A PALM VEIN AUTHENTICATION IMPLEMENTATION MODEL FOR ENHANCED ACCESS OF BIOMETRIC SYSTEMS: A CASE OF MOUNT KENYA UNIVERSITY MAIN CAMPUS

BONIFACE MWANGI WAMBUI

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE DEGREE IN INFORMATION CYBER SECURITY OF MOUNT KENYA UNIVERSITY

JUNE 2023

DECLARATION AND APPROVAL

I do hereby declare that this research thesis is my original work and has not been presented for a degree in any other University or for any other award. No part of this thesis should be reproduced without my consent or the consent of Mount Kenya University.

Boniface Mwangi Wambui

MSCCS/2019/39971

Sign:  **Date:**20th June 2023

Declaration by the supervisor

I hereby confirm that the work reported in this thesis was carried out under my supervision as the University supervisor.

Dr. Joyce Gikandi

Mount Kenya University.

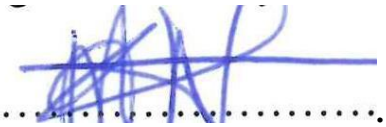
Sign:  **Date:**20th June 2023

Declaration by the supervisor

I hereby confirm that the work reported in this project was carried out under my supervision as the University External supervisor.

Dr. Geoffrey Mariga

Murang'a University of Science and Technology

Sign:  . **Date:**20th June 2023

DEDICATION

I dedicate this research to my loving mother, Irene Wambui Mwangi.

ACKNOWLEDGEMENT

I'm grateful to the All-Powerful God for giving me the grace, calmness, power, and health I needed to complete this thesis. I would want to express my sincere appreciation to everyone who offered me the chance to complete my coursework and research. My sincere appreciation is extended to my supervisors, Dr. Joyce Gikandi and Dr. Geoffrey Mariga, for their guidance and countless constructive criticisms of my work. Prof. Ongus and Dr. Kamau, I appreciate you for the role you played in supporting me, your time, and your encouragement. Thanks to the entire fraternity of Mount Kenya University for granting me an opportunity to pursue my masters.

ABSTRACT

One of the crucial components that contributes to the efficacy and efficiency of information systems is system integrity. One security method used to increase system integrity is biometrics. The existing fingerprint system is prone to spoofing attacks, high FRR and FAR, tear and wear of the sensor scanner. The goal of this study was to look at the integrity issues that affect the security of biometric technologies in Kenyan higher education institutions, IT security factors, implementing a new model and validating it. The implemented contactless security model sought to solve the current security problems facing the current biometric system. The study's particular goals were to look into the IT security factors that influenced biometric system integrity, review the success and failures of present biometric systems in boosting learning institution integrity, and design and validate the model. The research was guided by the extended integrated system theory which consisted of contingency and management theory. Since the contactless model had been approved by security system specialists, the researcher used an experimental and descriptive research approach. The research subject was Mount Kenya University's faculty and employees. Stratified sampling provided a true depiction of the varied population. 300 randomly chosen employees from particular departments made up the study's target population, and 169 individuals were picked for the sample using simple random sampling. The Zetech University served as the site of the pilot study. In the study area, questionnaires were used to collect the data. The researchers employed an equation for multivariate regression. Analysis of Variance (ANOVA) was used to examine the model's fitness, with a 95 percent confidence level test of significance. From the findings a strong correlation coefficient of 0.792 was obtained on objective one. This showed that the model fitted well and their statistical relationship between the variables. The correlation coefficient between the variables was at 0.792, indicating that the constructed model was more efficient in terms of data integrity. One objective two the R^2 of 73.4% indicated the data fitted the model well on the assessment the IT security metrics that influenced the integrity of biometric systems in higher learning institutions since it was greater than 50%. The experiment consisted of a control group having 15 participants. From the experiment the palm vein had an FRR of 93.33% while fingerprint had 60% which demonstrated superiority in authentication accuracy. On objective three a F value of 0.714 was produced regarding the integrity of the new security model. This value is lower than the table value at (1.70) degree of freedom (10,59), which showed that there was statistical significance. 87.5% of the experts concurred that the security system satisfied the requirement for a system that can improve the integrity of the data. The researcher added feature extraction component that represented infrastructure variable in the conceptual framework. The institution should consider changing its present fingerprint security system, which failed to verify legitimate users and was therefore inconsistent with data integrity. Learning institutions should implement the contactless system that does not require physical touch to verify people, which was more useful in the current COVID 19 epidemic, which has rendered the existing fingerprint security system useless. Organizations should consider implementing live detection systems or employ cancellable biometric systems that helps overcome spoofing attacks. More research needs to be carried out on palm vein template protection in deep learning since little research has been done in the field and also new decision authentication algorithms.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ATMs : Automated Teller Machines.

BVR : Biometric Voter Register

CASIA : Chinese Academy of Science Institute of Automation

CC : Cloud computing

CCD : Charge Coupled Device

CCOEFF: Cosine Coefficient

CNN : Convolutional Neural Networks

DOS : Denial of service

ECG : Electrocardiogram

FAR : False Acceptance Rate

FRR : False Rejection Rate

HEI's : Higher Education Institutions.

IEBC : Independent Electoral and Boundaries Commission

ICT : Information Communication Technology

ID : Identification Card

ICP : Iterative Closest Point

ISMS : Information security management system

LED : Light Emitting Diode

LBP : Local binary Pattern

MP : Megapixels

NIR : Near Infrared Light

NN : Neural Networks

PCA : Principal Component Analysis

ROI : Region of Intrest

RTS : Results Transmission System

SIFT **:** Scale-Invariant Feature Transform

SSL : Secure Socket Layer

SVM **:** Support Vector Machine

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

A biometric confirmation framework could be a design acknowledgment that verifies an individual's identity by contrasting the qualities that have been kept in the database with the information that has been provided (Mondal & Bours, 2017). The words "biometrics" and "metrics" are two synonyms for "life" and "measure," respectively. According to a study by Thakral (2012), the biometric data of the individual presenting themselves is compared with what is already present for each entry in the database in the verification system. He suggested that the biometric systems assess a person's physiological and behavioral traits. The characteristics include fingerprint and iris patterns, speech patterns, and hand measures. These characteristics are used to determine a person's legitimacy. Biometrics have never been more advanced, complex, or sensitive than they are now. They are used to protect citizens and companies. Biometrics, above all, is concerned with a person's biological traits (Thakur & Vyas, 2019). Over the past ten years, biometrics has developed into an intriguing yet difficult field. Contactless facial and palm recognition are among the most promising biometrics techniques, although they are vulnerable to spoofing risks. In order to safeguard biometric authentication systems from spoofing attacks utilizing printed photos, video replays, etc., several researchers concentrate on facial recognition, liveness detection, and also utilizing the veins on the hand. Therefore, it is vital to investigate the most recent advances in face and palm liveness detection research to see whether they could offer solutions to minimize the growing problems. Biometrics include hand and palm vein geometry, iris recognition, fingerprinting, and palm veining, according to Jain,

Hong, and Pankanti (2000). Many individuals believe that biometrics is the most accurate and superior method for identifying and authenticating persons (Heracleous & Wirtz, 2006).

The biometric approach to identification and authentication has also been adopted by the banking sector. The system evaluates its physical and behavioral traits for the purpose of verification (Poe & Labuschagne, 2011). These biometrics features are tightly connected to a person thus making it had to be stolen by unauthorized personnel. Out of the many biometric systems available currently, the fingerprint system is the most widely used because of its low cost. Biometrics technology has been associated with some failures. For example, a biometric system at a Malaysian border post failed a speed test, resulting in lost business when visitors canceled their trips (Mulumba, 2012). These shortcomings have made some people not to utilize the biometric system. According to Watanabe et al (2008), there is a more reliable technology referred to as palm vein pattern recognition. This technology uses veins which cannot be purloined through taking images thus forgery would be very tough beneath standard conditions. Palm vein pattern squares measures are distinctive to all persons. Though these facts haven't been medically evidenced like the fingerprint, iris and so on. Results from experiments supported by in-depth information and actual experiences with financial institutions showed that palm vein authentication is more reliable. Babalola, Bitirim, and Toygar (2021) claim that the palm vein employs the vascular patterns as a form of personal identity. A person rests his palm on the device or a few centimeters above the sensor that flashes infrared light that passes through the haemoprotein thus illuminating the deoxygenated blood to form a black network which is stored in the database template. During authentication the stored algorithm is compared with the person's palm for accurate matches.

Biometric system technology has been used by some business sectors and the government. In the banking sector, electronic images of banks and pay slips are stored electronically to reduce fraud (Selvarani & Natarajan, 2013). Some governments like the United States have used biometric systems to identify and verify both citizens and non-citizens. A good example is the USA government which has widely implemented this technology.

Voter registration in Nigeria has been done using this technology. According to Evrensel (2010), it was challenging to register voters since they lived in remote locations with challenging terrain, which made it difficult to move the delicate equipment. The biggest issue was that each polling place's biometric equipment could only register a small number of voters. This resulted in a large number of people getting registered in other, far-off polling places, which created confusion on election day. Given that Nigerian elections are held outside, it is impossible to ignore how the environment affects the physical state of fingers. The quality of the fingerprints may be significantly impacted by the physical traits of the fingertips, which can range from dry to damp (sweaty) (Samuel et al., 2022). A study by Iwuoha (2018), on Nigerian elections in 2015 found that the machines broke down when election observers were present and there was a low turnout as compared to other elections. The 2012 Ghanaian elections were a failure, according to Effah and Debrah (2019), because electoral officials were not adequately trained on how to use biometric technologies.

Electronic voting is presently used in Kenya's national political elections. The application of this technology in Kenya's 2012 elections shows that biometric accuracy is not always dependable, necessitating the use of human counting. The IEBC had a bold technological strategy that was based in part on the BVR (Biometric Voter

Registration) and the RTS (Real-Time Voting System) (Results Transmission System).

