I.J. Information Technology and Computer Science, **2023, 3, 42-54**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2023.03.04

Multi-Factor Authentication for Improved Enterprise Resource Planning Systems Security

Carolyne Kimani*
Africa Nazarene University, Nairobi, Kenya
E-mail: kimanicarolyne@gmail.com
ORCID iD: https://orcid.org/0000-0001-5169-2738
*Corresponding Author

James I. Obuhuma
Department of Computer Science, Maseno University, Private Bag, Maseno, Kenya
E-mail: jobuhuma@gmail.com, jobuhuma@maseno.ac.ke
ORCID iD: https://orcid.org/0000-0002-1360-4562

Emily Roche
Department of Computer & Information Technology, Africa Nazarene University, Nairobi, Kenya
E-mail: eroche@anu.ac.ke

Received: 16 October 2022; Revised: 25 November 2022; Accepted: 11 February 2023; Published: 08 June 2023

Abstract: Universities across the globe have increasingly adopted Enterprise Resource Planning (ERP) systems, a software that provides integrated management of processes and transactions in real-time. These systems contain lots of information hence require secure authentication. Authentication in this case refers to the process of verifying an entity's or device's identity, to allow them access to specific resources upon request. However, there have been security and privacy concerns around ERP systems, where only the traditional authentication method of a username and password is commonly used. A password-based authentication approach has weaknesses that can be easily compromised. Cyber-attacks to access these ERP systems have become common to institutions of higher learning and cannot be underestimated as they evolve with emerging technologies. Some universities worldwide have been victims of cyber-attacks which targeted authentication vulnerabilities resulting in damages to the institutions reputations and credibilities. Thus, this research aimed at establishing authentication methods used for ERPs in Kenyan universities, their vulnerabilities, and proposing a solution to improve on ERP system authentication. The study 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 that involved a survey of chartered Kenyan Universities, where questionnaires were used to collect data that was later analyzed using descriptive and inferential statistics. Stratified, random and purposive sampling techniques were used to establish the sample size and the target group. The dependent variable for the study was limited to security rating with respect to realization of confidentiality, integrity, availability, and usability while the independent variables were limited to adequacy of security, authentication mechanisms, infrastructure, information security policies, vulnerabilities, and user training. Correlation and regression analysis established vulnerabilities, information security policies, and user training to be having a higher impact on system security. The three variables hence acted as the basis for the proposed multi-factor authentication framework for improve ERP systems security.

Index Terms: Authentication, Enterprise Resource Planning System, ERP System Security, Multi-Factor Authentication, System Security.

1. Introduction

Organizations and even individuals are shifting their day-to-day activities from manual records and transactions to the use of ERP systems and other digital services. An ERP system is a kind of software consisting of a suite of integrated applications that organizations can use to collect, process, manage, store, and interpret data from business activities. 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 [1]. 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 [2], identified privacy and security as the two major system security concerns. Unfortunately, little investment is made to address these concerns. It is worth noting that attackers are always working tirelessly to exploit these systems with varied missions. Unfortunately, gaining illegitimate access to these systems enables attackers to access valuable information for their benefit, to the disadvantage or loss of the owner. This has led to research on ways of strengthening authentication mechanisms.

Authentication which is the process of verifying a user's identity, process, or device, as a prerequisite to allowing access to a system's resources, is a common risk area since it is the entry point for an ERP system. 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. 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 [3]. 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 [4]. Across the world, various leading technology companies including Google, Apple, Facebook, Twitter, Visa, Paypal, among others, have moved fast in adopting and implementing optional multi-factor authentication strategies. This aims at securing the large amounts of personal, transactional, sensitive information contained in their systems and mitigating the ever-rising cyber threats [3].

Mayieka [5], highlights the fact that institutions of higher learning in Kenya, Africa and globally, are facing a high rate of increase in cyber-threats. The study further underscores the importance of reinforcing responsible cybersecurity measures and investing in cybersecurity technologies. According to [3], the use of passwords alone is considered the most vulnerable authentication method, thus, needs to be done away with or enhanced. Passwords can be easily cracked, guessed or attacked since most of them are normally formulated based on users' personal information. Student hacktivism to interfere with school information systems to alter grades and/or fee balances have also been on the rise and therefore requires proper solutions to be developed [5].

The increase in cybersecurity threats, therefore, calls for the improvement of ERP authentication mechanisms to ensure tougher systems securities. This study was based on a presumption that the use of passwords is currently the most common authentication method for ERP systems in Kenyan universities. This authentication method requires enhancement since it has been identified to be prone to vulnerabilities like password guessing, password reuse, social engineering, among others. This was hence the prime motivation behind this research. The research, therefore, sought to address the presumption with its associated weaknesses by identifying current authentication methods in use, establishing their vulnerabilities and potential attacks, and finally proposing ways to improve ERP systems security. Specifically, the study focused on addressing three key objectives, using a case of selected Kenyan Universities:

- To identify the current authentication methods used in ERP systems.
- To establish vulnerabilities in existing ERP systems' authentication methods.
- To develop and validate a multi-factor authentication framework prototype for improving ERP system security.

