Computer and Information Science; Vol. 15, No. 2; 2022
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Survey of Biometric Authentication Technologies Towards Secure And Robust Systems: A Case Study of Mount Kenya University

Boniface Mwangi Wambui[1,2], Joyce W Gikandi[1], & Geoffrey Mariga Wambugu[3]

[1] School of Computing and informatics, Mount Kenya University Thika, Kenya

[2] Department of ICT & Engineering, Zetech University, Ruiru, Kenya

[3] School of Computing and Information Technology, Murang'a University of Technology, Murang'a, Kenya

Correspondence: Boniface Mwangi Wambui, Department of ICT & Engineering, Zetech University Ruiru, Kenya.

Received: January 21, 2021 Accepted: March 4, 2022 Online Published: March 17, 2022

doi:10.5539/cis.v15n2p43 URL: https://doi.org/10.5539/cis.v15n2p43

Abstract

In response to the increased demand for more effective authentication methods, the usage of biometric authentication to secure systems against unwanted access has grown. Because of the recent COVID-19 pandemic outbreak, any direct physical contact with the system should be avoided. Furthermore, current authentication systems lack the necessary security features, making them vulnerable to cyber risks such as forgery by unethical employees and unauthorized users. The goal of this paper is to investigate the existing biometric authentication systems and propose the best security models to overcome the weaknesses of existing technologies. The study employed mixed methodology, which was qualitative and quantitative in nature and relied on primary and secondary sources of data. The researcher collected the data from a population of 300 staff of Mount Kenya University with a sample size of 169 respondents. The R2 value on the relationship between the studied dependent and independent variables was R2 = 0.792 showing a good fit of the model since is greater than 50% of the test item used in the case study. Therefore the study recommends that institutions to implement a contactless biometric system to eliminate physical contact and use multimodal system that will help overcome the existing challenges associated with unimodal systems. There are still gaps for future researchers where they need to focus on the various decision algorithms that are best efficient in verifying users before they are authenticated in the system.

Keywords: security, integrity, contactless, biometrics, authentication systems, model

1. Introduction

The goal of this research was to look at existing biometric authentication solutions at higher education institutions to see how they might increase system robustness in terms of safe authentication and system integrity. The researcher utilized the findings to make recommendations for improving security mechanisms and safety in higher education institutions. To increase authentication accuracy and other relevant quality indicators, many biometrics authentication systems have been developed. Traditional methods, punch cards, QR codes, RFID, and biometrics are among the present solutions. The current biometric systems consists of fingerprint, palm vein recognition, iris recognition, and hand geometry, face recognition and voice authentication systems. Because they eliminate the need to learn long passwords and carry tokens, biometric systems are more convenient to use than traditional authentication techniques such as token-based (e.g., ID cards) or knowledge-based (e.g., passwords).It also protects the user from retaliation. Personal authentication systems based on biometrics can function in two modes: identification and verification, (Mwema, 2015).

Identity theft, spoofing and reliability of authentication tools in institutions of higher learning are some of the key problems that compromise system integrity and deprive quality service delivery. The students and employees of the institution who utilize the biometric system to clock in to access services are the target population. When the system users try to clock in, the system is unable to authenticate their information. The biometric system also has a high False Rejection Rate. Such problems demonstrate the biometric system's inefficiency and ineffectiveness, which puts the system's integrity at risk. A range of characteristics and application areas influence the success or failure of a biometrics system. One of the solutions that can be used to overcome the

difficulties outlined is contactless authentication. (Martin, 2007).Due to virus transmission via surfaces and physical contact, the present biometric system has been underutilized since the advent of the covid-19 pandemic. Moreover, unauthorized individuals have drugged users or applied social engineering tactics, particularly targeting those in charge of systems, databases, and servers, and recorded their fingerprints. They're then utilized to create fake fingerprints that can be used to log into computers. Because the information can be manipulated, the integrity and security of the data might be jeopardized, resulting in inconsistencies and data loss. This manifests the inefficiencies and challenges that can affect quality of system operations and service delivery. Integrated system theory was considered in this research. The research objective was to investigate the effectiveness of existing biometric authentication systems in higher learning institutions.

The main contributions of the paper were:

- Developing a contactless security model that can enhance more access integrity in biometric systems especially during COVID-19 era.
- Providing the extent of biometric usage in Higher education Institutions towards developing robust security systems.

This paper contains the following section, introduction, literature review, methodology, research design, hypothesis, inclusion and exclusion criteria, study populations, sampling procedure, data collection tools, location of the study, reliability and validity of the instruments, data analysis, ethical considerations, results, discussions, limitations of the study, conclusion and future work.

2. Literature Review

Biometric authentication, which is now displacing conventional authentication methods such as passwords, has piqued the interest of both researchers and practitioners. Because user activity patterns may be easily identified, this is the case. These human characteristics are difficult to duplicate or forget, making them useful for identification. Face, fingerprint, iris, and voice recognition, for example, can rapidly identify people during authentication, preventing unwanted access. Biometric technology, according to Tekade and Shende (2017), can solve personal identification security concerns in a variety of critical application sectors. When using multiple forms of personal identity to verify users, Parkavi (2017) emphasize the importance of biometrics. The necessity of user authentication mechanisms for cloud photo authentication is explored by Kakkad (2019).