There were reports that voter biometric data had been leaked, and that the data had been used to tamper with the final results. Voters have been identified and verified using biometric verification systems in conjunction with electronic voting. It is expensive to automate an election process, and to make sure it runs smoothly, computers and highly qualified employees are needed. A system malfunction on election day, the system disqualifying some qualified voters, a compromised central database, and other issues were among the challenges experienced. The accuracy and integrity of the electronic voting system were threatened by some voters who used it multiple times. A benefit of the system was its capacity to provide real-time results of votes cast and shorten the time required for vote counting (Mulumba, 2012). Despite the fact that various research on various aspects of biometrics and service delivery have been conducted, none has looked at the influence of contactless security systems on service delivery in Kenyan educational institutions. Guleker and Keci (2014) investigated fingerprint biometric systems for class attendance in Kenyan educational institutions. The fingerprint system for class attendance has failed since sometimes it fails to verify or recognize legitimate students due to wear of the scanner of poor ridges on the students' fingers. A study by Nyamberi (2016), looked into the creative approaches used by the NHIF Nakuru branch, concentrating on the connection between service delivery and biometric registration methods. From his findings the input variables he used were the employees of the NHIF who consisted of the managers and staff members from all functional departments. The findings revealed a correlation for the subject of 0.675 with a significance level of 0.05. The correlation's low level was undesirable because a robust security system should have a correlation of positive 0.7. Owiti (2010) looked into the internal elements that affect how well mobile computing is received in the healthcare industry.

The problems that medical institutions have with ICT acquisition, implementation, and maintenance were the focus of a study by Kariuki (2010). Soliman (2021) offered a good solution that made use of the greatest common divisor (GCD) method. recovering the biometric by computing the GCD of the two resulting cancellable biometrics after blurring it with two prime operators. According to Almomani et al (2023), the cancelable biometric can be generated without the need for additional information or images. We developed an effective palm vein authentication model in this work due to some of the flaws in the linked biometric security systems' poor resilience and security outcomes. The majority of enterprises have given up on biometrics as a result of the current Covid-19 (Corona virus) epidemic since they are useless against the virus's ability to spread through touch on surfaces. This gap needs to be solved by using a contactless security system that does not entail any physical contact.

1.2 Statement of the Problem

The availability of high-quality services for accessing services in higher education institutions is hampered by concerns with identity theft and the dependability of authentication systems. The integrity of the data has been compromised by the increased number of security loopholes brought about by the combination of biometric systems and the Internet. There are several spoofing attacks associated with fingerprint systems due to their intrusive nature. Guillen et al. (2012). The target audience that was impacted was the university's workers and students who utilized the biometric system to clock in and access different buildings and rooms. Sometimes the affected personnel tried to clock in but the system could not verify their information. The False Rejection Rate for the biometric system was extremely high. These problems highlighted the inefficiency and ineffectiveness of the biometric system, putting its integrity in jeopardy. According to a report by (www.statista.com (accessed on 16 January 2023), the "Facial Recognition Business" FRB report (2022), the market for face-based biometric recognition will reach

12.11 billion USD by 2028 as a result of potential applications in a number of categories. The market for contactless biometrics, in contrast, would be worth 37.1 billion USD. Numerous instances when security is essential have seen the successful usage of biometrics. Personal identification cards for use when checking into and out of airports, protecting private data from unauthorized parties, and validating payment cards (Khairnar et al., 2023). According to (Petrov,2020), The market for speech and voice recognition is anticipated to develop between 2019 and 2025 at a CAGR (Compound Annual Growth Rate) of almost 17,2%, reaching an estimated $26,8 billion by that year. Consumers favored voice recognition

(32%), fingerprints (27%), facial scans (20%), hand geometry (12%), and iris scans (10%), with a strong preference for familiarity and use. Mishu and Rahman (2018) claim that in order to access the system, a spoof, or phony or fraudulent fingerprint, is presented to the scanner. Still, the scanner is unable to distinguish between fake and genuine traits. The system is now easily accessible to the hacker. Putte and Keuning (2002) developed fake fingerprints and tested them on various sensors both with and without the owner's assistance. They displayed a result demonstrating that almost all sensors first recognized the fake fingerprint as real. Gummy (fake) fingers were tested against 11 distinct fingerprint systems by Matsumoto et al., In their testing, the system accepted between 68% and 100% of gummy fingers during the verification process. Additionally, they demonstrated the ways in which an attacker could trick the scanner's system.

Existing biometric based systems are mainly contact based and are challenged when there is a contact viral pandemic outbreak such as Covid-19(Corona virus) in 2019. Dry skin ridges of the users cause wearing out of fingerprint systems thereby reducing recognition accuracy which causes High FAR (False acceptance rate) and False Rejection Rate

(FRR). Mobile biometric authentication is unquestionably significant in the COVID-19 age. Touchless, individual mobile biometrics systems can support

reliable authentication while also fulfilling stringent hygiene standards, even if it is still challenging to integrate biometric identification technology into mobile device platforms. As described in this section, using remote biometric authentication in the COVID-19 era has a number of advantages. However, establishing reliable identity management also necessitates the use of efficient privacy protection techniques. It is also essential to have barriers against or warning signs of presentation attacks. The latter is often more challenging in a remote authentication environment, where means of detecting assaults may be more restrictive than in a conventional (accessible) biometric system (Gomez-Barrero et al.,2022). Vein recognition is high in accuracy, according to Lee (2012) based on Fujitsu research, it had an FRR of 0.01 percent and a FAR of less than 0.01. The lack of reliable fingerprint authentication and verification of students or other individuals was a major issue which was also demonstrated by a gap in the integrated system theory where infrastructure component was missing. Technology is seen as intrusive and has the ability to spread contagious skin diseases. Security issues and systems can fail to identify people for a variety of reasons, such as dry skin on the fingers or machine wear. Compared to palm vein technology, fingerprint technology has a higher rate of erroneous acceptance. Due to their intrusive nature, fingerprint systems are susceptible to numerous spoofing attacks (Guillen,2012). Due to the intrusive nature of biometric devices and the Covid-19 epidemic, which prevents users from touching the sensor, they are no longer usable.

According to Jacobsen and Sandvik (2018) the alternative is the use of contactless access systems such as Palm Vein technology (anti-spoofing security infrastructure).

However, recognition accuracy, verification and authentication speed in palm vein technology are not 100% effective being a new technology. Therefore, more research is

required with the goal of enhancing service access. The goal of the study was to find an answer to the following dilemma: What impact does the implementation of a contactless security model have on the integrity of biometric systems in Kenya's educational institutions?

1.3 Purpose of the Study

The goal of the project was to develop a contactless authentication implementation model based on palm vein for enhanced security access of biometric systems in higher learning institutions.

1.4 Objectives of the Study

i. To investigate the effectiveness of existing security systems in Higher learning institutions.

ii. To assess the IT security factors that influences the integrity of biometric systems in higher learning institutions iii. To develop a logical model that enhances integrity access of biometric systems in higher learning institutions.

iv. To validate the developed logical model that will help enforce integrity by using palm vein biometric authentication system.

1.5 Research Questions

i. What is the effectiveness of existing security systems in enhancing the integrity in higher learning institutions? ii. What are the IT security factors that influences the integrity of biometric systems in higher learning institutions? iii. Will the developed logical model enhance the integrity access of biometric systems in higher learning institutions?

iv. Will the developed logical model be validated in order to enforce integrity by using palm vein biometric authentication systems?

1.6 Justification of the Study

The institution needed to develop new methods that guaranteed a high degree of integrity due to the rise in counterfeiting, inconsistent impersonation, and other reliability difficulties. In relation to Mount Kenya University the biometric systems have worn out and the user had to place his hand several times for the system to recognize him or her. This was evidenced by a queue at the university gate where the system was unable to verify the students at a fast rate. Since the existing fingerprint biometric technology is external to the body, it is simpler to replicate. Users' fingerprints have occasionally been stolen by unauthorized parties, who subsequently faked replicas of the users' prints that could be used to access the systems. These users typically control the servers, databases, and systems. Due to the possibility of modification, which might lead to inconsistencies and data loss, this compromised the information's integrity and confidentiality. This technique is used by Carolinas Healthcare in the United States to identify patients during admission (Nelson, 2008). Concerns about infection, the device's contactless nature, and the wear and tear on fingerprint scanners all drove their decision to employ this technology.

The developed contactless security model was free from impersonation. The proposed palm vein biometric technology was suitable for Mount Kenya University since it had embraced technology. The university had adopted the use of biometric system during student registration, class attendance monitoring, examination verification and access to the university premises. The university staff had to be verified by the same biometric system during lectures as well as accessing the University. Since it’s growing and there are new loop holes in the current system, the university has to adopt the contactless palm vein technology which is impossible for unauthorized persons to copy. The University should adopt it since it has a good security, enhanced data integrity, reliable and its cost

efficient. The developed model was more secure since it was free from physical contact thus would be of great benefit especially during COVID-19 error where users do not have touch the physical sensor during authentication.

1.7 Significance of the Study

This study added to the body of knowledge in the field of life sciences and offered knowledge to academicians, stakeholders from the institution, and students. The scholars and university fraternity will be ready to create wise decisions relating to application of palm vein technology in learning establishments. The main beneficiary was the University fraternity who will adopt the new palm vein Technology in their student registration, gate entrance authentication and class attendance verification in enhancing a better security. The technology reduced the false rejection rate. The study was going to be helpful to all personnel within the learning institution where the matter of identity theft has been prevailing. Since the Kenyan government and its departments are currently developing numerous biometric systems, knowledge of the palm vein will be of great value to them. The fact that it served as a foundation for any analytical work on alternative facets of life science was also advantageous to the researchers. The research provided a better solution in ensuring that the integrity of the records is not compromised by the illegitimate personnel. The proposed technology sealed prevailing loops holes that have been used by hackers or unauthorized users in compromising the security on organization. Decision-makers at Kenyan educational institutions should increase the integrity of information systems by using the study's findings.

1.8 Scope of the Study

There was a geographic scope, and the researcher conducted the study in a constrained setting, like a university. In respect to the content scope; the researcher focused on the student registration data, biometric authentication details and class attendance using the current fingerprint biometric system.