The significance of this study is two-fold: first, actual vulnerabilities and potential attacks to ERP systems are determined and discussed. Secondly, a multi-factor authentication framework is proposed, prototyped and tested. The outcomes of the study will be beneficial to Universities, other private and public organisations, and government agencies towards enhancing the security of their systems.

The rest of the paper explores related work, the methodology used in this study, findings and their discussion, and finally the conclusion and recommendations for further research, in that order.

2. Related Works

Authentication is the verification of a user's process or device's identity to allow access to the system's resources. Authentication can be categorized based on three authentication approaches, namely, something that the user knows, something that the user has and something that the user is. The three align to knowledge-based authentication, ownership-based authentication and biometric-based authentication respectively. Use of at least two or three factors from either category for verification is considered to provide a positive, secure authentication.

2.1. Knowledge-based Authentication

This refers to the use of something that the user knows such as a password, Personal Identification Number (PIN),

passphrase, security question or challenge-response. Unfortunately, knowledge-based factors offer a low level of security and may jeopardize confidentiality [6]. The use of passwords, PINs or security questions offer better usability, familiarity and low-cost advantages over the other mechanisms. However, knowledge-based authentication factors offer low levels of security, requires users to recall, and may be prone to vulnerabilities such as impersonation, they can be forgotten, shared, leaked, stolen, or easily guessed. They are also prone to social engineering kinds of attacks where social engineering entails the use of social factors to extract sensitive information from system users. A study by Obuhuma and Zivuku [7], elaborates on the widespread use of social engineering in Kenya.

2.2. Ownership Based Authentication

This refers to the use of something the user has like an identification card, security token, device token, or Quick Response (QR) code among others [8]. Authentication factors in this category have advantages of portability of credentials, security with limited log in attempts, difficult to masquerade and prevents data manipulation. Their security level is however medium.

Certificate-based authentication mechanism uses software-based identifiers to identify users or devices. The use of digital certificates guarantees a high security level, privacy, integrity and portability. Unfortunately, they pose usability complexities for different types of data, provide single-sign-on and must be kept secure.

2.3. Biometric Based Authentication

This refers to the use of something the user is or does. This authentication method verifies a user's identity based on evaluating their distinct physical or behavioral characteristics. These physical biometric characteristics include fingerprints, facial recognition, hand geometry, iris and retinal patterns. The behavioral traits include voice recognition, keystroke patterns and signature. Biometrics provide the strongest authentication. The most commonly used biometric authenticators are fingerprints, which are verified by a fingerprint scanner that validates a user's identity based on fingerprint data stored in a database [9]. This kind of authentication provides high security level, uniqueness, is difficult to circumvent, they do not require the user to recall information, cannot be lost and are accurate. Biometrics may be difficult to integrate, can be costly and sometimes viewed as a violation of user privacy.

First Identity Online Alliance [3], comparison of five authentication mechanisms sampled from the three categories of authentication factors shows a variance in accuracy, cost, required devices and social acceptability. This therefore means that a combination of two or more mechanisms has a higher likelihood of improving security as recommended by [9]. Such an approach will result in multi-factor authentication. Multi-factor authentication (MFA) has been known to be a better security option. However, it has implementation complexities that requires deployment and integration of additional software for them to work. This position 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.

Ting et al., [10], reviews methods to secure resources using a multi-factor authentication policy consisting of various access control methods. The study establishes that 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. Biometrics is 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.

Multi-factor authentication is commonly being adopted in the banking, mobile money, and 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, and Microsoft Outlook, where it can be set as an optional feature. The 2019/2020 Africa Cybersecurity report by Serianu [4] recommends the implementation of multi-factor authentication and biometrics to improve systems identity and access management in Africa.

According to Ntonja et al. [11], 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. The study was carried out in Maua Methodist Hospital in Meru County, Kenya, as a survey of 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 and 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. 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, [12] aimed at addressing security issues associated with password-based authentication mechanisms in e-commerce websites. The study by Odera [12] used a design science approach with a focus group discussions of 7 security experts from Jphiego Corporation 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 validity of the prototype was tested by a team of experts, with results demonstrating that passphrases can enhance

e-commerce security.

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 [13] carried out a research aimed to improve the Mpesa authentication process by incorporating voice biometrics for better user control and efficiency. 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, and 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 [13].

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 fraudulent claims loopholes 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 [14].

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 [15]. 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 [4]. It was, therefore, necessary to conduct this study to identify authentication methods used for ERP systems in Kenyan universities, their vulnerabilities and ways of enhancing secure authentication. This research sought to identify authentication methods used in Kenyan Universities and their vulnerabilities and to suggest ways to improve ERP systems security. It gives insights into the security vulnerabilities facing ERP systems and authentication methods. It will also be beneficial to universities and other organisations and government agencies to enhance the security of their systems.

