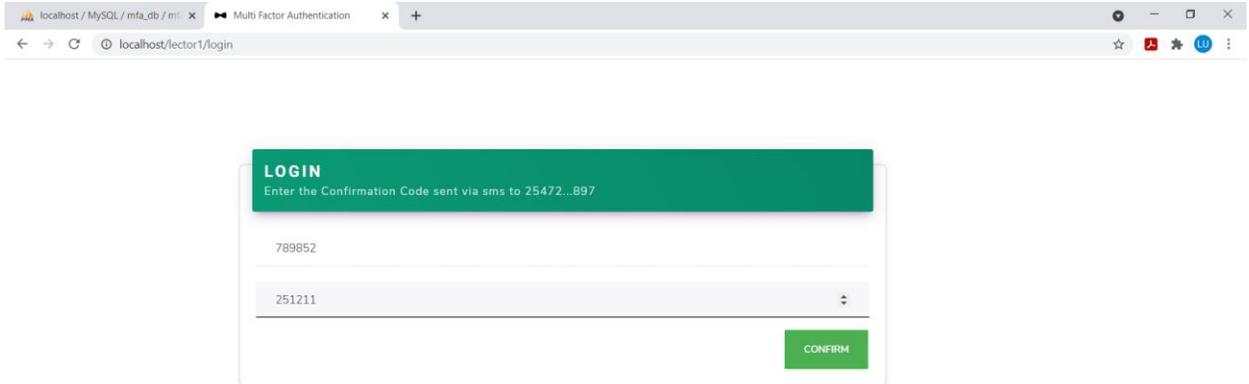
LOGIN
Enter the Confirmation Code sent via sms to 25472...897

789852

SMS confirmation Code

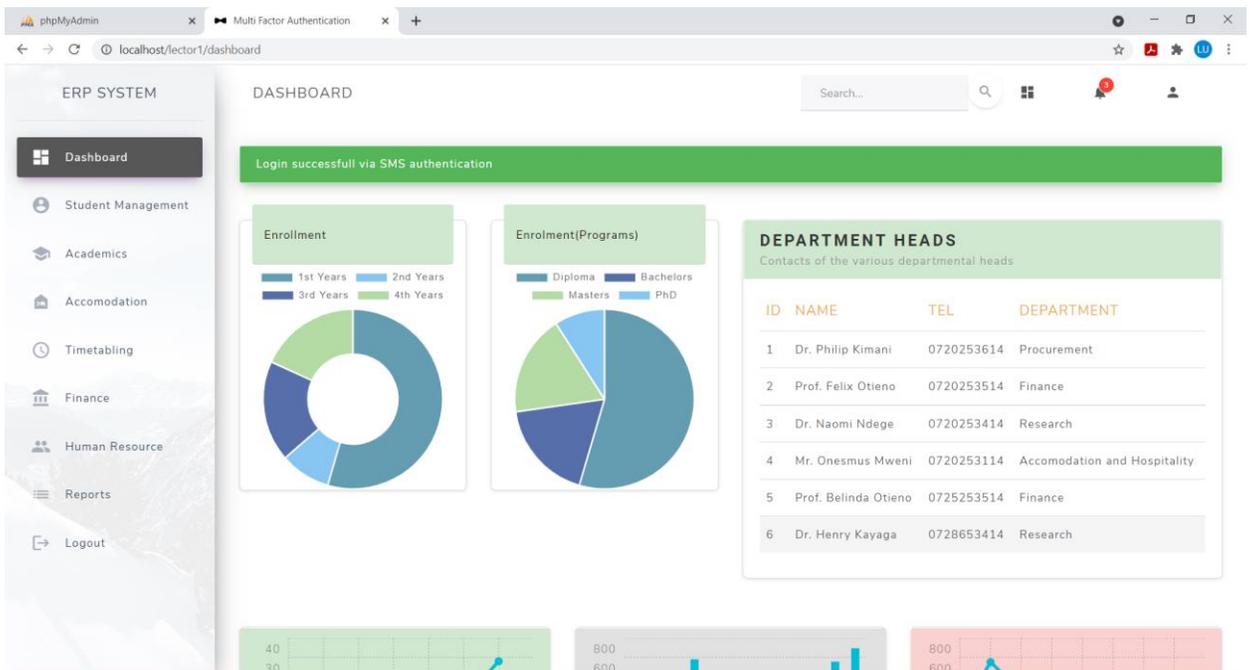
CONFIRM

MFA Prototype Login Step 2 with SMS Code Verification



© 2021

MFA Prototype Login Step 2 with SMS Code Verification



MFA Prototype Dashbard on Successful Login

ERP SYSTEM

SYSTEM USERS

Search...