1.9 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.

1.10 Delimitations of the Study

i. The amount of time the researcher had to complete the research was constrained. This was due to the fact that the researcher was required to gather and analyze the data for four months in 2021.Thus, the researcher used the time effectively to prevent postponing other project tasks like project analysis and presentation. ii. The researcher piloted the use of palm vein contactless security model with a limited proportion of the sample size due to cost implications of buying the devices.

1.11 Assumptions of the Study

i. There was an assumption that the university staff provided all the necessary information required.

1.12 Operational Definition of Terms

Authenticity: It refers to the state of being genuine.

Biometrics: It's a technology that verifies persons based on physical characteristics.

Efficiency: It refers to the state through which a system is able to accomplish a task very quickly ensuring accuracy, time saving and good performance output.

Identity Theft: It entails deliberate use of someone's credentials to gain an advantage over his resources or to be granted to a facility through masquerading.

Integrity: It's the assurance that the information stored in a system is accurate and confidential and can only be accessed by the trusted legitimate users. The system is reliable since there are no issues of inconsistencies with respect to the data.

Service delivery: It describes the process through which a company gives its clients access to its facilities.

Unauthorized Access: It is the process by which an unauthorized user gains access to a computer system and manipulates data without permission.

Verification: Verification involves comparing a person's biometric data to a particular entry in a database that relates to that person.

1.13 Chapter Summary

This chapter outlined the numerous biometrics systems in use around the globe, the flaws in the fingerprint systems now in use, as well as the goals, rationale, and parameters of the study. The study advises higher education institutions to increase employee understanding of access integrity issues and to think about deploying contactless palm vein authentication technology.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The chapter examined a broad range of biometrics literature, as well as concepts and designs for cutting-edge security systems. The contemporary biometric technology system's theoretical and analytical aspects, as well as literary criticism, were investigated. This chapter explored the conceptual foundations for biometric systems as well as the theoretical and empirical literature.

2.2 Empirical Literature

2.2.1 Security Efficiency of Palm vein Authentication Technology

Internal body vein properties are used in the technique. This distinguishes them from each other, even if they are identical twins. These characteristics are extremely difficult to create. The unique blood vessel pattern found beneath the skin surface of the human finger is the basis for this technology. The vascular pattern of a human finger could be linked to other previously or freshly saved venous finger IDs using this identifying method. Vein identification reconnaissance systems use infrared light and a monochrome CCD camera in order to capture the palm patterns. The hemoglobin in your deoxygenated blood absorbs infrared light via your finger, causing a camera to capture an image. Black lines in the image represent the finger vein pattern. These data are converted to digital format and processed before being utilized for authentication. Since the vein pattern is concealed within the tissues of the palm and can only be verified using sophisticated technology, it is very challenging to replicate (Shaheed,

2018).

How it Works

Source: Image retrieved from Fujitsu Research Institute (2009)

Figure 1 Palm vein Scanner

This technology is being used at Carolinas Hospital in the United States to track patients throughout their stay (Nelson, 2008). Concerns about infection and fingerprint scanner wear and tear influenced their choice of technology. Vein recognition, according to Fujitsu (2005), is extremely accurate, with a FRR of 0.01 percent and a FAR of less than 001 percent. Japan is the first country in the world to use the technology to verify customers in its library and in the financial sector. The following are some of the reasons to consider palm vein authentication technology:

a) The palm is Secure.
b) Vein patterns area unit distinctive to every individual.
c) The palm has no hair.
d) Non-Intrusive:
e) Palms have a broad and complex tube-shaped structure pattern and therefore contain a big quantity of differentiating options for private identification.

The palm vein procedure involves the following stages.

a) **Image Acquisition**- Images are captured using a NOIR camera module connected to a Raspberry Pi and an infrared LED light source. Between 760 and 110

nanometers is the wavelength range. The 5MP resolution of the camera is being used. The image is kept on an SD card by the Raspberry Pi (Raut, 2015).

b) **Image Processing**- To produce the desired results, image processing applies specific algorithms to the image. To speed up processing and do away with the need for extra color channels, the image is first made grayscale. After that, its histogram is equalized, which merely means that the light and dark extremes are brought closer together. The final application of Gaussian blur to the output image smooths out any remaining noise and image artifacts.

c) **Template matching**- Template matching is the process of comparing an image to a base image. After iterating through numpy arrays with the image, the ratio of similarity is determined. This system uses TM CCOEFF NORMED template matching to match source and destination images (Min Peng, 2016).

2.2.2 Related Literature on palm vein

A study by Vijayalakshmi (2015), a standard web camera together with Independent Part Analysis and Gabor Texture Patterns was used. A Gabor algorithm was used to extract the palm print's ROI and its attributes after the hand was separated into frames. A distance and NN-based classifier are then used to remove and sort the ICA highlights.

The ICA approach performed better than the non-dimension approach. The researchers Ranjith and Karthikeyan (2016), used palm dorsum to confirm vein design. The images of palm veins are first improved, then features are separated using neural networks, feed forward, and SVM computations, which provide great precision and competence. According to a study conducted by Yan and Wu (2016), some palm veins were created using directional cues drawn from binary patterns found in the area. To accentuate the augmentation, a multi scale Gaussian filter was used. The palm traits that were retrieved were then encoded in binary format. The Laplacian Filter was used to conduct a survey

on human palm vein identification. During the survey, features were extracted from convolved pictures using the Laplacian filter, and vein properties were improved using histogram equalization. It can be employed in both unimodal and multimodal veins, the study found. The study also shown how valuable the technology may be for biometric online security systems (Kamil, 2020).

In a 2018 study, Kavitha and Sripriya looked at how to recognize persons from pictures of their hand veins. A sophisticated edge detection method was used to construct the image's edges and curves, and the properties of vein pictures from the palms were retrieved. This strategy has cheap operating costs and minimal computational complexity. The research found that the recognition time was only 0.5 seconds. In 2015, Acta Polytechnic Hungary published a paper by Bharathi and Sudhakar on a multimodal biometric system based on hand veins. Shearlet transform and scale-invariant feature transform were used to obtain the features. The database including the palms was updated using the finger hand and vein coefficients. This fusion approach was able to attain the highest accuracy of 94% using FAR and FRR.

Palm vein recognition out ways all other biometric systems, according to a study (Soh & Ibrahim, 2018). This is owing to its high recognition accuracy and the fact that different papers provide diverse methods to use it (Du & Yuan, 2019). Pixel-to-pixel handling is particularly susceptible to aberrations, its display is usually impacted. Because they are essential to the accuracy of the results, the feature extraction and recognition phases are the main focus of the research (Soh & Ibrahim, 2018).

The majority of research focuses on the contactless palm vein recognition model (Soh et al., 2018). For real-life situations, a palm vein contactless model is preferable. In any case, a contactless model causes problems such as non-uniform enlightenment and relative change, which are incompatible with particular methods. Aside from that, distortions,

which occur as a result of scale change, hub change, and model precision, have a significant impact on palm vein images, just as they do on finger images. Visual improvement procedures such as histogram leveling are commonly used to improve picture quality (Wang and Zhang, 2014). Regarding the accuracy of vein images, it is important to take into consideration the study by Meng and Yang (2018), which offers a unique viewpoint that can assist in addressing the problem of distortions for finger-vein biometric systems. Their dedication stands out in comparison to previous research that, among other things, execute a more precise ROI division or use a more effective component extraction to lessen the impact of inaccuracy (Liu & Zhang, 2016). Based on the hypothesis that the distorted nature of venous pictures led the biased data created by the removal of pixels to create in the coordinating with measure, the highlights at the pixel level were accomplished.

2.2.3 Biometric systems vulnerabilities and attacks

Failures subsequently have a direct impact on the system's performance rate, according to Bernal et al. (2023). Designing a specific method of preprocessing, feature extraction, and decision-making for the behavior of the biometric trait and its intra-user variability is the most common course of action to address the inherent problems. Khanna and Kaur (2020) gives a unique instance dealing with intra-user fluctuations under practical concerns for biometric authentication based on ECG data. Due to damage, illness, changes in the acquisition environment, or modifications in the user's physical state, a biometric trait's information slightly varies in several presentations (Newaz, 2021). Therefore, intra-user variability or issues with the sensing and processing modules, which are intrinsic flaws, may cause biometric systems to draw the wrong conclusions. Extrinsic failures, on the other hand, are caused by external attacks that alter the environment and the proper operation of the recognition system.

Extrinsic failures may be the result of passive or active attacks. The confidentiality of biometrics is at risk from attacks that are passive and only watch or track data. The secrecy and integrity of biometrics are in danger when there are active assaults that alter, steal, or erase data. The performance of the system is then impacted by active assaults that result in denial-of-service (DoS), unauthorized access by a fake user, or usage of biometric data crucial to user identity. The attacks consist of the following;

a) **Brute force attacks**- An attacker transmits every possible combination of the protected data to the decision-making module up until successful recognition.
b) **Hill climbing attacks**- An attacker continuously sends fake templates to the decision-making module until successful recognition. The attacker receives feedback after each attempt to modify the fictitious template.
c) **Dictionary based attacks**- Only the protected templates having the greatest chance of being successfully recognized are sent by an attacker to the decisionmaking module.
d) **Known template attacks**- An attacker tries to guess the method or find out more information when both the original template and the protected template are compromised at once.

2.2.4 Types of Biometric Systems

a) Fingerprint-According to Aboalsamh (2009), many biometrics are inefficient due to some technical problems either due to wearing of the sensors or ridges from the users. A biometric system at a Malaysian border station, for example, failed a speed test, resulting in lost money due to visitors canceling their travels (Homeland Security News Wire, 2011).

Palm vein recognition is a newer technology that takes advantage of fingerprints' flaws. In healthcare, vein technology appeals because it eliminates the need for personnel to

contact the scanner, lowering the danger of infection. Kenya's Independent Electoral and Boundary Commission (IEBC) has previously tested a biometric voter registration and verification system that will be implemented across the country (Neurotechnology, 2011).