3. Methodology

The study used an exploratory sequential research design, which involved collection and analysis of both qualitative and quantitative data. The target population for this study was the forty-nine (49) chartered universities in Kenya. The study used a combination of stratified, random and purposive sampling techniques to narrow down to a more specific sample size and target group. Stratified sampling was used to categorize the universities into two strata, namely, private and public universities for subsequent analysis. Random sampling was then used to select Universities to be involved in each strata. Finally, purposive sampling was employed to determine the respondents for the survey. This involved a conscious selection of the participants, who were ICT personnel carrying out system administration-related roles. The Slovin's formula was applied to compute the sample size as shown in equation (1). This was particularly with respect to the determination of the number of Universities to be involved, which in return informed the number of ICT personnel to participate in the survey.

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

Where:

n = Number of samples

N = Total population

e = error tolerance level

The sampling process established a total of twenty-one (21) universities, distributed as thirteen (13) public and eight (8) private universities as computed in (2) and (3), based on equation (1). Thus, this translated to the engagement of a sample of twenty-one (21) ICT personnel carrying out ERP system administration roles in the sample universities.

Public Universities:

$$n = \frac{31}{(1+31(0.21^2)} = 13 \tag{2}$$

Private Universities:

$$n = \frac{18}{(1+18(0.25^2)} = 8 \tag{3}$$

Data was collected through document analysis and a survey using a questionnaire designed in Google forms. The link for the form was shared with the selected participants to fill online. Responses were captured in a file downloadable

in Microsoft Excel format. The study commenced with a pre-study that involved three representative universities to ensure the reliability and validity of the data collection instrument. Data collected from the pre-study was used to compute a Cronbach's alpha coefficient which yielded a value of 0.745. The outcome deemed the data collection instruments to be reliable for use in the main study. During the main study, the data collected was analyzed using Microsoft Excel and the Statistical Package for Social Science (SPSS), where descriptive statistics were used to establish patterns of the data and the relationship between the variables. Both correlation and regression analysis were performed to determine the extends of the effects of independent variables to the dependent variable. Study findings were thus presented in tables and charts as outlined and discussed in the subsequent subsection.

4. Result and Discussion

The findings revealed that 58% of the sampled universities currently use passwords only, 26% use passwords with email verification, 5% use passwords with Windows Domain Authentication, 5% use biometrics integrated smart cards and 5% use 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 study also required respondents to indicate whether there was a need to improve the current authentication method. The respondents unanimously agreed on a need for improving the current authentication method for ERP security. A follow up question sought to determine vulnerabilities to the current authentication methods. The findings are as shown in Fig.1.

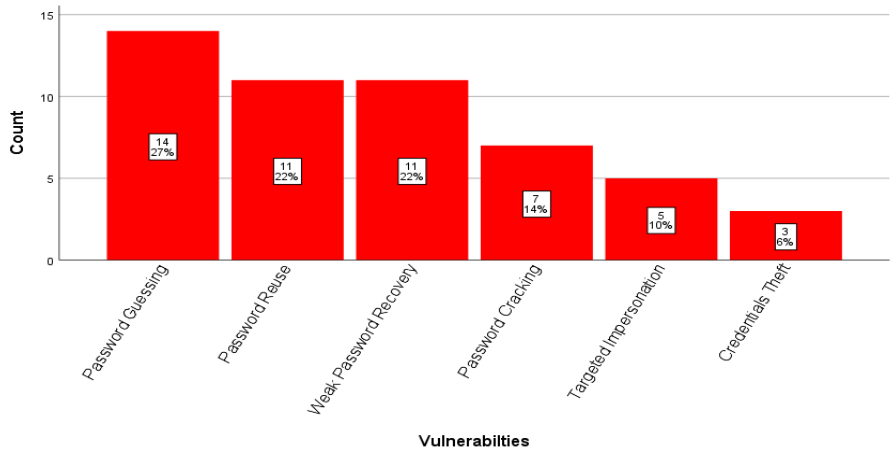

Fig.1. Current Authentication Method Vulnerabilities

The findings revealed that the responses captured included both vulnerabilities and attacks, since this was a an open ended qualitative kind of question. These were therefore analyzed separately in two categories, namely, vulnerabilities and possible attacks that can exploit 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.1. Other vulnerabilities include password complexity, password encryption, default credentials, password masking, hardcoded passwords and code recompilation [16]. These should be addressed by having better control measures in place for the systems.

The vulnerabilities identified in current systems authentication methods may be exploited through various attack techniques resulting in loss or harm. Attacks in this case refer to potential incidents that may cause unauthorized access or transactions. The attacks included social engineering, malware, brute force attacks, denial of service attacks and replay attacks, as summarized in Fig.2. These vulnerabilities with some of their associated attack types were comparable to those identified by Njoroge, Ogalo and Ratemo [15] in a study on information security risks facing Kenyan public universities.