Users Logs Devices Fingerprint

SYSTEM USERS
List of Users

CREATE

EMP NO	FULL NAME	USERNAME	FINGERPRINT	TEL/EMAIL	ROLE	ACTION
789854	Carolyne Kimani		.	254721311897 kimanicarolyne@gmail.com	Administrator	DEL EDIT
78956	Beatrice Wairimu	beatrice	.	254720279909 beatrice@gmail.com	Secretary	DEL EDIT
789852	Evans Maoncha	evans	1.5B553CD3A2	254721311897 evansmaoncha@gmail.com	Secretary	DEL EDIT

ERP SYSTEM

- Dashboard
- Student Management
- Academics
- Accommodation
- Timetabling
- Finance
- Human Resource
- Reports
- System Administration**
- Logout

MFA Prototype - System Users Data

ERP SYSTEM

FINGERPRINT DATA
Manage Fingerprint Data

Users Logs Devices Fingerprint

USER ID	EMP NO	TEMPLATE	ACTION
39	78956	0	REGISTER
38	789852	1	DEL FINGERPRINT
40	789854	0	REGISTER

ERP SYSTEM

- Dashboard
- Student Management
- Academics
- Accommodation
- Timetabling
- Finance
- Human Resource
- Reports
- System Administration**
- Logout

MFA Prototype - System Users Fingerprint Data

User Activity Logs

The screenshot shows the 'LOGS HISTORY' section of the ERP SYSTEM. It features a search bar and a table with columns for TIME, EMP NUMBER, IP, and DATA. The table lists various system events such as user updates, logins, and password validations.

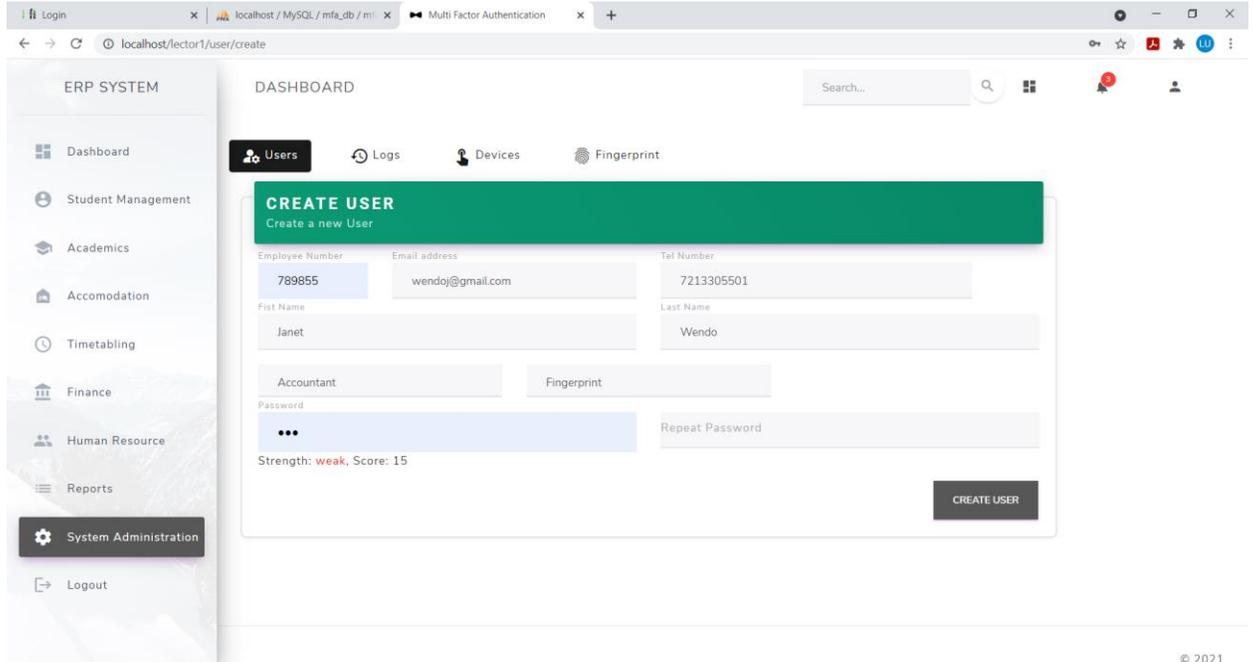
TIME	EMP NUMBER	IP	DATA
2021-07-08 09:04:18	789854	:::1	789856 User Updated Successfully.
2021-07-08 09:03:09	789854	:::1	SerialNo L120E15865
2021-07-08 09:02:59	789854	:::1	System Login. Password and Employee Number authentication Successful.
2021-07-08 09:02:59	789854	:::1	System Login. Fingerprint Login Initiated.
2021-07-06 15:11:04	789854	:::1	789855 User Created Successfully.
2021-07-06 15:08:14	789854	:::1	SerialNo L120E15865
2021-07-06 15:08:07	789854	:::1	System Login. Password and Employee Number authentication Successful.
2021-07-06 15:08:07	789854	:::1	System Login. Fingerprint Login Initiated.
2021-07-06 15:04:48	N/A	:::1	789854 Attempted Login. Password validation Unsuccessful
2021-07-06 15:01:06	N/A	:::1	789854 Attempted Login. Password validation Unsuccessful