Vulnerabilities and Performance Security Analysis on Fingerprint System A study by Guillen et al. (2012), was conducted to better understand fingerprint biometric system weaknesses. The fingerprint recognition system analysis approach was divided into two components. The biometric fingerprint technology is covered in great detail in the first section, and the database server, built-in app, fingerprint scanner, and network in general are all covered in the second section. The study divides attack on biometric identification systems into two categories. The first are direct attacks, while the second are indirect attacks. When physical devices are attacked directly, this is referred to as a direct attack. As direct attacks, the study identifies false fingerprints and sensor damage. Unauthorized communication access violates authentication systems, resulting in indirect attacks. The results of these tests will help detect any system dangers, allowing the system's creator and users to make an informed decision on which biometric system to utilize. Fingerprint biometric authentication may not be sufficient to provide the desired level of security. As a result, the author suggests that finger vein biometrics technology be used in addition to fingerprint authentication (Aboalsamh, 2009).

b) **Retina Scanning**-The blood vessels in the eye are analyzed using scans, however the user must be quite close to the equipment. Iris scans are better compared to the retina scans due to the distance. The iris reacts to variations in light and can be used as a supplemental verification tool (Dua, 2019).

c) **Voice Recognition**-Using a pass-through, this device analyzes speech characteristics to identify persons. Because the technology is non-intrusive and contactless, it has a high level of societal acceptance. The behavioral and

physiological characteristics are associated with the movement of the mouth. The sound of what is being spoken can be used to identify both the speaker and the content because it may be different from that of another speaker. Speech recognition is widely used and reasonably priced, although it takes longer and is less precise (Abozaid et al, 2019).

d) **Facial Recognition**-This technology is used to record the distinctive attributes of the face. It's non-intrusive since no contact is required. This technology can be affected by using glasses or hair and the human face may change with time. Face recognition may now be used to recognize a target from afar utilizing highresolution cameras with zoom capabilities, making it more suitable for safety and security applications. It's simple to set up facial recognition software (Cook et al., 2019).

e) **Ear Authentication and Identification**-Physiological biometric traits are also represented by the biometric elements of the outer ear. Sound waves are utilized to identify the ear canal. The form of the human ear canal is likewise unique, similar to fingerprints or the iris. For ear authentication, external devices are also necessary. The sound waves that are released from within the ear canal are recorded using an earpiece with a microphone. Because no pictures or testing are necessary, ear authentication is exact and simple to adjust, making it appropriate for today's fast-paced lifestyle. However, the patient must wear special external earphones for in-ear verification, which increases the cost

(Nakamura, 2017).

2.2.5 Security policy Issues

It's a legal document that provides the direction and data security support depending on the organization or business requirements. The end users are considered the most

vulnerable through insider threats where legitimate users who have access to sensitive information pass it to outsiders who use the information against the organization causing economic crimes and data loss. In adequate awareness among users has contributed to the loss of data according to a survey done by Global Information Security Survey. Many firms have implemented information security policy in order to improve their security levels (Doherty & Fulford, 2006)

2.2.6 IT Security Metrics

Luna and Suri (2011) suggested that the security metrics analyze the level of implementation of security measures, as well as their efficacy and efficiency, and identify potential corrective actions and/or enhancements in order to gauge the completion of performance goals and objectives. These are the main elements that make up metrics.

a) **Initiation of the information security metrics program**- According to Swanson (2003), it entails analyzing all the key requirements in the metrics program such as setting clear objectives and ensuring good cooperation between the stakeholders so as to ensure its successful. A metric must have clearly defined goals (Brotby, 2008)

b) **Metrics for information security development.** The part involves developing a new metric program. For certain businesses, not all metrics are applicable. A good metric should be easier to use, subjectively measured, computerized, and consistently measured. All the stakeholders should be engaged during metric development and the firm has to ensure the metrics conforms to the legal requirements (Jaquith, 2007).

c) **Analysis of information security metrics**- According to Swanson (2003), the component outlines the data collection methods and visiting other organizations

in order to benchmark how they perform their duties. It entails identifying the areas that requires improvements.

d) **Reporting information security metrics**-Once data has been analyzed. The areas that require improvement are reported to the management for action (Jansen, 2009).

e) **Maintaining an information security metrics program**-This entails deploying the metric to the organization. Periodic reviews will be required in order to measure whether the objectives are being met or the metrics are being followed (Kark & Stamp, 2007).

2.2.7 Cloud computing Security Infrastructure

To ensure that an organization is to be considered successful, it must secure data confidentiality, integrity, and availability. ICT security is defined by ISO/IEC 13335-1 (2004) as the state where data confidentiality is implemented, available, and free of illegal change, as well as ensuring nonrepudiation. It is critical to have a good grasp of these extra features because information cannot be regarded safe without them (Dalmarco & Barros,2018). The beneficial attributes of cloud computing are that they provide demand self-service and they are elastic. The CC allows the subscribed users to access the data in the cloud servers without any human intervention. Cloud computing approaches like deployment and service can have a big impact on system security, but they can also help by giving solutions. The cloud computing can be categorized into two; deployment and service models.

2.2.8 Cybercrime Issues for Higher Learning Institutions

Cybercrime is any illicit action that relies mostly on computers or other electronic devices to carry out the crime or any data theft. Cyber-attacks are launched more in

HEIs as compared to other public sectors. This is according to a public sector report 2016. These attacks are occasioned with DOS attacks, network interference, data interception, theft of data and unauthorized access to information in the systems (Marang & Nelson, 2019). Numerous HEIs testified against various cases of confidential data/information loss, modification of specific data/information, such as alteration on student's school fee balances, and modification of student grades, according to a report by (Communications Authority of Kenya; Kenya National Bureau of Statistics, 2017).

According to a report by Cyberoam (2016), there was an increase in student hacktivism where students have interfered with information systems and adjusted their grades and fees in countries like Egypt, Kenya and Morocco. It has become a booming business during graduation time and end of the semesters when marks are being processed. With these reports it's very clear that higher learning institutions are suffering and it's essential to conduct a cyber-security research to understand the challenges they are facing (Marang & Nelson, 2019).

2.2.9 Related models and algorithms on palm and finger vein recognition

A study by Xie and Kumar (2017), introduced CNN for finger vein detection with supervised discrete hashing to overcome the problem of large template storage space by reducing template size and therefore increasing matching speed. A deep CNN model was proposed by Hong and Park (2017) to address the misalignment and shading issues.

The time and labor needed for feature extraction and pre-processing are also reduced. Lack of training data creates a substantial hurdle for finger vein recognition. To solve this problem, Fang and Kang (2018) developed a similarity measure network employing two-channel network learning.

To increase robustness against outliers and vessel breaking, Yang et al. built generative adversarial networks for the first time in the field of finger vein representation in a publication that was published in 2019. Instead of CNN's completely linked layers, it uses solely convolutional networks to cut down on the processing costs of feature extraction. To boost identification rate and accuracy, Luan and Wu (2014) presented an effective method called LBP (Local binary pattern). LBP has discrimination powers and processing economy thus it is commonly utilized for texture representation. The discrimination power is diluted when employed to show the sparse texture in palm vein photographs, resulting in decreased performance, especially for large images.

Pflug and Busch (2012) proposed using a new technique called the ICP algorithm to match the veins of the palm. Multispectral palm images were combined at the pixel level and registered at the feature level to increase the contactless system's verifiability. Filters that match features are used to extract them. This method requires obtaining images in a contact-free, multi-spectral environment with a specialized equipment. Palm vein identification is claimed to be more hygienic because it is contactless. The vein patterns are not altered as a result, and the rate of false rejection is lower.

Dai and Zhou (2011) introduced multifeatured based palmprint recognition, which has a lower false rejection rate (FRR) than earlier techniques. Hand veins are a promising biometric modality since they are obtained in Near Infrared light, which means that skin differences and dirtiness are less noticeable than in visible light. Additionally, the hemoglobin in the veins responds to NIR light, making it possible to record the hand veins in excellent detail. The palm or the back of your hand may be utilized. In order to increase the information security of a hybrid system, a number of factors need to be considered (Al-juaid, 2017).

Spoof attacks are "methods of misleading a biometric system by providing a fake sample of the subject for authentication," according to Tome and Marcel (2015).

Attacks that spoof faces and videos have used a range of high-resolution images, like a 3D mask that looks like real skin. On the other hand, finger spoofing uses molds to trick the biometric system. Printing images of the palm on a common printer, which is capable of readily overcoming biometric authentication, has been used to fake palm veins (Tome, 2015).

In light of these limitations, we provide a unimodal robust palm spoof detection system that employs CNN-based high-level features and SVM algorithms for enhanced classification. CNNs use several convolutional layers followed by fully linked layers which helps to obtain a good distribution for class trainings. Scene recognition, action recognition, spoof detection and picture retrieval are some of the applications that leverage the activation of neurons from the connected layers. Hand-crafted features are utilized in traditional approaches, followed by classifier training which provides an efficient mechanism that can be used to deal with anti-spoofing issues. The technology has been applied in mobile devices (Cai & Han, 2022).

2.2.10 Cyber Crime & Security

Cybercrime entails all the illegal activities conducted via the internet and the computer is used as a tool to facilitate the crime. The abuse of computers by hackers has led to birth and growth of various cybercrime attacks such as spoofing, pharming, smishing, phishing, ransom ware attacks, email frauds and also identity fraud (Joshi, 2016). Due to the integration of biometrics and the internet there have been scenarios where the systems have been hacked very easily especially on the sensors, matching algorithms or in the database template. The sensor is very prone since it entails direct attack where the user

must have a physical interaction with the system when placing a finger or in hand geometry. According to Giri, (2019), these cybercrimes can be directed against individuals, governments or even private companies. Although the terms "information security" and "cyber security" are frequently used interchangeably, the former highlights the possibility of a target being the focus person, while the latter talks about the function of the human in the security process. Although necessary for protecting personal information and computer networks, firewalls, antivirus software, and other technological solutions are insufficient to guarantee security. Every nation's security depends on enhancing cyber security and safeguarding critical data infrastructure. The advancement of IT and internet services depends heavily on cyber security. Security strategies, policies, and procedures both policies and the use of security technology must be in place. Cyberwarfare poses a serious threat to highly digitalized societies and cultures. No government has been able to create a security plan that totally secures security in operations involving international communication.