Study findings established that universities have the infrastructure to support improved ERP system authentication. The respective number of universities having particular infrastructure was as follows: Email (18), Biometrics (10) and SMS (10). Respondents indicated that the infrastructure could be open to integration with their institutional ERP systems.

The study further determined that 95% of universities have ICT Security Policies in place, which offered guidance on secure authentication and privacy policies. This is as shown in Table 1. These findings concurred with outcomes of [15], that established security as a vital requirement for universities, and that 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. Furthermore, it was established that user training on ERP Secure Authentication was mostly conducted once during system implementation, at a rate of 50% and often, at a rate of 50%. The level of user training on secure ERP

Authentication was scored as moderate using a Likert scale. This differed slightly from the study by Bett [1], 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.

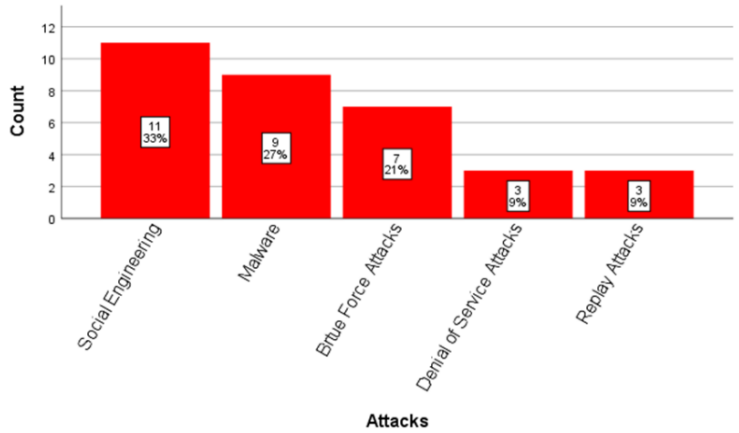

Fig.2. Possible Attacks to the Current Authentication Methods Vulnerabilities

Table 1. 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 study finally sought to find out how ERP systems security can be improved in line with Mayieka [5], who recommended that institutions of higher learning should take a proactive approach to minimize cyber security challenges. The respondents suggested the measures outlined in Fig.3.

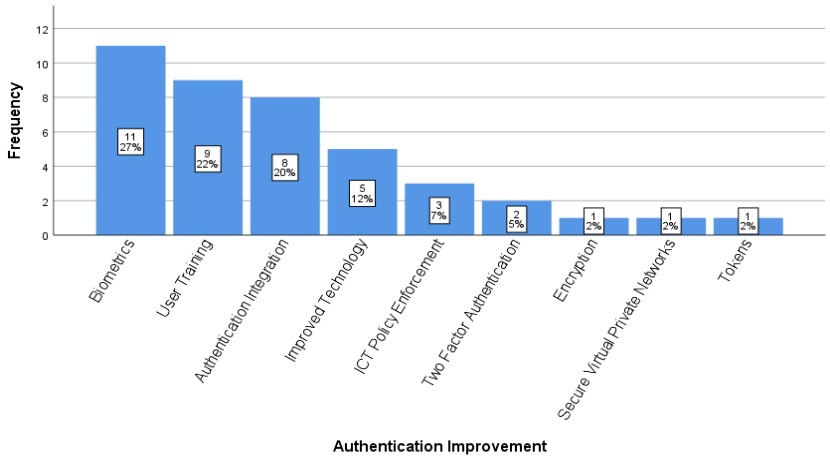

Fig.3. Suggested Authentication Improvement

Based on the survey analysis shown in Fig.3, the use of biometrics was the leading proposed method that could improve ERP security. Based on collected study data, the biometrics technology available was fingerprint-based and smart-card-based biometrics. According to First Identity Online Alliance [3], fingerprint scanning was the most desired authentication feature among consumers. Some notable advantages of fingerprint biometrics include: providing high-security assurance, usability, privacy, non-transferability and being difficult to circumvent. This showed that fingerprint-based biometrics provide an improved authentication method.

Correlation

Pearson Correlation was computed to establish the relationship between the dependent and independent variables of the study. The dependent variables for system authentication were confidentiality, integrity, availability, and usability while the independent variables for improved ERP system security were adequacy of security, authentication mechanisms, infrastructure, information security policies, vulnerabilities, and user training. For the sake of the correlation analysis, a variable called Security Rating was used to represent the set of dependent variables. The independent variables were arrived at based on aspects that influence ERP system security from the Socio-technical Systems and Technology

Acceptance Model theories. The correlation analysis established a strong positive relationship between ERP system security rating and vulnerabilities at 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 Table 2. The prototype framework therefore, factored in vulnerabilities, level of user training and ICT policy components such as password management and user identity to ensure enhanced ERP systems authentication security.