MFA Prototype Validation

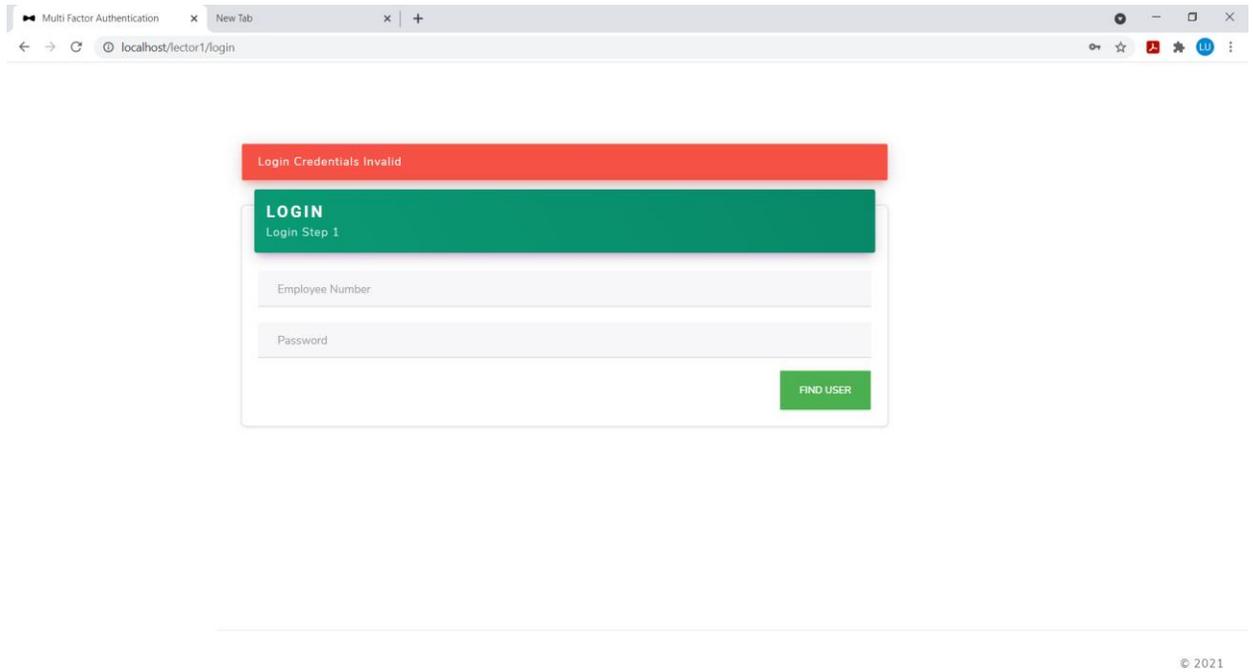
The screenshot shows the 'FINGERPRINT DATA' section of the ERP SYSTEM. A modal message box displays the error: 'localhost says '789855' registration fail!'. Below the message is a table with columns for USER ID, EMP NO, TEMPLATE, and ACTION. The table lists users with their respective fingerprint registration status and actions.

USER ID	EMP NO	TEMPLATE	ACTION
39	78956	0	REGISTER
38	789852	1	DEL FINGERPRINT
40	789854	1	DEL FINGERPRINT
41	789855	1	DEL FINGERPRINT
42	789855	0	REGISTER

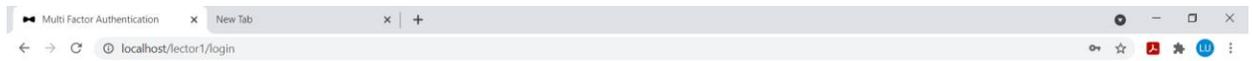
MFA Prototype - User Registration with Incomplete Data