2.2.11 System integrity

Integrity is the guarantee that the information is true and accurate and has not been modified by an outside entity, such as hackers. Since biometrics and the internet are currently integrated, it is simple to alter the data, endangering the accuracy of the data. The system's integrity depends on accurate data. When processed and compared, the data from the sensor must be accurate and maintain its integrity at all times. This is an essential counterattack strategy for man-in-the-middle and replay attacks. Privacy activists worry that the capacity to recreate biometrics from template data could compromise the integrity of the templates. Because of the multiple cyberattacks that can compromise the system's integrity and the security of the data, liveness and cancellable biometrics, such the usage of palm technology, may be a solution. Live organisms that permit fluid to pass through

their bodies must be used for liveness identification. The blood flow in the palm serves as the foundation for the suggested security technology. Hill climbing is the best technique for reconstructing the biometric, and it will be used to iteratively process template data (Roberts, 2007).

2.3 Model Implementation Approaches

The process of transforming a security model into a working system that complies with particular security requirements is known as security model implementation. Both logical and physical model implementation are required for the implementation. Security models provide a framework for achieving security objectives, but the implementation of the security model can often be a challenging task. It requires careful consideration of the intended security goals, the design of the security controls, and the technology and tools required to implement those controls. There are several common approaches to implementing a security model. The following are the most widely used approaches:

a) **Policy-Based Approach:** The policy-based approach to security model implementation involves defining and enforcing policies that dictate how security controls should be implemented. This approach is often achieved through automated systems that enforce the policies. Devika et al (2017) used the policy-based approach to implement a novel framework for cipher using cloud-based technique for health care centers and he provided the overall architecture of the system and all functional components. Hagan et al (2018) conducted a study using policy-based implementation approach on threat modelling of emerging embedded architectures. Use case-based application threat modeling is a frequently used technique for creating a device's security architecture. The use case, deployment circumstances, and device functionality are evaluated in this process to determine which device assets may be targeted by an adversary. This

procedure is described in a way that supports the life cycle of device development. A security model, a technical document that offers security rules particular to that use case, is the final result of this approach. To accomplish the intended application security, the designers then adhere to security rules. Therefore, only dangers considered during the modeling phase are included in the device's model design implementation.

b) **Risk-Based Approach**: The risk-based approach involves analyzing the organization's risk appetite, identifying risks, and prioritizing the implementation of security controls based on risk levels. This approach is often used in conjunction with the policy-based approach. According to Hoffmann et al (2020), The method may be applied by firms that plan to deploy security measures to comply with legal requirements or to cut down on cyber risks to a manageable level. The risk-based approach utilized in conjunction with the cyber kill chain is a futuristic concept that will include many laws, rules, regulations, and best practices for information processing, information transfer, and data protection, including personal data. To detect threats, vulnerabilities,

and their possible effects on data or information that directly affected the data's integrity, confidentiality, and availability, a risk management model was put into place.

c) **Compliance-Based Approach**: According to Li et al (2022), The compliancebased approach is similar to the policy-based approach, but it focuses on satisfying specific compliance requirements, such as regulations and standards. Individual motivation has a direct impact on how likely they are to adopt compliance-based strategies for managing digital identities (Koohang et al. 2019). Even while businesses actively deploy cutting-edge technologies to manage digital identities, their efforts will be for naught if staff members lack the

drive to abide by the rules and guidelines. The execution of digital identity management policies and standards may be hampered by employees with unfavorable attitudes (Hong and Furnell 2022).

2.4 Model Validation Approaches

2.4.1 Expert validation

This approach entails using a group of experts who have the knowledge in the area of research where they individually provide responses. As a result, it's crucial to combine elicited assessments. According to Clemen and Winkler (2007), the experts evaluate the methods that are accessible. Experts can be used as essential personnel to validate models and frameworks.

2.4.2 Machine learning validation

This entails the system or model by using some test data with known outputs (Gareth et al. 2013). This method entails' training the model by using some test data using a certain data set. A collection of "common and current regression and classification algorithms" for predictive analytics is known as "machine learning," or "statistical learning" (Gareth et al. 2013). Regression is used to forecast quantitative data, whereas classification is used to forecast categorical data. To train and test the model, a few datasets are employed. The testing data set's main objective is to assess how well a trained model generalizes Alpaydin, (2010). The model is validated after it has been trained.

2.5 Theoretical Literature

A theoretical framework is utilized in a research project to make predictions about the relationships between variables, and it has an impact on every choice made throughout the process (Lloyd, R., & Mertens, 2018). The management system theory states that in order to secure information assets, an ISMS must be documented.

2.5.1 Contingency Security theory

The detection, prevention, and response to threats and vulnerabilities that occur in an information system are all covered by this theory. It is in charge of the security implications both inside and outside the company. The information system analyst, according to this approach, must consider information security management elements. Security controls, policy actions, and management activities are among the characteristics that can assist mitigate risks. The contingency theory examines and acknowledges the variables in order to fulfill the organization's security goals (Drazin & Van, 1995; Robbins, 2009). The information Security Model (ISM) was proposed with five security layers (Von Solms and colleagues, 1994).

a) Baseline
b) Idea
c) Prescribed
d) Current
e) Survival

Apart from ideal level, all other four are dependent on the environmental conditions within the information system. The contingency theory approach is based on the following major functions:

a) Contingency Management-Organization management & control.
b) Information Security Strategy-policy orientation, audit & control, risk management.

With respect to the proposed research, the theory was useful since it helped to analyze and recognize the variables in order for the organization to achieve the security objectives. According to theoretical procedures, the methods for dealing with information security problems are indeterminate because they are based on situational variables. As a result,

an organization's contingency plan dictates whether or not to participate in policy-oriented managerial or risk management activities. Since the contingency approach to information security management has been implemented, this theory has influenced the investigation into how integrity can be compromised. A fivelevel information security model (ISM) with ideal, prescribed, baseline, current, and survival levels was put forth by Solms et al. in 1994. All four levels are dynamic and reliant on external factors such as information security threats, vulnerabilities, and business effect, with the exception of the ideal level. The solutions are based on various environmental factors thus the techniques for dealing with corporate information security concerns are mostly ambiguous.

2.5.2 Management System Theory

The relationship between organizations and the environment in which they operate is examined in management systems theory. This focus is focused on a company's ability to adapt to its surroundings (Katz & Kahn, 1978). A security architecture for information that integrates business needs, significant security plans, security services, security procedures, and security goods and technologies is called SALSA, according to Sherwood's (1996) proposal. It was based on security plans and organizational requirements. This theory has an impact on the study because it emphasizes the importance of a documented ISMS in a university setting for regulating and maintaining information assets like login credentials and data.

2.5.3 Integrated System Theory

Contingency management is the primary focus of an integrated systems theory, according to Hong et al. (2003). Any aspect of managerial actions that must adapt to a rapidly changing environment could be highlighted. The practitioners are limited in terms of approaches and regulations. It's possible that this is due to a lack of a complete and cohesive philosophy of information security management. This strategy considers

control, policies about security dynamics, management of the risks and auditing from a variety of angles.

The author suggests an integrated system theory that, by combining management systems with contingency theories, might offer a more reliable foundation for upcoming empirical research. This theory serves as a framework for the investigation since it considers organizational behavior while managing information security and offers workable organizational security management solutions. Making security decisions may be aided by understanding organizational attitudes and conduct toward information security management (Solms, 2005). The researcher therefore used the integrated system theory to forecast the intended results of the investigation.

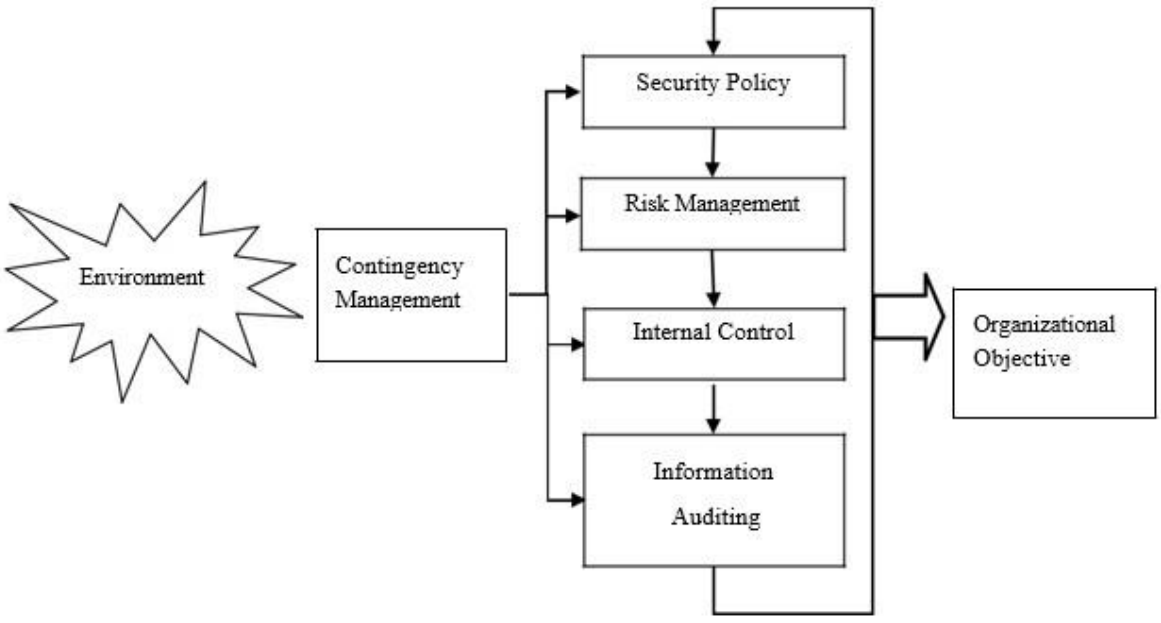


Figure 2 A diagrammatic illustration of integrated system theory Source: (Hong, Chi, Chao, & Tang, 2003, p. 253-248)

According to surveys, an organization's expertise is typically its most important asset. In order to run their daily operations, both public and private institutions rely substantially on information. Information system security can be compromised relatively quickly

(Pearson, 2013). Management in many countries also demands that proper precautions be taken to lessen the risk connected to the business and the use of ICT systems. Some of the issues that such legislation might address include healthcare, financial markets, privacy, and data security.