Table 2. Correlations

Variable		Security Rating	Adequacy of Security	Authentication Type	Infrastructure Present	ICT Policy Adequacy	Vulnerabilities	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
Vulnerabilities	Pearson Correlation	0681**	.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 also done using SPSS to establish the relationship between the dependent variable, improved ERP security rating and the independent variables: Level of user training, ICT Policy adequacy, authentication type, infrastructure present, authentication improvement, adequacy of security and vulnerabilities. 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 Table 3 of the coefficients.

Table 3. Model Summary

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

- Predictors: (Constant), Level of User Training, ICT Policy Adequacy, Authentication Type, Infrastructure Present, Authentication Improvement, Adequacy of Security, Vulnerabilities.

Table 4. 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			

- Dependent Variable: Security Rating
- Predictors: (Constant), Level of User Training, ICT Policy Adequacy, Authentication Type, Infrastructure Present, Authentication Improvement, Vulnerabilities, Adequacy of Security

Table 5. Coefficients

Model		Unstandardized B	Coefficients Std. Error	Standardized Coefficients Beta	t	Sig
1	(Constant)	.126	1.632		.077	.940
	Adequacy of Security	-0.70	.172	-.084	-.407	.692
	Authentication Type	.166	.251	.128	.662	.521
	Infrastructure Present	.113	.173	.122	.652	.528
	ICT Policy Adequacy	-.069	.157	-.071	-.441	.668
	Vulnerabilities	.066	.157	.095	.417	.685
	Authentication Improvement	.010	.207	.009	.047	.963
	Level of User Training	.768	.201	.804	3.829	.003

- Dependent Variable: Security Rating

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 outlines in (4).

$$Y=\beta 0+\beta 1X1+\beta 2X2+\beta 3X3+\beta 4X4+\beta 5X5+\beta 6X6+\beta 7X7+e \quad (4)$$

Where Y is the dependent variable (improved ERP security), $\beta 0$ is the constant, $\beta 1$- $\beta 7$ are the regression coefficients. The X's represent the independent variables' factors, while the e represents the error term. The specific independent variables with their associated X's are as follows:

$X1$ = Adequacy of Security
$X2$ = Authentication Type
$X3$ = Infrastructure Present
$X4$ = ICT Policy Adequacy
$X5$ = Vulnerabilities
$X6$ = Authentication Improvement
$X7$ = Level of User Training

In the regression model, the coefficients of the independent variables show that Authentication type, infrastructure present, vulnerabilities, 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 had positive correlation coefficients but resulted in negative beta coefficients. This could be as a result of suppression by the other independent variables. The final predictive model using the forward variable selection regression technique, outlined in equation (5), shows the measure of the influence of the variables on the model.

$$Y = .126 + 0.768(X7) \quad (5)$$

This implies that user training has a positive and the highest effect on improved ERP system security. This matches with findings by Obuhuma and Zivuku [7] where user education/awareness was determined as the most critical factor that could avert social engineering attacks. The proposed multi-factor authentication framework prototype for improved ERP systems security, therefore, is as shown in Fig.4.

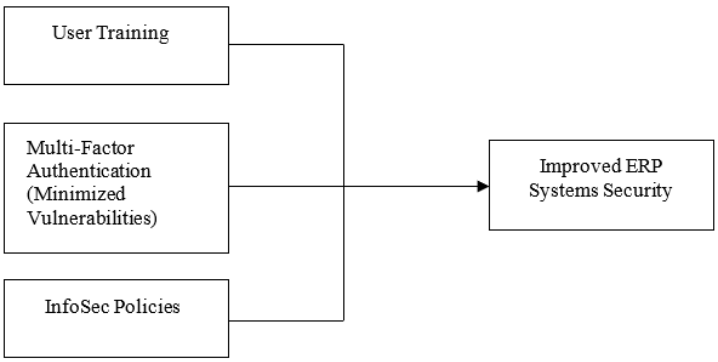

Fig.4. Proposed Multi-Factor Authentication Framework Prototype

Multi-Factor Authentication (MFA) Prototype

This study, therefore, proposes the use of multi-factor authentication comprising of passwords, currently in place, enhanced with 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 of the two factors.