Unimodal biometric technology, according to Kakkad (2019), has a number of drawbacks, including noisy data, intra-class discrepancies, a limited degree of freedom-anti-universality, spoof assaults, and low mistake detection. Implementing multimodal biometric systems that include data from multiple sources can help to overcome some of these challenges. Some of these issues can be addressed by implementing multimodal biometric systems that incorporate data from many sources. In these circumstances, attempting to increase individual match performance will be futile due to the inherent difficulties, (Ahmad , 2012). By giving several proofs of the same identification, multi-biometric systems tend to reduce some of these limitations. These technologies help generate efficiency gains that would be impossible to obtain with a single biometric system. Anti-faking features in multi biometric systems make spoofing many biometric traits at the same time impossible. However, numerous domain experts believe that an effective fusion approach is needed to integrate the data (Solayappan & Latifi, 2006). A person's biometric traits are discreet and unique when it comes to biometrics, (Ahmad, 2012). Some of these traits are tough to imitate. These are, in theory, the best controls. However, there are a number of issues that arise when using biometric recognition. Biometrics have never been more advanced, intricate, or sensitive than they are now. They're utilized to keep citizens and businesses safe. Above all, biometrics is concerned with a person's unique biological characteristics that cannot be reproduced, (Thakur & Vyas, 2019).

2.1 Types of Biometric Systems

Voice Recognition- The voice has behavioral and physiological features based on the makeup of the throat and mouth, as well as movement components. Both the speaker and the content of what is being spoken can be identified via sound. A voiceprint is a visual representation of language that may be measured in terms of frequency, length, and amplitude. Despite the fact that both rely on human speech, most systems employ both speaker and voice detection. However, they serve different purposes and are implemented differently. Speech recognition is popular and inexpensive, but it is less accurate and takes longer to authenticate a user (Abozaid, 2019).

Iris recognition- The iris is a flexible, thin, and colorful circular connection. The size and diameter of the pupil are controlled by this tissue. The pupil controls how much light gets into the eye. Each person's iris is distinct, even if they are twins. The cornea protects the iris, which is visible from the outside. Because the iris can be

seen from a few meters away, iris scans are less invasive than retina scans. The iris is a light-sensitive organ that can give significant secondary verification (Dua, 2019).

Fingerprint verification- Because everyone's fingerprints are unique, fingerprint identification is one of the oldest, most powerful, most commonly utilized biometrics. It recognizes and certifies a person's identity using data saved in advance, as does all biometric technologies. Among the techniques employed are electrical, capacitive, thermal, and others. A biometric model is created utilizing numerous advanced, person-specific algorithms once the collected human fingerprint picture is altered to make it accessible (Ali, 2016). To prevent image fluctuation caused by fingerprint captures, Engelsma et al. (2018) presented solutions to improve fingerprints in the future. As an option to improving image variability, they proposed a universal 3d fingerprint target. The extraction of sweat glands, which is based on cell locations, can also be used to improve 3d fingerprint resolution. Valdes-Ramirez et al. (2019) looked at fingerprint features to see if they could use minutiae to detect latent fingerprints. Makhija et al. (2017) looked into the performance of various latent fingerprint systems and found places where they may be improved.

Ear authentication- Physiological biometric properties are represented by biometric elements of the outer ear (a biological pinna). Sound waves are utilized to determine the ear canal. The form of the human ear canal is unique, just like fingerprints or the iris. Ear authentication also necessitates the use of external devices. An earpiece with a microphone picks up sound waves from the ear canal and sends them to the device (Nakamura et al., 2017).

Palm vein technology- Internal body vein properties are used in the technique. This distinguishes them from each other, even if they are identical twins. The risk of infection is lessened because users do not have to touch the scanner. It's difficult to cultivate these qualities. The distinctive blood vessel pattern discovered beneath the skin surface of the human finger is the basis for this technique. The vein pattern is extremely difficult to recreate since it is hidden beneath the finger tissue and can only be validated using specialized equipment. (Shaheed, 2018).

2.2 Cancelable Biometrics

The notion behind cancelable biometrics is that the original template data is transformed into a new version throughout the enrollment process using a non-invertible transformation function. During the verification stage, the same non-invertible transformation is applied to the query data. To match the altered template and query data, the domain is changed. Ratha (2007) developed three transformation functions: Cartesian, polar, and functional. The suggested modification techniques modify the original features on purpose, making obtaining raw template data impractical or computationally expensive. The proposed technique has one disadvantage: it is based on registration, which necessitates effective unique point detection. Because of biometric ambiguity, reliable registration is usually difficult. Wang (2018) used random projections to develop a cancelable fingerprint template.

Thanks to the feature decorrelation technique, the developed template can fend off record multiplicity attacks. Meanwhile, the technique generates a Delaunay triangulation-based local structure that can mitigate the negative impacts of nonlinear distortion on matching performance.

Sandhya and Prasad (2017) used a random projection based cancelable protection technique to combine two structures at the feature level, local and distant structures, to yield binary-valued features. Some academicians advocated for the use of multimodal cancelable biometrics to further improve security and recognition. To increase recognition accuracy and security, Yang et al. (2018) proposed a multimodal cancelable biometric system that incorporates fingerprint and finger-vein data. To achieve non-invertibility and revocability, the suggested system employs an enhanced partial discrete Fourier transform.

In order to overcome constraints in each modality independently, Dwivedi and Dey (2018) developed a hybrid fusion (score level and decision level fusion) technique that includes cancelable fingerprint and iris modalities. Multimodal cancelable biometric systems surpass their unimodal counterparts in terms of performance, according to experimental evidence.

2.3 Biometric System Attacks

The direct attack surface takes place on the surface thus does not require any algorithm. The attacker does not need to know anything about the system. They consist of sensor assaults, which, unlike direct attacks, require knowledge of the authentication system's inner workings in order to be successful. According to Jain (2004), Biometric-based applications are subject to a variety of attacks, which can be divided into two categories: direct and indirect attacks. Due to Covid 19 outbreak the fingerprint system has been rendered useless due to the

physical contact with the sensor that is prone to direct attacks. The solution for this type of attack is using the contactless security system such as pal vein for both registration and authentication.