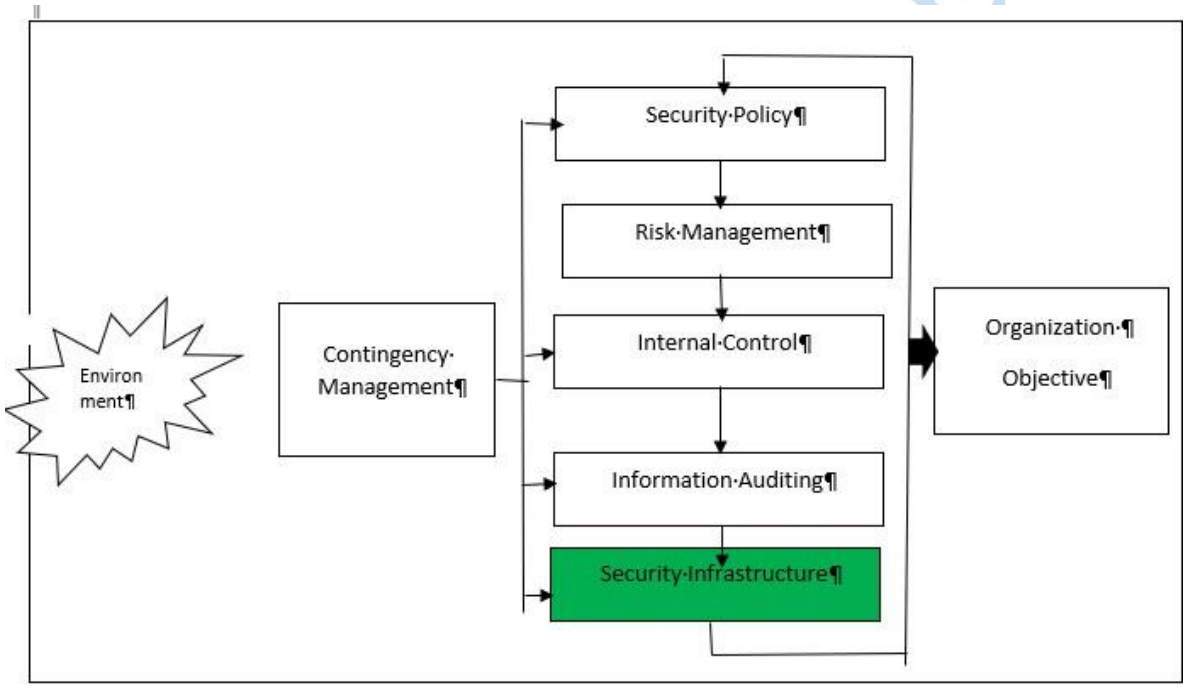


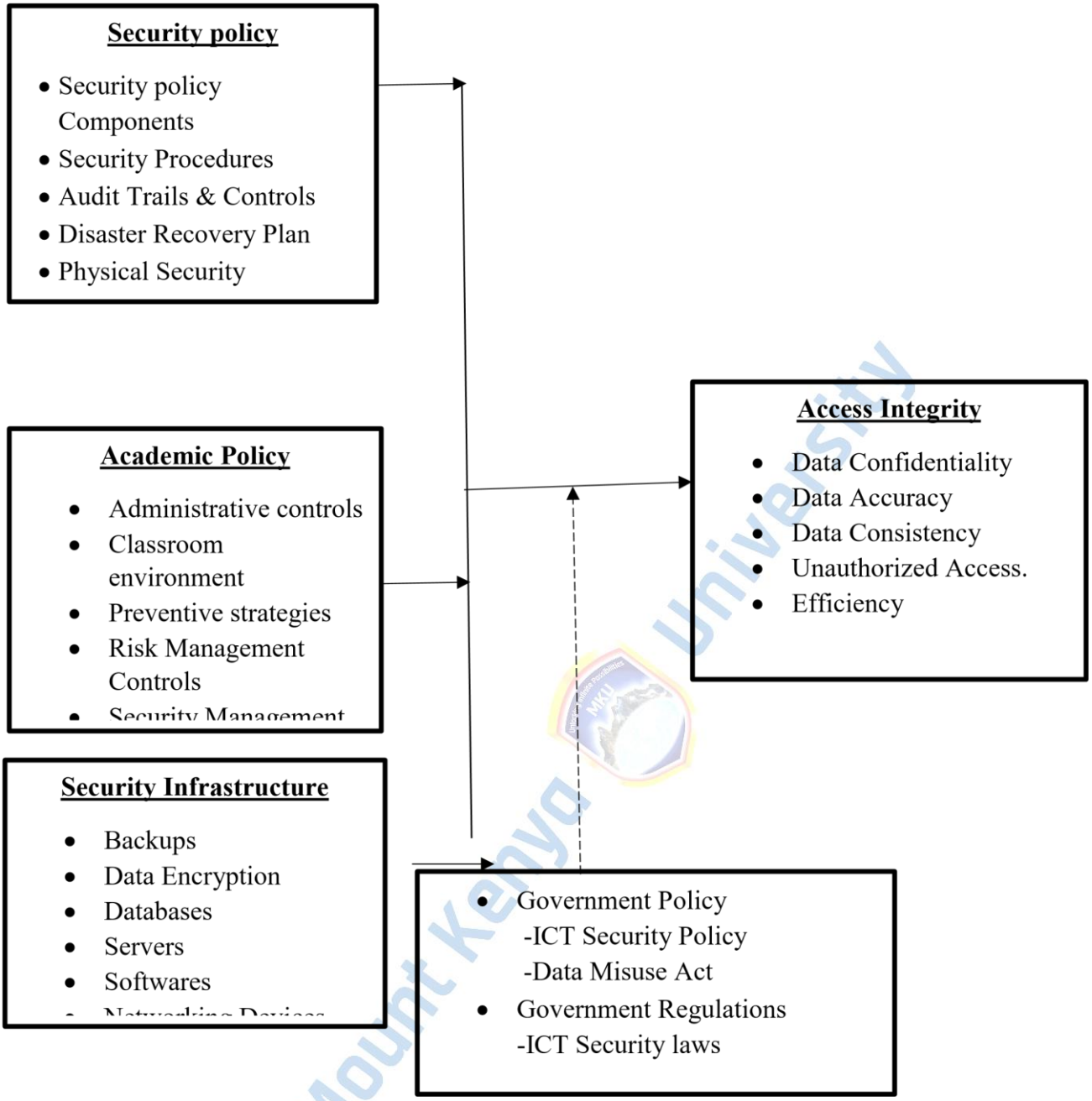
Figure 3 Diagrammatic illustration of the extended integrated system theory

The researcher extended the theory by adding the infrastructure component which was ideal in model implementation. The feature transformation within the developed model represented the component which was also reflected in the conceptual framework. Infrastructure and technical safeguards are important, but management also needs to invest in "making good security behaviours part of the business process, converting humans from risks into the first line of defence in the organization's security posture"

(Olavsrud, 2015). Leaders must first comprehend the full range of human security risks and how they will impact their personnel before they can take this step.

2.6 Conceptual Framework

Figure 4 shows the various relationships between three variables. The dependent, Independent and the intervening variables. The intervening variables are those that affect both the dependent and the independent variables such as government security policies and other regulations such as the ICT laws. The integrity of the palm vein Technology depends on the IT security policy, academic policy and the security infrastructure in the organization. The principle of relative advantage in Diffusion of innovation theory will have a great impact to my conceptual framework since it acknowledges that a new technology is superior to the currently biometric technology. The contingency theory will be helpful in relation to the suggested research since it will aid in the analysis and recognition of the variables necessary for the organization to fulfill the security objectives. The researcher thinks that despite being more userfriendly, the additional security features will improve integrity. The administrative controls and physical control will be efficient in-service delivery as well as enhancing the integrity.



Conceptual Framework

Source Researcher (2021)

Figure 4 Conceptual Framework.

2.7 Summary

The chapter analyzed the various applications of biometric systems globally, regionally and locally. Related and recent studies in regards to palm vein models and algorithm used

were also discussed. The use of palm veins in HEIs has received scant research. The palm vein has been employed in Japan as a substitute for traditional library cards and to authenticate customers in the retail industry. The same palm vein technology has been employed by Carolina's healthcare to validate patients in the hospital. In 2005, Fujitsu. The use of palm vein technology in academic settings has not received significant research. Guleker and Keci (2014) concentrated on the usage of fingerprint biometric technologies for tracking attendance in Kenyan educational institutions. He didn't do any research on the usage of biometric systems to improve integrity. The fingerprint system for class attendance has failed since sometimes it fails to verify or recognize legitimate students due to wear of the scanner of poor ridges on the students' fingers and also, it's prone to cyber spoofing attacks as well as replay attacks. Debrah and Effah concentrated on the value of social factors for the adoption of biometric technologies in the Ghanaian elections of 2012 in their 2019 study. Various cyberattacks and cybercrime in higher education were also examined. With respect to the proposed research the integrated system theory will be useful since it will help to analyze and recognize the variables in order for the organization to achieve the security objectives. According to the theory procedures; the procedures of dealing information security problems are undefined since they depend on situational variables. Empirical studies, research gap theoretical and conceptual framework were also discussed. For upcoming empirical study, the author suggests an integrated system theory that offers a more reliable model. This could be used to predict organizational attitudes and behavior with regard to information security management to assist with security decisions (Safa & Solms, 2016). The IST only concentrates on the security policy, internal controls, risk management, and information audits that can be used to achieve the objectives of the firm. There is a research gap since the theory does not concentrate on the security infrastructure, a crucial variable in the

model. By introducing the security infrastructure as a superior component that can be employed to improve the integrity, the researcher has expanded the notion.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter goes into detail on the methodological approaches that were used in the study. It contains information about the study's research design, sample layout, data gathering methods, research strategies, and data analysis methodology.