MFA Prototype - User Registration with Weak Password

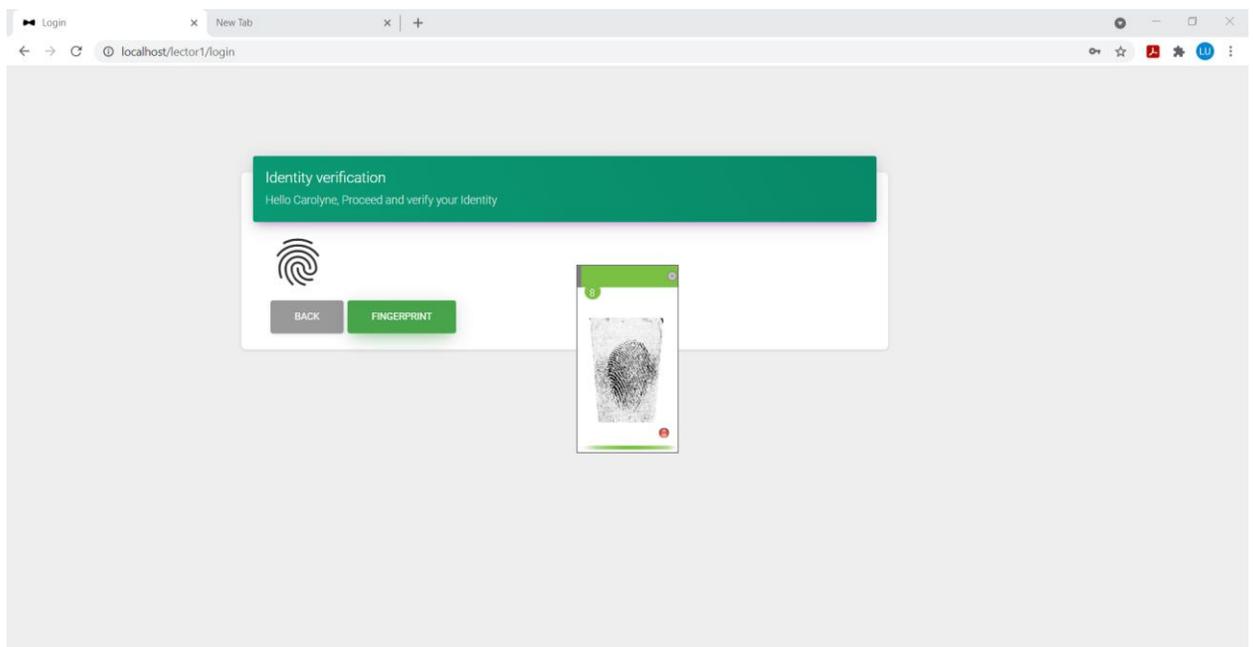


MFA Prototype Login with Invalid Credentials



© 2021

MFA Prototype - User Deactivation on Maximum Login Attempts



MFA Prototype - Login with Invalid Fingerprint

Appendix 7 – Multi-Factor Authentication Prototype Source Code

```
function checkUserName($user_name) {
    $sql = "SELECT user_name FROM mfa_user WHERE user_name =
    '$user_name.'";
    $conn = conn();
    $result = mysqli_query($conn,$sql);
    $row = mysqli_num_rows($result);

    if ($row>0) {
        return "Username exist!";
    } else {
        return "1";
    }
}
```

```
function getUserFinger($user_id) {

    $sql = "SELECT * FROM mfa_finger WHERE user_id= '$user_id.' ";
    $conn = conn();
    $result = mysqli_query($conn,$sql);
    $arr = array();
    $i = 0;

    while($row = mysqli_fetch_array($result)) {

        $arr[$i] = array(
            'user_id' =>$row['user_id'],
            'finger_id' =>$row['finger_id'],
            'finger_data' =>$row['finger_data']
        );
        $i++;
    }
    return $arr;
}
```

```
function getLog() {

    $sql = 'SELECT * FROM mfa_log ORDER BY log_time DESC';
    $conn = conn();
    $result = mysqli_query($conn,$sql);
    $arr = array();
    $i = 0;

    while ($row = mysqli_fetch_array($result)) {
        $arr[$i] = array(
```

```

        'log_time'      => $row['log_time'],
        'user_name'    => $row['user_name'],
        'data'         => $row['data']
    );

    $i++;
}

return $arr;
}

function createLog($user_name, $time, $sn) {

    $sql      = "INSERT INTO mfa_log SET user_name='".$user_name."',
data='".$date('Y-m-d H:i:s', strtotime($time))." (PC Time) | ".$sn." (SN)".' ";
    $conn = conn();
    $result1 = mysqli_query($conn,$sql);
    if ($result1) {
        return 1;
    } else {
        return "Error insert log data!";
    }
}

function getDevice() {

    $sql = 'SELECT * FROM mfa_device ORDER BY device_name ASC';
    $conn = conn();
    $result = mysqli_query($conn,$sql);
    $arr = array();
    $i = 0;

    while ($row = mysqli_fetch_array($result)) {

        $arr[$i] = array(
            'device_name' => $row['device_name'],
            'sn'          => $row['sn'],
            'vc'          => $row['vc'],
            'ac'          => $row['ac'],
            'vkey'        => $row['vkey']
        );

        $i++;
    }
    return $arr;
}

```