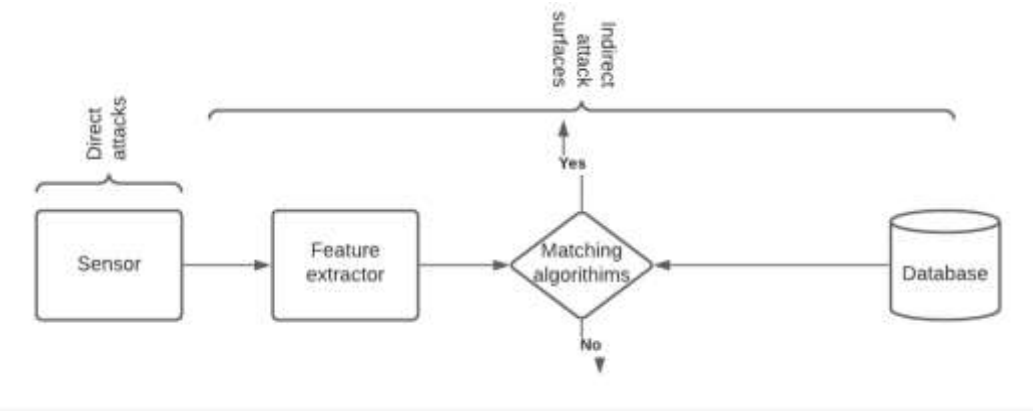

Figure 1. attack surfaces of biometric systems

Fig 1 above demonstrates the attack vectors of biometric systems. Most of the attack takes place between the sensors to the database while direct attacks only occur on the sensor module.

Table 1. Types of attacks on biometric systems

Type of Attack	**Attack surface**	**Counter Measures**
Direct Attacks	Attacks on the Sensor module such as spoofing attacks. eg fake biometrics	• Liveness detection
Indirect Attacks	Attacks on the software modules	• Use strong tested algorithms
	Attacks on the database template through modifying existing templates such masquerade attacks	• Sign templates, Store encrypted templates •
	Attacks on the interface between the modules such as the replay attacks.	• Transmit data over encrypted path/secure channel • Mutually authenticate/use symmetrickey or Asymmetric key
	Attacks on the feature extraction module through intercepting the communication between the sensor & extraction module. -Trojan horse attacks	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data
	Attacks on the matching module through intercepting communication channel between matcher module and application device such Hill climbing attacks.	• Use strong tested biometricalgorithms • Multibiometric/multifactor
	Attacks through intercepting the communication channel between system database and matcher module.	• Secure channel • Mutual Authentication

2.4 Biometric Features

Table 2. Features to consider for biometric security

Type of biometric systems	**Features**
Fingerprint	High FAR, Medium accuracy, Low security, Medium speed, Medium template, Low cost and Physical access
Finger vein	Contactless access ,High security, low speed
Palm vein	Low FRR, High accuracy, High security, Low speed, Large template, High cost and Contactless access
Face recognition	Contactless access, High cost
Iris recognition	Contactless access, High cost, High accuracy, fast

2.5 Criteria for Biometric Security

The criteria to select the suitable biometric systems in any organization depend on some factors such as universality, acceptability, permanence, performance and the uniqueness and circumvention.

Table 3. Criteria for biometric security system selection

Type of biometric systems	**Criteria for selection**					
	Universatility	**Acceptability**	**permanence**	**Performance**	**Uniqueness**	**circumvention**
Fingerprint	Medium	Medium	High	High	High	High
Palm vein	High	High	High	High	High	low
Voice	medium	High	low	low	low	low
Face recognition	High	High	Medium	low	low	low
Iris recognition	High	Low	High	High	High	high
Hand geometry	Medium	Medium	Medium	Medium	Medium	Medium
Keystroke	High	High	low	Medium	low	high

From the table above it is very evident that the fingerprint, keystroke and iris recognition circumvention is high thus the traits can easily be imitated by using a substitute or an artificial artifact which makes the authentication system vulnerable.

2.6 Balance between Security, System Performance and Usability in Universities

A biometric system detects whether or not a user is authentic. It leads to a system usability and security test. FAR and FRR are both dependent on a threshold value, as evidenced by this. The decision threshold should be flexible enough to accommodate the application's desired security features. In some applications, a high FRR rate is a vital system design need, whereas in others, a high FAR rate is a fundamental system design requirement (Gregory & Simon, 2008). High-security apps have a low FAR, which causes FRR to rise, whereas low-security applications have a low FAR. The biometric performance level creates several obstacles when using biometric technologies and systems. According to Harinda and Ntagwirumugara, (2015), Universities in Rwanda must take into account that the biometric system's ability to alter authorization varies depending on the system's sensitivity to the threshold value. Adjustments to reduce system threshold values to deal with tolerance to input variations in students' environments may be necessary, and this will increase FAR, implying that the system can easily grant access to unauthorized students or staff, whereas increases in system threshold values to make the system more secure will increase FRR, implying that the system may deny access to even authorized students or staff.

According to Patrick (2008), Social and human issues, notably the system's use and adoption, will be critical. The service is likely to fail if people have problems using it or refuse to accept it. Most colleges prioritize usability and performance over security, relying on the assumption that the system is secure. There is a link between biometric accuracy and usability. The most accurate technologies, such as iris and retina recognition, are also the least useable. On the other hand, the most practical systems, such as speech and facial recognition, are also the least accurate. Fingerprint systems are known for their reasonable accuracy and usability.