3.2 Methodology

The variables under investigation were determined using a mixed methodological approach with conjunction of an experiment to validate the science part of the study. The experiment was used to validate the science part of the study and determine the accuracy of the authentication systems based on FRR and FAR It was useful in investigating the strengths and weaknesses between services offered and the performance of the biometric systems**.** It was appropriate since it allowed the researcher to have a low level and a deeper understanding of the research. It was more appropriate strategy for answering research questions which ask ‘how’ and ‘why. Both methods supplemented each other by ensuring that was no biasness (Zang, 2014). The possibility of a hazard and the projected loss as a result of the organization's sensitivity to the threat determine risk exposure, whereas qualitative methodologies are determined by experts' assessments of potential losses (Bodin, Gordon, & Loeb, 2008). According to Feng and Li (2011), both methodologies should be employed when assessing the information security risk because of the intricacies of businesses.

According to Ryan, Mazzuchi and Cooke (2012), each methodology has flaws, therefore management bears the brunt of the responsibility for creating or executing either method or a hybrid approach, as well as adjusting in light with the information infrastructure. To address those flaws, management must design technical and social solutions.

Objective I: The researcher achieved this objective by using the research tools to obtain data from the respective area of study.

Objective II: The researcher achieved this objective by using Likert scale in the questionnaire that consisted of the academic policy, security policy and the IT infrastructure in the institution.

Objective III: The researcher achieved this objective by developing a logical security model. The logical model development was achieved by conducting systematic literature review from 50 journals from Google scholar where the best combination of components was obtained and also results obtained from the conducted experiment helped in the proof that the palm vein technology was the better model.

Objective IV: The researcher validated the implemented logical model by obtaining opinions from the experts.

3.2.1 Hypothesis

H0: The implemented contactless security logical model enhanced the integrity access of biometric data in Higher Education Institutions.

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

3.2.2 Parameters used in the experiment

The researcher conducted the experiment in Mount Kenya University. A biometric device that consisted of fingerprint and palm vein sensors was used in user registration and verification. The researcher used a control group during the experiment where 15 users were randomly selected during the experiment. Both staff and students were part of the control group. The researcher contacted potential volunteers and gave them an

explanation of the study's goals and inclusion/exclusion standards. After expressing interest in the study and meeting the requirements, participants were enrolled. Before participating in the study, the subjects gave their informed consent. This indicated that they were aware of the study's goals, the tasks they would be performing, and any dangers or advantages of taking part. The same users used both the fingerprint and the palm vein system. Some of the users had their fingerprint worn out while others had theirs in good condition, mad was applied in the fingers and palms to check the registration speed and authenticity. A timer was used to record the time taken to register and verify the user under the given conditions.

3.3.3 Exclusion and Inclusion Criteria

Inclusion Criteria: The researcher included the staff and the students of Mount Kenya University Thika Campus in the selected departments. The researcher focused on security issues related to biometric systems that could affect the integrity of the data.

Exclusion Criteria: The researcher excluded all other staff and students who were not part of Mount Kenya University Thika Campus.

3.3 Research Design

In this study, both an experimental and a descriptive research design were used. It is the general method used to bring together the many elements of a study in a way that makes sense and addresses the analysis (Polit & Hungler, 1999). Experimental research was used in this study because it involved figuring out the characteristics of an observed phenomenon or looking into potential relationships between two or more events. The experimental research was suitable since the researcher used a control group to conduct the experiment by manipulating the variables and observing the effects. The developed model based on the experiment outcome was validated by experts. The researcher focused on the staff and students of the university concerning the biometric systems as per this

study. The experiment was essential to proof the concept that palm vein model was better than the fingerprint authentication system.

3.4 Location of the Study

The research was conducted in Mount Kenya University Main Campus Thika SubCounty.

3.5 Target Population

Population, as defined by Mugenda & Mugenda (2003), is the total number of people residing in a particular territory. A numerical measuring scale was employed to quantify the data before instrumentation and collection because it was assumed that the population in the study would be finite. The study's target population was Mount Kenya University's faculty and students. It was selected since the university has been using biometric systems for more than 7 years. They are used in class attendance, gate access, accessing specific rooms and student registration and verification. Most of the university staff and students have been using the technology either for access or verification within the premises. A large sample size was required since the researcher analyzed the data using the multivariate technique (Hair et al., 1995). However, in order to determine the sample size from a specific population for this study, the random table

2 below was used (Krejcie et al., 1998). The population was distributed with selected populations that consisted of all administrative assistants, staff in the school of social sciences, computing & informatics, education, Examination officers, security personnel and other departmental coordinators.

Table 1 Target Population and Sample Size

Target Type	Population	Sample size
Teaching & NonTeaching Staff	300	169

Source (Mount Kenya MIS, 2021)

Table 2 Sample size Table from a given Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	351
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	190	1200	291	6000	361
45	40	180	118	400	196	1300	297	7000	364
50	44	190	123	420	201	1400	302	8000	367
55	48	200	127	440	205	1500	306	9000	368
60	52	210	132	460	210	1600	310	10000	373
65	56	220	136	480	214	1700	313	15000	375
70	59	230	140	500	217	1800	317	20000	377
75	63	240	144	550	225	1900	320	30000	379
80	66	250	148	600	234	2000	322	40000	380
85	70	260	152	650	242	2200	327	50000	381
90	73	270	155	700	248	2400	331	75000	382
95	76	270	159	750	256	2600	335	100000	384

Source: Krejcie, et al, (1998)

Key: N-Target Population S-Sample Size.

Table 2 above helped to determine the sample size from a given population.

3.6 Sampling Procedures and Techniques

An approach to study sampling describes the steps performed by a researcher to select an appropriate sample (Saunders, 2016). It also outlines the process for calculating the sample size for the study.

3.6.1 Sample Size

The fewest number of observations needed for each test sample is known as the sample size. A sample could also be a subset of the entire population. Since the researcher used the multivariate technique to examine the data, a large sample size was necessary (Hair et al., 1995). The sample size was nevertheless determined for the purposes of this study using the random table in table 2 above.

3.6.2 Sampling Technique

Due to time, resource, and cost restrictions, sampling methodologies provide a set of procedures that allow a researcher to evaluate data from a unit or a sub-group rather than all potentially relevant components in order to optimize the amount of data needed (Saunders, 2016). For this investigation, the stratified random sampling approach was utilized to produce a diverse population. By reducing sampling error, the researcher was able to improve the sample's representativeness. The university's teaching and support employees were the strata that needed to be considered. Each stratum was subjected to random sampling. The target demographic sample for this study was chosen via random sampling. All items in the sample have an equal probability of being included when using the approach of random sampling (Baayen, & Davidson 2008). Respondents for this survey were given an equal chance to participate in random sampling.

3.7 Data Collection Methods

3.7.1 Data Collection Instruments

In addition to using surveys, the researcher also obtained secondary data from 50 periodicals relevant to the study field. 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. The study also conducted observations to see what was going on with the current fingerprint biometric technology on the university premises. Three sections made up the questionnaires. In the first portion, demographic data about the respondent was gathered. The second component was used to collect data on how the respondent thought the fingerprint biometric technology performed. This section gathers information on internal dynamics such as security policy, security infrastructure, and IT security metrics can affect biometric system performance and have a direct impact on service delivery. The final component gathered information on the respondent's perceptions of how biometric authentication influenced service delivery and how the suggested palm vein technology helped to improve data integrity. In Section B On a 5-point Likert scale, respondents were asked to rank contemporary biometric technologies. Which allowed them to express both negative and favorable feelings about them. The questionnaire was used to measure whether there is adequate training provided by the university management. This was because the university must ensure the security policy components such as training, disaster recovery plans, security procedures are enforced and followed in order to enhance the integrity. Also, it measured the academic policy administrative controls laid by the management and preventive mechanisms to enhance data integrity. Open and closed questionnaires analyzed the security infrastructure available such as backups that were used to restore the data once the security infrastructure had been compromised. A questionnaire was also used to validate the model with the experts and also during the experiment with the control group.

3.7.2 Data Collection Procedures

To accomplish the goals of the study, the researcher used the data collection methods at his disposal. Every survey question was developed with a particular goal in mind.

3.7.3 Reliability of the Instruments

Reliability, as defined by Jack and Clarke (1998), is the consistency with which research questions are responded to. Cronbach's Alpha was used to assess the reliability of the instruments on a scale of 0 to 1. A rating nearer to one than zero implies a high level of trustworthiness. Nonetheless, the study used a 0.7 reliability criterion, with a coefficient of less than 0.7 indicating that the sub components were not reliable 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.

3.7.4 Validity of the Instruments

A validity test can determine what a questionnaire is supposed to gather (Sullivan, 2011). It captures the inconsistencies or discrepancies between reality and explanations. Professionals knowledgeable in biometric systems and their performance were polled to determine the content validity. The experts expressed their opinions on whether the tools were appropriate. Addressing all of the issues that surfaced during the pilot study required the supervisors' counsel. Instruments' validity was evaluated with the aid of a research expert and the research supervisors. Given that a research instrument must be related to the variable being examined in order to be declared valid, it was chosen and included in the questionnaire. In a pilot study at Zetech University, the researcher tested the tools on a randomly selected sample of participants.

3.8 Data Analysis

Using the primary data that was acquired, processed, and reviewed, descriptive statistics for the study were generated. The association between the variables was ascertained by applying a regression model to the source data. Both the regression model and the correlation analysis were used in the study to determine the strength of the link between the variables. Data integrity was improved as a result of the new security model, as shown by the strong positive correlation of 0.792.

Multivariate regression equation that was used.

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

To determine whether or not the association between two or more variables is the result of pure chance, tests of statistical significance were utilized. The analysis addressed the problem of relationship relevance by allocating a probability that the model will show a relationship between the variables (Andre et al., 2011). The proposed model's suitability was evaluated using an ANOVA at 95 percent confidence level test of significance.