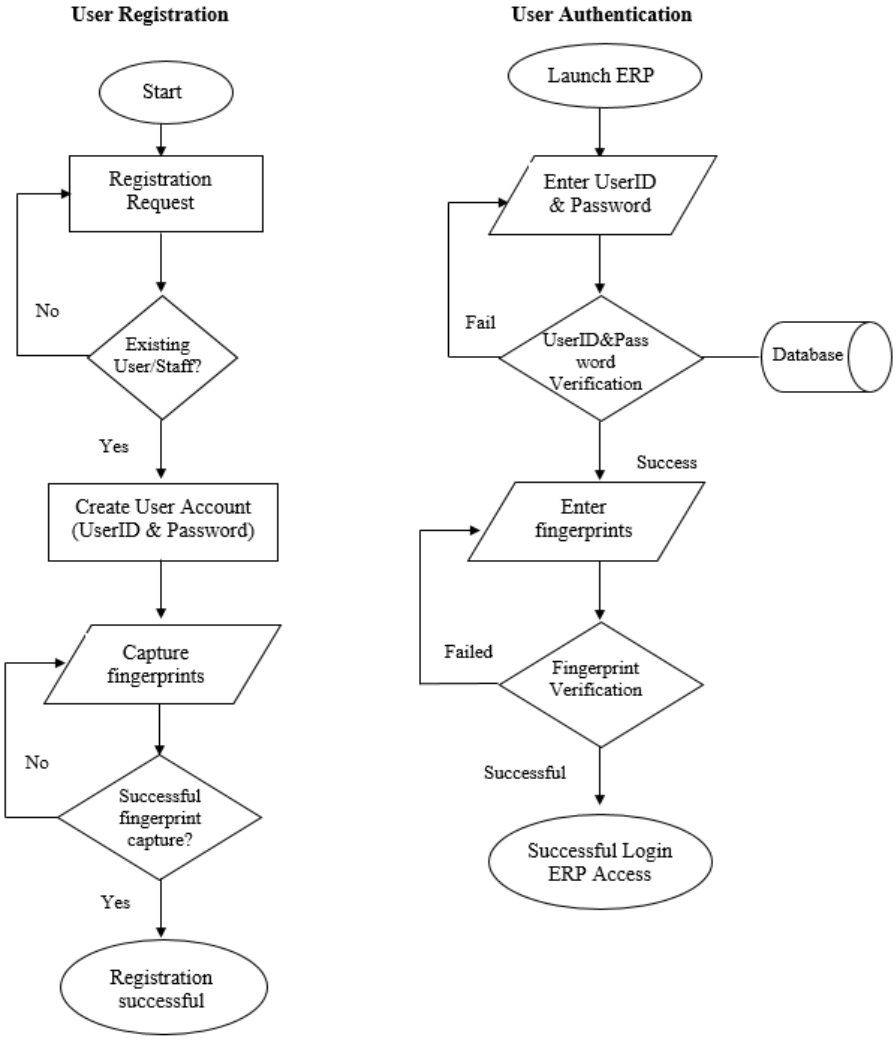

Fig.5. System Flow Charts

A prototype can be perceived as an early version of software that demonstrates concepts, designs and can be used to find out more about the problem and possible solutions. The Rapid prototyping approach was used, entailing the following steps: establishing prototype objectives, defining prototype functionalities, developing the prototype and evaluating the prototype. The prototype was developed using the following tools:

- Hardware: Computer Intel core i5, Digital Persona Biometric Reader
- Operating system: Windows 10
- Software Development Tools: FlexCode SDK, CodeIgnitor
- Relational Database: MySQL
- Web server: Apache
- Programming Languages: PHP

The concept of the proposed prototype takes the following process, which is also as summarized in Fig.5:

- A user is registered by the system administrator, an account created for him/her, password set with fingerprints captured.
- The user accesses the system and lands on the log-in page. He/she logs in by submitting the correct username and password. Once username and password are successfully authenticated, the user enters their fingerprint as 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.
- The user is authenticated/not authenticated, and the transaction is successful/fails.

The prototype with functionalities of user registration, authentication and system activity logs, was developed. Some of the prototype's user interfaces are as shown in Fig.6 to Fig.8.