3. Methodology

The study employed mixed methodology, which was qualitative and quantitative in nature and relied solely on primary and secondary sources of data. Combining data sets can help investigators obtain a deeper grasp of the problem and produce more thorough evidence, giving them both depth and breadth. Quantitative approaches provide objectivity, whereas qualitative methods explain a specific study phenomenon. The core concept is that combining quantitative and qualitative methodologies allows for a more comprehensive and synergistic use of data in solving research problems and understanding complicated phenomena than either strategy alone,(Fetters & Freshwater, 2015). In addition, focus on current literature-based comparative analysis that relied on previous research evidence enabled the researcher to collect more relevant information to the study's scope and deduce knowledge from these sources in order to present a new theoretical perspective in the field of knowledge, particularly in terms of the utility of various biometric systems. By triangulating secondary and primary data using both qualitative and quantative techniques, one can gain a better understanding and improve the validity of inferences.

With respect to the methodological approach the researcher achieved the objective by using the research tools to obtain data from the respective area of study. For selection of digital libraries several factors were considered such as value or quality of the materials that were rich on content under study and features contained that enabled high level of success. According to this article it was possible to cover all the digital libraries but the selection process considered the two major factors.

3.1 Research Design

An experimental research design was used in this study. It is the overarching technique used to combine the many aspects of a study in a logical and coherent manner, allowing it to effectively address the analysis, (Polit &

Hungler, 1999). This study used experimental research to identify the characteristics of an observed phenomenon or to investigate possible relationships between two or more phenomena. The experimental research was appropriate since the researcher conducted the experiment with a control group, altering the variables and observing the effects. Experts validated the generated model based on the experiment results. As part of this study, the researcher focused on the university's staff and students in regards to biometric systems.

3.2 Hypothesis

H0: The contactless security model enhanced the integrity of data in Higher Education

Institutions.

H1: The contactless security model did not enhance the integrity of data in Higher Education Institutions.

3.3 Inclusion and Exclusion Criteria

3.3.1 Inclusion Criteria

The research included the teaching and non-teaching members and students of Mount Kenya University from the selected departments.

The research included digital libraries from institutional repositories, digital archives**,** library collections and digital preservations.

3.3.2 Exclusion Criteria

The research excluded workers who are not part of the university fraternity.

The research excluded other materials that were not included in the digital libraries selected.

3.4 Study Populations

According to Mugenda & Mugenda (2003), population refers to the total number of people living in a certain region under study. Because the study's population will be deemed finite, data quantification will be done using a numerical measuring scale before instrumentation and collection. The researcher had 300 employees, all of whom were related to the study's issue. The study was conducted in Mount Kenya University. The study was ideal since the University had been using biometric technology for several years.

Table 4. Target Population and Sample Size

Target Type	Population	Sample size
Teaching & Non-Teaching Staff	300	169
Total	300	169

Source (Mount Kenya University MIS, 2021)

3.4.1 Sampling Technique

Sampling approaches provide a set of processes that allow a researcher to maximize the amount of data needed by evaluating data from a unit or a sub-group rather than the entire possible elements, (Saunders, 2016). For this investigation, the stratified random sampling approach was utilized to produce a diverse population since it increased the representativeness of the sample by lowering sampling error. The strata to be considered were the university's teaching and nonteaching workers.

3.5 Data Collection Tools

The data was gathered by the researcher via questionnaires given to students and staff. The majority of the questions were designed and sought to cover the document's objectives. It required the use of both open and closed structured surveys by both staff and students. There were two types of questionnaires used: one for staff and one for students. Observations were also made as part of the investigation to understand what was going on with the current fingerprint biometric technology.

3.6 Data Collection Procedures

To achieve the study's objectives, the researcher used the data collection methods available to him. Each question in the survey was designed to address a specific goal. The researcher applied for a research permit from the school of postgraduate Information Technology department after successfully defending the project at the departmental and school levels. This allowed the researcher to apply for a data collection permit from the National Commission of Science, Technology, and Innovation (NACOSTI). The researcher then sought permission from the research institution. The questionnaires were then given to the responders and collected later by the researcher for analysis.

3.7 Validity of the Instruments

A validity test can determine what a questionnaire is supposed to gather, (Newing, 2011). It captures the inconsistencies or discrepancies between reality and explanations. The content validity of the study was confirmed by experts who were familiar with biometric systems and their performance. The experts expressed their opinions on whether the tools were appropriate. The supervision by the supervisors was critical in addressing all the concerns that arose during the pilot study . The content validity of the instrument was evaluated with the help of a research specialist and the research supervisors. The content was chosen and included in the questionnaire because it was related to the variable being researched for a research instrument to be declared valid. With a randomly selected sample, the researcher conducted a pilot test on the equipment.

3.8 Reliability of the Instruments

According to Jack and Clarke (1998), reliability is defined as the consistency with which research questions are answered. Cronbach's Alpha was used to determine whether the instruments were reliable on a scale of 0 to 1. A value that is closer to one than 0 indicates a high level of reliability. Nonetheless, the study utilized a reliability threshold of 0.7, with a coefficient below 0.7 indicating that the sub components were not trustworthy in capturing the variable. 10% of the sample size was examined to guarantee that the questionnaire was efficient and effective. The questionnaire was entirely completed by twenty (20) randomly chosen respondents, and reliability was tested which was at 0.78.

3.9 Ethical Procedures

The informed consent letter was read and signed by all participants in this study. The study's aims were explained to them. The researcher gave the correspondents a thorough explanation of the study's goals so that they could give their consent. They were told that their responses to the items on the data collection instruments would be kept private. The responders were told that once the report was finished, they could request a copy. The researcher got an introduction letter from Mount Kenya University in order to introduce the research to the respondent and the appropriate authorities. Experts and other scholars were consulted for any health or ethical issues that could be related with palm vein technology. The researcher got a research authorization from the National Commission of Science, Technology, and Innovation (NACOSTI) to collect the data. The researcher then sought permission from the research institution. The questionnaires were then given to the responders and collected later by the researcher for analysis.