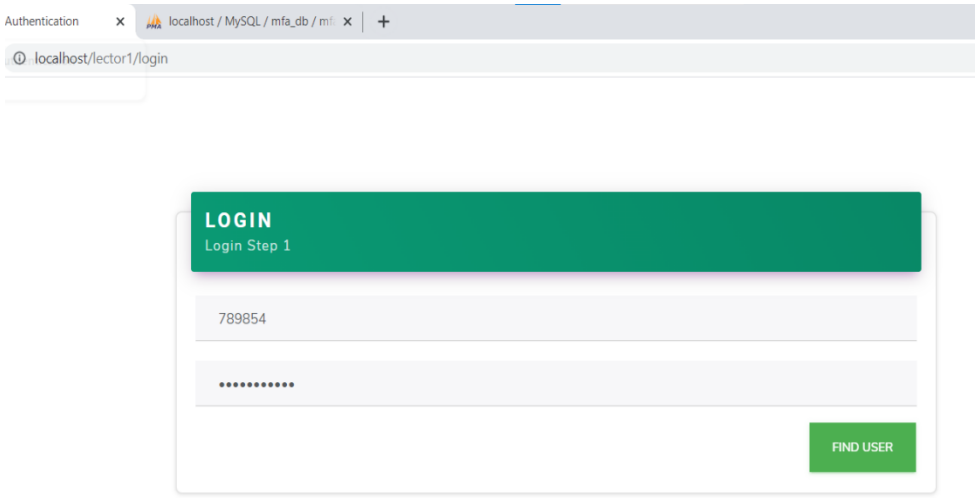

Fig.6. Log in using Multi-Factor Authentication

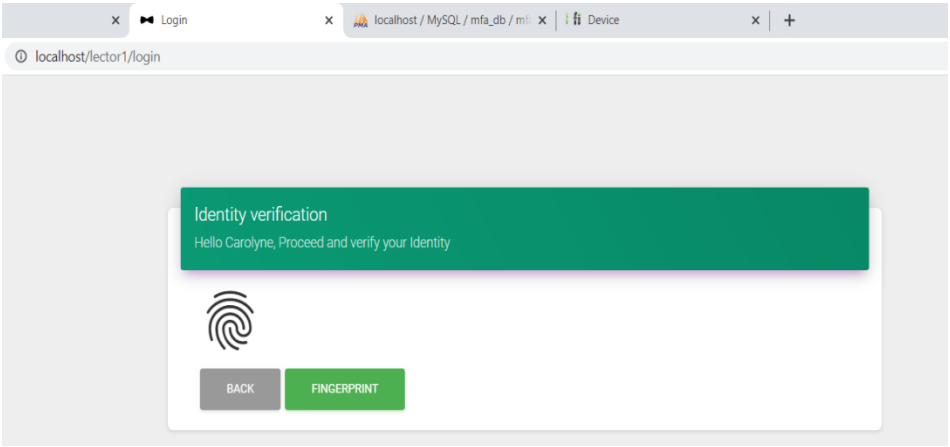

Fig.7. MFA Prototype Login Step 1 for Password and Fingerprint Option

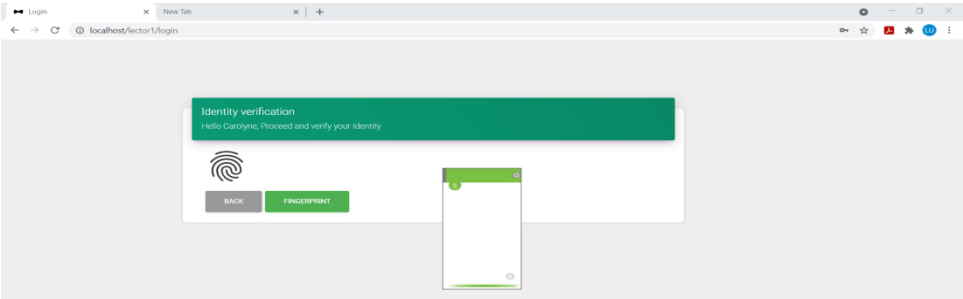

Fig.8. MFA Prototype Login Step 2 with Fingerprint Verification

The prototype was then 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 appropriately, hence providing a guarantee for improved ERP systems security.

In summary, the study was carried out to establish current authentication methods with their associated vulnerabilities, and to develop and validate a multi-factor authentication prototype for improved ERP systems security, using a case of Universities in Kenya. The findings were as summarized in Table 6.

Table 6. Summary of Findings

Objective	Findings
1. To identify ERP systems authentication methods.	▪ 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.	▪ Identified vulnerabilities were 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. ▪ Use of multi-factor authentication is proposed to improve ERP systems security.
3. To develop and validate a multi-factor authentication framework prototype for improving ERP system security.	▪ A Multi-factor authentication prototype using a combination of password and biometrics was developed to improve ERP systems security for Kenyan Universities. ▪ The prototype was tested by use of test cases, unit, functional and system testing. ▪ Successful test results was an indicator of guaranteed improved ERP system security.

5. Conclusions

Authentication is a crucial area in systems security with risks that should be mitigated. The study identified passwords as the most common authentication method used for ERP systems in Kenyan Universities. Unfortunately, the password method requires enhancement, due to its vulnerabilities such as password guessing, password reuse, and weak password recovery, among others. These vulnerabilities make ERP systems prone to various forms of attacks, including, brute force attacks, replay attacks, social engineering, malware and denial of service attacks, among others. The results of this study show that ERP system authentication can be improved by enhancing user authentication through the use of multi-factor authentication.

The study in a bid to improve ERP systems security proposed a framework for secure ERP systems authentication coupling effective user training, enforcement of ICT security policies, and multi-factor authentication to address authentication level vulnerabilities and cyber-threats. A multi-factor prototype combining passwords and an additional layer to authentication using fingerprint-based biometrics was hence developed and validated to improve ERP systems security for Kenyan Universities and other organizations. Its adoption and implementation could lead to enhanced system security, with respect to vulnerabilities and attacks to the current password-based authentication method.

Systems security is a key area that organizations must invest in. Organization are recommended to consider implementation of the proposed enhanced authentication framework. The main significance of this study can be viewed in two perspectives: first, real vulnerabilities and potential attacks to ERP systems have been singled out and discussed. Secondly, an enhanced authentication framework has been proposed, prototyped and tested. Thus, outcomes of the study will be beneficial to Universities in Kenya and worldwide, other private and public organisations, and government agencies towards enhancing the security of their systems.