4. Results

4.1 Data Analysis

The study's descriptive statistics were generated using primary data that was collected, edited, and analyzed. In addition, a regression model was used to establish the association between the variables using secondary data. To establish the degree of link between the variables, the regression model and correlation analysis were used in the study. The new security model was effective in boosting data integrity, as evidenced by a strong positive correlation of 0.792.

The following is a multivariate regression equation that will be used:

$$Y=\boldsymbol{\beta}0 + \boldsymbol{\beta 1}\ X1 + \boldsymbol{\beta 2}\ X2 + \boldsymbol{\beta 3}\ X3$$

Tests of statistical significance was used to address the question of whether or not the relationship between two or more variables is caused by mere chance or not. The analysis addressed the issue of relevance of relationship by assigning a probability that the model show the relationship between the variables. ANOVA was used to test whether the proposed model was suitable with a test of significance of 95% confidence level.

The following results were obtained

Table 5. Types of Biometric systems used by respondents

Which biometric technologies have you used before

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	only one(Finger print)	84	68.3	68.3	68.3
	several Total	39	31.7	31.7	100.0
		123	100.0	100.0	

Source (Field data, 2021)

Table 5 above showed that a high percentage of respondents have used only one type of biometric system which is finger print which attributes to 68.3%.From the usage, some have used more than one type of biometric systems which might be a combination of either fingerprint and voice recognition or fingerprint, face recognition and iris. This attributed to 31.7%.From this the researcher concluded that the most common, cheap and easily available biometric technology is the fingerprint.

Table 6. Weaknesses of biometric systems

Will the proposed palm vein security technology help to enhance the data integrity in service delivery?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	103	83.7	90.4	90.4
	No	8	6.5	7.0	97.4
	Not Sure	3	2.4	2.6	100.0
	Total	114	92.7	100.0	
Missing	System	9	7.3		
Total		123	100.0		

Source (Field data, 2021)

Table 6 above demonstrates the respondent's feedback concerning the weakness of biometric systems.83.7% agreed that the proposed contactless security systems will solve the problems and enhance the integrity of data in service delivery. 6.5% suggested that the proposed security system will not enhance any integrity.2.4% were not sure while 7.3% of the respondents never gave their response. Based on that analysis it was evident that the proposed security model would solve the current security problems.

Failure of biometric systems in authentication

Table 7. Biometric system authentication

Is there a scenario when the current biometric system had failed to authenticate you?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	73	59.3	60.3	60.3
	No	48	39.0	39.7	100.0
	Total	121	98.4	100.0	
Missing	System	2	1.6		
Total		123	100.0		

Source (Field data, 2021)

Table 7 above shows that 59.3% of the respondents had encountered a scenario where the current biometric system had failed to authenticate the users. This happened when the staff were trying to access the university premises and also during lecturer clocking. Other users were denied access when they were trying to access the control rooms. 39% of the respondents never encountered any authentication problem while 1.6% of the respondents never gave out their response. These authentication problems occurred when a user placed their finger in the sensor but it failed to verify the user's credentials by comparing the data stored in the database template. The areas where biometric systems were used in the university consisted of library access, student registration, student class attendance, student exam attendance, lecturer clock in, accessing the control rooms and accessing directorate of exams office.

Regression Results on investigate the effectiveness of existing security systems in Higher learning institutions

A linear regression was performed to investigate the existing security systems in Higher learning institutions. The following multiple linear regression was formulated. The findings are presented in model summary, ANOVA and regression coefficients.

Table 8. Model Summary on the investigate the effectiveness of existing security systems in Higher learning institutions

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.319[a]	.792	-.032	1.41772

Source (Field data, 2021)

As the model summary in Table 8 above reveals, the R^2 value on the relationship between the studied dependent and independent variables was $R^2 = 0.792$ showing a good fit of the model since is greater than 50% of the test item used in the case study.

Table 9. ANOVA on the investigate the effectiveness of existing security systems in Higher learning institutions

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18.397	12	1.533	.763	.686[b]
	Residual	162.805	81	2.010		
	Total	181.202	93			

Source (Field data, 2021)

From the model summary above it indicated an F-value of 0.763 at (12, 81) which is less than the table value is 1.95, hence we fail to reject the null hypothesis that there was statistical significance between the existing security systems and the Higher learning institutions.

Table 10. Suitable authentication system from the experiment

From the experiment, which technology was better?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Fingerprint	1	6.7	6.7	6.7
	Palm vein(contactless)	14	93.3	93.3	100.0
	Total	15	100.0	100.0	

Source (Field data, 2021)

According to table 10 above, 93.3% of the participants suggested that the palm vein (contactless) was better than the current fingerprint system which was at 6.7%.Most of the participants selected the palm vein since it was not affected by wearing out of the palm as compared to the fingerprint where users who had worn fingers, muddy fingers and wet fingers were no longer registered or authenticated by the system.

Table 11. Likert scale from the control group

Scale: *Strongly Agree 5, Agree 4, Neutral 3, Disagree 2, Strongly Disagree 1*

	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
The contactless security system(pam vein) is more secure than fingerprint system	0.0%	0.0%	6.7%	0.0%	93.3%
The contactless security system(pam vein) was more efficient in user registration	0.0%	0.0%	6.7%	20.0%	73.3%
The pam vein(Contactless) was more accurate in authentication	0.0%	0.0%	0.0%	6.7%	93.3%
The pam vein(Contactless)was consistent in validation	0.0%	0.0%	6.7%	26.7%	66.7%
The pam vein(Contactless)was not affected by wearing out of hand palm during registration and verification	0.0%	0.0%	0.0%	20.0%	80.0%
Wearing out of fingerprint ridges affected the speed in which a user was registered	0.0%	6.7%	20.0%	20.0%	53.3%
The pam vein(Contactless) prevented unauthorized access	0.0%	0.0%	0.0%	13.3%	86.7%
The fingerprint system should be replaced with contactless security system	0.0%	0.0%	6.7%	6.7%	86.7%
Wetness of the finger affected the registration and authentication	0.0%	6.7%	0.0%	40.0%	53.3%
The palm vein was not affected by wetness or sweating of the palm	0.0%	0.0%	6.7%	0.0%	93.3%

Source (Field data, 2021)

Table 11 above shows the various responses from the participants in the control group.93.3% strongly agreed that the contactless security system (pam vein) is more secure and accurate in authentication than fingerprint system while 9.3% were neutral. In terms of registration efficiency 7.3% strongly agreed that the palm vein was more efficient, 20% agreed while 6.7% were neutral. With respect to validation 66.7% strongly agreed that palm vein was better, 26.7% agreed while 6.7% were neutral.80% strongly agreed and 20% agreed that the wearing out of the palm never affected the registration and authentication since the palms were internal as compared to the fingerprint where some users had their finger ridges worn out affecting it and also the wetness since 53.3% strongly agreed,40% agreed while 6.7% disagreed with the effect on wetness on user authentication and registration.93.3% strongly agreed that the palm vein was not affected by the wetness while 6.7% were neutral.86.7% strongly agreed and 13.3% agreed that the palm prevented unauthorized access thus why 86.7% strongly agreed, 6.7% agreed while 6.7% were neutral that the current finger print system should be replaced with a contactless secure system.

From the experiment it was conclude that it was essential for the university to implement the palm vein biometric technology due to its efficiency, security aspects and performance.

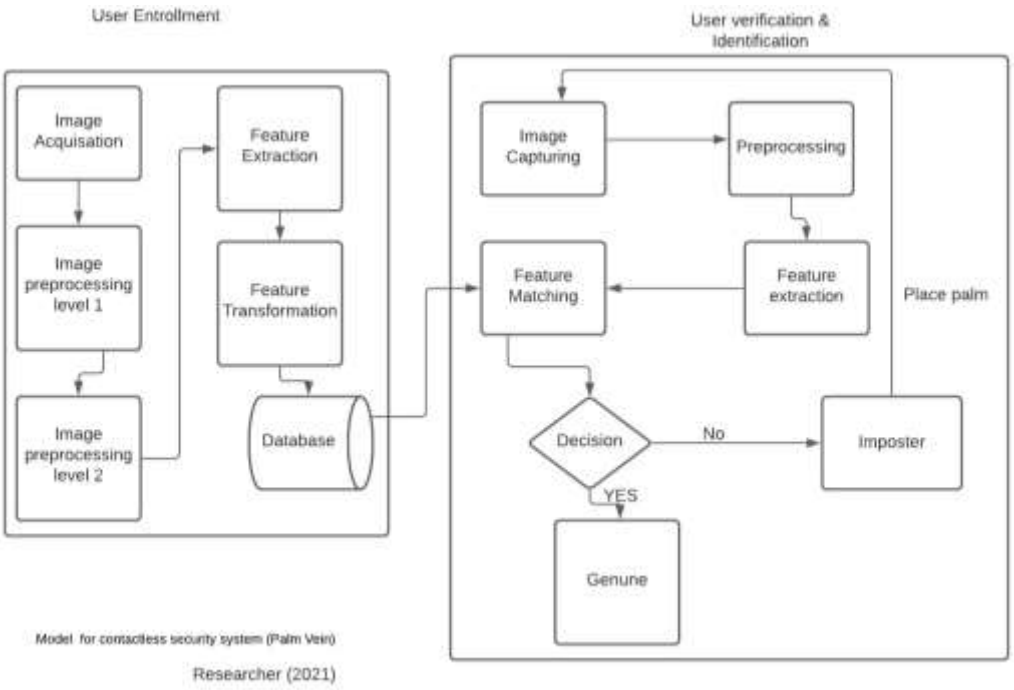

Figure 2. Developed model for contactless security system

Fig 2 Show the developed model of a contactless security (palm vein) model that can be used to enhance the access integrity of biometrics systems in higher education institutions. The model consisted of two authentication steps: user enrollment and verification. The users were expected to place their palm above the palm vein scanner thus this prevented the physical contact with the gadget especially due the COVID-19 infections via surfaces.

Figure 3. Palm vein scanner (contactless)

Figure 3 above shows the scanner scanning the palm of the user. The hybrid scanner contained the finger print, palm vein and access card.

Expert Validation

Table 12. Expert validation Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.810a	.656	.264	.89395

Source (Field data, 2021)

From the table 12 above, it indicated an R^2 of 65.6 % indicating the data fitted the model well on the expert validation of the security the model using biometric systems for higher learning institutions. This demonstrated that the contactless security system was efficient in overcoming the shortcomings associated with existing physical systems in the COVID-19 era.

Table 13. ANOVA for the model validation that with experts on model usage

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.685	8	1.336	1.671	.256[b]
	Residual	5.594	7	.799		
	Total	16.279	15			

Source (Field data, 2021)

According to table 13 above an F value of 1.671 was obtained on the model validation with experts concerning the integrity by using palm vein biometric authentication system this was less than the table value at (3.50) degree of freedom(8,7) which demonstrated that there was statistical significance.

5. Discussions

The paper focuses on investigating the effectiveness of existing biometric authentication systems in Higher education institutions. Based on results from the respondents it was clear that the widely used biometric system was fingerprint system which attributed to 68.3% .The University has been using the system for the last four years in authenticating students before they can access the university premises, lecturer and student attendance in the lecture room. It was also used in accessing the directorate of finance offices, library and also control room a clear indication that it was the most widely used form of authentication in the university. With regards on whether the proposed palm vein biometric systems, 83.7% of the study participants agreed that the proposed contactless biometric systems will solve security problems and enhance the integrity of data in service delivery as well as enhance safety of users. However, 6.5% suggested that the proposed biometric system will not

enhance any integrity. Biometric systems are becoming increasingly popular in terms of technological applications. Each biometric technology has its own set of advantages and disadvantages. Finding a recommended practice for all applications is likewise impossible. Its own utilization aims may be different.