Further research should focus on: the implementation of phone-integrated authentication, addressing other systems security issues that go beyond authentication, and implementation of other biometrics authentication for improved ERP systems security.

References

[1] 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). "doi:10.18535/ijsrm/v6i2.em01"

[2] Ziani, D., & Al-muwayshir, R. (2017). "Improving Privacy and Security in Multi-Tenant Cloud ERP Systems." 8(5), 1–15. "doi:10.5121/acij.2017.8501"

[3] First Identity Online Alliance. (2019). "The-State-of-Strong-Authentication-2019" Report.https://media.fidoalliance.org/wp-content/uploads/2019/01/The-State-of-Strong-Authentication-2019-Report.pdf

[4] Serianu. (2020). "*Africa Cyber Security Report" 2019/2020*. 1–104. https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

[5] Mayieka, J. M. (2019). "Emerging Issues in Cyber Security for Institutions of Higher Education." International Journal of Computer Science and Network, 8(4).

[6] Alhakami, H., & Alhrbi, S. (2020). "Knowledge-Based Authentication Techniques and challenges." International Journal of Advanced Computer Science and Applications, 11(2), 727–732. https://doi.org/10.14569/ijacsa.2020.0110291

[7] Obuhuma, J., & Zivuku, S. (2020). "Social Engineering Based Cyber-Attacks in Kenya". 2020 IST-Africa Conference, IST-Africa 2020, 1–9.

[8] Akif, O. Z. (2017). "Secure Authentication Procedures Based on Timed Passwords, Honeypots, Honeywords and Multi-Factor Techniques."

[9] Velasquez, I., Caro, A., & Rodiruez, A. (2019). "Multifactor Authentication Methods: A Framework for Their Comparison and Selection." InTech Open Computer Network and Security." doi:10.5772/intechopen.89876

[10] Ting, D. M. T., Hussain, O., & LaRoche, G. (2016). "Systems and Methods for Multi-Factor Authentication" (Patent No. US 9,118,656 B2).

[11] 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. doi:10.35940/ijrte.C4458.099320

[12] Odera, S. (2016). "Integrating Passphrases as an Authentication Mechanism in E-Commerce.", United States International University, Kenya, 2016.

[13] Chetalam, L. (2018). "Enhacing Security of M-Pesa Transactions by use of Voice Biometrics." United States International University, Kenya, 2018.

[14] 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

[15] 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, 1–19.

[16] Miessler, D. (2021)."The Consumer Authentication Strength Maturity Model (CASMM) v5." https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model/

Authors' Profiles

Carolyne Wanjiru Kimani holds a Master of Science in Applied Information Technology from Africa Nazarene University and Bachelor of Science in Information Technology from Jomo Kenyatta University of Agriculture and Technology (JKUAT). She is currently an ICT Officer in the Department of Computing and Informatics – ICT Section, at Laikipia University, Kenya. She is currently working in the Systems Office of the department. Her research interest is in Information Systems Security. This research was undertaken for her Master of Science in Applied Information Technology at Africa Nazarene University.

Dr. James Obuhuma holds a PhD in Computer Science from Maseno University, Kenya, with a specialty in Intelligent Systems. He also holds an MSc in Computer Science from the University of Nairobi, Kenya, and a BSc in Computer Science and Technology from Maseno University. He is currently a member of faculty and current coordinator of Postgraduate Studies, Department of Computer Science, Maseno University, Kenya. His research interest is in the application of intelligent systems in different fields. Dr. Obuhuma is also a certified Cisco Cybersecurity Ops instructor, and a certified IBM Web Application Security and IBM Security Intelligence instructor. Apart from the Computing and Informatics field, he is also a Design Thinking coach. He is part of the Impact Week group that fosters entrepreneurship and innovation through building of sustainable business models. Dr. Obuhuma was the main masters research supervisor to Carolyne Wanjiru Kimani.

Dr. Emily Roche holds a PhD in Biostatistics from Moi University, an MSc in Statistics and a Bed in Double Mathematics from Kenyatta University. She currently facilitates the learning of mathematics at Africa Nazarene University doubling up as a mentor and advisor to the learners. Her greatest research interest is in statistical modelling and in the facilitation of learning is to demystify mathematics. Professionally she is a member of International Biometric Society and Kenya National Statistical Society. Dr. Roche was the second masters research supervisor to Carolyne Wanjiru Kimani.

How to cite this paper: Carolyne Kimani, James I. Obuhuma, Emily Roche, "Multi-Factor Authentication for Improved Enterprise Resource Planning Systems Security", International Journal of Information Technology and Computer Science(IJITCS), Vol.15, No.3, pp.42-54, 2023. DOI:10.5815/ijitcs.2023.03.04