The fingerprint and iris-based techniques, according to Khan and Alghatbar (2010), they are more accurate than the voice-based technique. Because biometrics are being more widely used in a variety of applications, the biometric market has begun to expand. From the model summary above it indicated an F-value of 0.763 at (12, 81) which is less than the table value is 1.95, hence we fail to reject the null hypothesis that there was statistical significance between the existing security systems and the Higher learning institutions. With F-value at 0.763 it demonstrated that there was strong relationship between the variables and the value was close to positive 1 thus the proposed contactless security system will be more efficient in enhancing the security especially after the outbreak of Covid-19 which has rendered fingerprint system unusable to the physical contact with the sensor. According to the model summary in Table 5, the R^2 value on the relationship between the studied dependent and independent variables was $R^2 = 0.792$ showing a good fit of the model since is greater than 50% of the test item used in the case study.

It was evident that unimodal biometric system were prone to noisy data, intra-class differences, a limited degree of freedom-anti-universality and spoof assaults.

Theft or leakage of the template information is the most serious threat to the fingerprint biometric technology. Furthermore, every individual has a finite and unique fingerprint that remains constant throughout their lifetime; hence, a breach of the fingerprint biometric poses a lifetime danger to an individual's security and privacy. (Onifade, 2020).

According to a study that was done by Nyamberi (2016), who explored on the innovative strategies in the NHIF Nakuru branch where he focused on the relationship between fingerprint biometric registration techniques and service delivery. From his findings the input variables were the employees of the NHIF who consisted of the managers and staff members from all functional departments. The findings were that the person's correlation was at 0.675 with a level of significance to be 0.05.The correlation was at moderate level which was not good since a good security system should have above positive 0.7 which demonstrates a strong correlation coefficient. From the current study findings the correlation coefficient between the variables exceeded 0.675 since it was at 0.792 thus contactless security framework system (palm vein) was better in service delivery based on efficiency in regards to data integrity. According to the experts the developed contactless model was suitable to solve the current problems associated with physical biometric systems in the covid-19 era. From the model summary R^2 of 65.6 % was obtained indicating that the data fitted the model well on the expert validation of the model using biometric systems for higher learning institutions.

Based on the research question to investigate the effectiveness of existing biometric authentication systems in higher learning institutions. It was evident that the current biometric system had failed to authenticate legitimate users and with the outbreak of Covid-19 the physical access to the systems was rendered unusable.

6. Limitations of the Study

Lack of co-operation: Some respondents did not cooperate with the researcher due to lack of interest and some because it never provided any benefits to them. The researcher overcame this by explaining to them the benefits the research will be to them.

Fear of victimization: Some of the respondents feared filling the questionnaires since once they provided negative responses the university management might take disciplinary measures on them. The researcher overcame this by explaining to them that the data obtained from the research was kept confidential.

7. Conclusion and Future Work

In conclusion, increasing security awareness and understanding of security flaws can help users avoid data leakage and protect their privacy. However, many corporations and educational institutions still have insufficient security awareness initiatives (Furnell & Vasileiou, 2017). As a result of this research, it is recommended that security awareness programs and training be implemented on a regular basis at not just educational institutions but also organizations that deal with data and information. Various biometric security systems such as fingerprint, voice, iris, ear and contactless palm vein security system were discussed. The goal of these authentication systems is to determine and authenticate access to any system component. The paper focused on presenting the findings on the use of current fingerprint system in Mount Kenya University. Based on the findings it was evident that it's inefficient, inconsistent with high FRR and FAR. Since the current fingerprint system has failed to meet the threshold of the security and safety levels needed, study recommends that the university need to

invest on the new contactless security system (palm vein technology) that is more secure and does not involve any physical contact with the sensor. The University can also consider using contactless biometric systems or multimodal security systems which will be more robust in enhancing the security and solve the problems of unimodal system such as noisy data, intra-class differences, a limited degree of freedom-anti-universality, and spoof assaults. It was evident that the current fingerprint system was no longer usable after COVID-19 outbreak due to the physical contact with the device. To overcome the safety threats associated physical contact, therefore the university should implement a contactless security system. Additionally, to overcome the weaknesses of unimodal systems the university should adopt a multimodal system that will help overcome the existing challenges. There are still gaps for future researchers where they need to focus on the various decision algorithms that are best efficient in verify users before they are authenticated in the system.

ACRONMYMS AND ABBREVIATIONS

ANOVA: Analysis of Variance

FAR: False Acceptance Rate

FRR: False Rejection Rate

ID: Identification Card

MIS: Management information Systems

NACOSTI: National Commission of Science, Technology, and Innovation

NHIF: National Health Insurance Fund

QR: Quick Response

RFID: Radio Frequency Identification

References

Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2019). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimedia Tools and Applications, 78*(12), 16345-16361. https://doi.org/10.1007/s11042-018-7012-3

Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. (2012). Technical issues and challenges of biometric applications as access control tools of information security. *International journal of innovative computing, information and control, 8*(11), 7983-7999.

Ali, M. M., Mahale, V. H., Yannawar, P., & Gaikwad, A. T. (2016). *Overview of fingerprint recognition system.* In 2016 International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT) (pp. 1334-1338). https://doi.org/10.1109/ICEEOT.2016.7754900

Dua, M., Gupta, R., Khari, M., & Crespo, R. G. (2019). Biometric iris recognition using radial basis function neural network. *Soft Computing, 23*(22), 11801-11815. https://doi.org/10.1007/s00500-018-03731-4

Dwivedi, R., & Dey, S. (2018). *A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification.* https://doi.org/10.1007/s10489-018-1311-2

Earnest, S., Nyaberi, D., & Kwasira, J. (2016). *Assessment of Innovative Strategies on Service Delivery at the National Hospital Insurance Fund Nakuru, Kenya.*

Engelsma, J. J., Arora, S. S., Jain, A. K., & Paulter, N. G. (2018). Universal 3D wearable fingerprint targets: advancing fingerprint reader evaluations. *IEEE Transactions on Information Forensics and Security.* https://doi.org/10.1109/TIFS.2018.2797000

Fetters, M., & Freshwater, D. (2015). The integration challenge. *Journal of Mixed Methods Research, 9,* 115-117. https://doi.org/10.1177/1558689815581222

Furnell, S., & I. Vasileiou, (2017). *Security education and awareness.* https://doi.org/10.1016/S1353-4858(17)30122-8

Gregory, P., & Simon, M. A. (2008). *Biometrics for Dummies.* Wiley Publishing, Inc., Indianapolis, 271-277.

Harinda, E., & Ntagwirumugara, E. (2015). Security & privacy implications in the placement of biometric-based ID card for Rwanda Universities. *Journal of Information Security, 6*(02), 93. https://doi.org/10.4236/jis.2015.62010

Jack, B., & Clarke, A. M. (1998). The purpose and use of questionnaires in research. *Professional Nurse*, *14*(3), 176-179. https://doi.org/10.1177/174498719800300304

Jain, A. K., & Uludag, (2004). Attacks on biometric systems: a case study in fingerprints. In *Security, steganography, and watermarking of multimedia contents, VI*(5306), 622-633. SPIE.

Kakkad, V., Patel, M., & Shah, M. (2019). Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design, 2*(4), 233-248. https://doi.org/10.1007/s41939-019-00049-y

Khan, B., Khan, M. K., & Alghatbar, K. S. (2010). Biometrics and identity management for homeland security applications in Saudi Arabia. *African Journal of Business Management, 4*(15), 3296-3306.

Makhija, S., Khatwani, A., & Roja, M. M. (2017). Performance analysis of latent fingerprint enhancement techniques. *In international conference on innovative mechanisms for industry applications.* (pp. 96-100). https://doi.org/10.1109/ICIMIA.2017.7975580

Martin, Z. (2007). *A New Application for Biometrics.* Health Data Management Magazine.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research Methods: Quantitative and Qualitative Approaches*. Acts Press: Nairobi.

Mwema, M. K., & Stephen, K. (2015). A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates. proc. *IJCTT, 20*(1), Feb. https://doi.org/10.14445/22312803/IJCTT-V20P103

Nakamura, T., Goverdovsky, V., & Mandic, D. P. (2017). In-ear EEG biometrics for feasible and readily collectable real-world person authentication. *IEEE Transactions on Information Forensics and Security, 13*(3), 648-661. https://doi.org/10.1109/TIFS.2017.2763124

Newing, H. (2011). *Conducting research in conservation: a social science perspective.* Routledge, England. https://doi.org/10.4324/9780203846452

Onifade, O. F., Olayemi, K. B., & Isinkaye, F. O. (2020). *A Fingerprint Template Protection Scheme Using Arnold Transform and Bio-hashing.*

Parkavi, R., Babu, K. C., & Kumar, J. A. (2017). *Multimodal biometrics for user authentication.* In 11th international conference on intelligent systems and control. (pp. 501-5). https://doi.org/10.1109/ISCO.2017.7856044

Patrick, A. S. (2008). Fingerprint concerns: Performance, usability, and acceptance of fingerprint biometric systems. *National Research Council of Canada*.

Polit, D., & Hungler, B. (1999). Nursing Research: Principle and Method (6th ed.). Philadelphia: Lippincott Company, 416-417.

Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007).Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.* https://doi.org/10.1109/TPAMI.2007.1004

Sandhya, M., & Prasad, M.V. (2017). *Securing fingerprint templates using fused structures.* https://doi.org/10.1049/iet-bmt.2016.0008

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students.*

Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., &Yin, Y. (2018). A systematic review of finger vein recognition techniques. *Information, 9*(9), 213. https://doi.org/10.3390/info9090213

Solayappan, N., & Latifi, S. (2006). *A survey of unimodal biometric methods.* In Proceedings of the 2006 International Conference on Security and Management (pp. 57-63).

Tekade, P., & Shende P. (2017). *Enhancement of security through fused multimodal biometric system.* In international conference on computing, communication, control and automation. https://doi.org/10.1109/ICCUBEA.2017.8463928

Thakur, K., & Vyas, P. (2019). Social Impact of Biometric Technology: Myth and Implications of Biometrics: Issues and Challenges. In Advances in Biometrics (pp. 129-155). https://doi.org/10.1007/978-3-030-30436-2_7

Valdes-Ramirez, D., & Medina-Pérez, M. A. et al. (2019). *A review of fingerprint feature representations and their applications for latent fingerprint identification: trends and evaluation.* IEEE Access.

https://doi.org/10.1109/ACCESS.2019.2909497

Wang, S., Hu, J., Zheng, G., &Valli, C. (2018). *A fingerprint and finger-vein based cancelable multi-biometric system.* Pattern Recogn. https://doi.org/10.1016/j.patcog.2018.01.026

Yang, W., Hu, J., Wang, S., & Wu, Q. (2018). Biometrics based Privacy-Preserving Authentication and Mobile Template Protection. *Wirel. Commun. Mobile Comput.* https://doi.org/10.1155/2018/7107295