3.9 Ethical Consideration

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 fact that the respondents might request a copy of the report after it was finished was disclosed to them. In order to introduce the research to the responder and the proper authorities, the researcher received an introduction letter from Mount Kenya University.

The researcher considered any health and ethical issue that could be associated with the palm vein technology from experts and other scholars. The researcher was given

authorization to collect the data by the National Commission of Science, Technology, and Innovation (NACOSTI). Every precaution was taken to ensure that the participant's psychological well-being and physical integrity was not compromised in the search of knowledge and truth. There was no right or incorrect answer because the questions were posed in an objective, non-judgmental manner (Ringheim, 1995). Participants were informed about the study before submitting their consent forms, and participation was fully voluntary. The researcher ensured that the plagiarism report was less than 15% from the Turnitin system as per the university recommended standards. Finally, because the respondents were aware of the cultural norms in my research area, the study avoided using words or terminology that appeared to be sensitive to religion, handicap, marital status, or tribe.

3.10 Chapter Summary

The chapter focused on the methodologies, research design approach, location of the study, population and data collection instruments to be used in the research. Mixed methodology was used to avoid biasness since both the qualitative and quantitative techniques supplement each other. While the descriptive research design helped the learner analyze the questionnaire, the experimental research design was used to validate the scientific portion of the study. Regression analysis was used to conduct the research and evaluate the degree of connection between the variables. A research permit from NACOSTI was required by the researcher in order to collect the data for the study.

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSION

4.1 Introduction

As outlined in the research findings and discussions chapter, this chapter represented the data analysis, results, and comments of the research findings. The results were presented

using tables, pie charts, and frequency tables. The data for each objective was examined, the results were discussed, and diagrams were used to help with understanding.

4.2 Demographic Characteristics of Respondents

4.2.1 Questionnaire Response Rate

The researcher conducted a pilot study in Mount Kenya University Thika where he distributed 17 questionnaires to the staff in the selected area of study which represented 10% of the sample size. In the distribution, there was a statistically significant high response rate of 95% from the pilot study, simple random sampling was applied. A total of 300 respondents, or 169 respondents, made up the researcher's target group. The researcher gave out 169 questionnaires to the participants during the actual data collection, and 123 of them were returned, or 73% of the questionnaires that were filled out. A response rate of 50% is considered enough for analysis and reporting, a rate of 60% is considered good, and a rate of 70% or higher is considered extraordinary, according to Mugenda & Mugenda (2003). On the basis of this assertion, the response rate was very good. Everyone who worked in the study's chosen field had an equal opportunity of participation. The demographic data was based on the age, gender, marital status, departments in which participants worked, level of education, Duration in which the participants had worked in the HEI's and their careers.

Table 3 Demographic information

Gender		**Count**
Male or Female	Male	52
	Female	71
	Subtotal	123

Source: Field data (2021)

Table 3 above displays the gender of the study's participants. There were 52 male which represented 42% while there were 71 females which represented 58% a cumulative total of 123 which attributes to 100%.

Demographic Information						
			Frequency	Percent	Valid Percent	Cumulative Percent
Age	Valid	18-25	10	8.1	8.3	8.3
		26-30	21	17.1	17.4	25.6
		31-35	42	34.1	34.7	60.3
		36-40	42	34.1	34.7	95.0
		41-45	4	3.3	3.3	98.3
		Above 45	2	1.6	1.7	100.0
		Total	121	98.4	100.0	
	Missing	System	2	1.6		
	Total		123	100.0		
Education Level	Valid	Certificate/Diploma	17	13.8	14.0	14.0
		Bachelor's Degree	62	50.4	51.2	65.3
		Master's Degree	36	29.3	29.8	95.0
		Phd	3	2.4	2.5	97.5
		Other	3	2.4	2.5	100.0
		Total	121	98.4	100.0	
	Missing	System	2	1.6		
	Total		123	100.0		
Career	Valid		11	8.9	8.9	
	System Administrator		2	1.6	1.6	10.6
	Lecturer		38	30.9	30.9	41.5
	Administrative Assistant		24	19.5	19.5	61.0
	Customer Care Representative		7	5.7	5.7	66.7
	Security Officer		9	7.3	7.3	74.0
	Director		2	1.6	1.6	75.6
	Other		30	24.4	24.4	100.0
	Total		123	100.0	100.0	
Working experience	Valid	1month-4years	6	4.9	4.9	4.9
		5-8 years	38	30.9	30.9	35.8
		9-12 years	55	44.7	44.7	80.5
		Above 12 years	22	17.9	17.9	98.4
			2	1.6	1.6	100.0

Source: Field data (2021)

The age range of the study's respondents was shown in Table 3 above. There were 123 participants but only 121 who stated their age while 2 never indicated their age. The majority of responders were between the ages of 31 and 35 and 36 and 40, with a frequency of 42 and 34.1 percent in each case. Those above the age of 45, who made up 1.6 percent of the respondents, were in the minority.

The respondents' educational levels were shown in Table 3 above. With a frequency of 62, or 50.4 percent of the total questionnaire response rate, degree holders were the majority. The masters holders were second with a frequency of 36 which is 29.3%, certificate/diploma came third with a frequency of 17 which is 13.8%,Phd and other respondents who never indicated their education level had 3 which attributed to 2.4%.There were two respondents who never selected the options availed in the questionnaire which attributed to 1.6%

The respondents' careers at Mount Kenya University Thika were depicted in Table 3 above. The majority of the responders (30.9 percent) were lecturers, with a frequency of 38. From the above analysis there were only 2 system administrators which is 1.6%. Customer care representatives were 7 which is 5.6%, administrative assistants were 24 which is 19.5%, security officers were 9 which is 7.3%. Security officers were very essential due to their strategic position at the entry points where students have to use biometric systems before they access the university premises as well as the library.24.4% respondents selected the other option where they specified their careers such as accountant and procurement officer.

The working length of all respondents who took part in the survey is shown in Table 3. 4.9 percent never stated how long they worked at Mount Kenya University. 44.7 percent of respondents have worked at the institution for 5-8 years, which represents the majority, while 1.6 percent have worked in the institution for more than 12 years, which represents the minority. 4.9 percent of respondents did not say how long they had worked.

4.3 Presentation of Findings

This part aimed to present the findings of the researches various objectives.

4.3.1 Objective 1: To investigate the effectiveness of existing security systems in Higher learning institutions

Which biometric technologies have you used before?

The purpose of the question was to find out what kinds of biometric systems the respondents had used previously. Fingerprint and voice recognition were among the technologies used. Systems for iris recognition, face recognition, and palm vein recognition are all available.

Table 4 Types of Biometric systems used by respondents

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

Source: Field data (2021)

According to Table 4 above, 68.3 percent of respondents had only ever used finger prints as a form of biometric identification. 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 was the fingerprint.

Table 5 Cyber Attacks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes No	115	93.5	93.5	93.5
		8	6.5	6.5	100.0
	Total	123	100.0	100.0	

Source: Field data (2021)

From table 5 above 93.5% of the respondents suggested that they had heard cyberattacks while 6.5% had not heard about them.

Table 6 Biometric Technologies Investment in the University

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Only one (Finger print)	102	82.9	83.6	83.6
	Several	17	13.8	13.9	97.5
	None	3	2.4	2.5	100.0
	Total	122	99.2	100.0	
Missing	System	1	.8		
Total		123	100.0		

Source: Field data (2021)

Table 6 above illustrated the type of biometric system that the university had invested before. From the analysis 102 respondents which attributes to 82.9% concluded that only one type of fingerprint systems had been invested before, similarly 17 respondents which attributes to 13.8% suggested that several types of technologies such as fingerprint and face recognition were being used, 2.4% suggested that none had been invested before while 0.8% never gave any suggestion.

Weaknesses of biometric systems

Table 7 Weaknesses of biometric systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	82	66.7	68.3	68.3
	No	37	30.1	30.8	99.2
	Not Sure	1	.8	.8	100.0
	Total	120	97.6	100.0	
Missing	System	3	2.4		
Total		123	100.0		

Source: Field data (2021)

According to the results of table 7 above, 66.7 percent of respondents agreed that the current security systems have flaws, 30.1 percent disagreed, 0.8 percent were unsure, and 3.4 percent did not respond to the question.

Table 8 Biometric system authentication

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	79	64.2	69.3	69.3
	No	34	27.6	29.8	99.1
	Not sure	1	.8	.9	100.0
	Total	114	92.7	100.0	
Missing	System	9	7.3		
Total		123	100.0		

Source: Field data (2021)

According to table 8, 64.2 percent of respondents agreed that the existing biometric system is vulnerable to manipulation, while 34 percent disagree. However, 0.8 percent were unsure, and 7.3 percent never responded.

Table 9 Hacking of MIS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	33.3	50.0 13.4	50.0
	No	11	8.9	36.6	63.4
	Not sure	30	24.4		100.0
	Total	82	66.7	100.0	
Missing	System	41	33.3		
Total		123	100.0		

Source: Field data (2021)

Table 9 above shows that 33.3 percent of respondents answered that MIS had ever been hacked, 8.9 percent disagreed, 24.4 percent were unsure, and 66.7 percent did not react to the question at all.

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

To investigate the current security systems at higher education institutions, a linear regression was done. The multiple linear regression shown below was developed. Regression coefficients, ANOVA, and a model summary were utilized to display the results.

Table 10 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)

The R2 value of R2 = 0.792 on the association between the analyzed dependent and independent variables indicates that the model fit well because it incorporated more than half of the test items utilized in the case study.

Table 11 ANOVA on the investigate the effectiveness of existing security systems in Higher learning institutions

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

ANOVA[a]

Model		Sum Squares	of 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)

We were unable to demonstrate the null hypothesis that there was statistical significance between the variables used to investigate existing security systems and Higher education institutions, based on the model summary in table 11 above, which showed an F-value of 0.763 at (12, 81), which was lower than the table value of 1.95.

Table 12 Regression Coefficients on the investigate the effectiveness of existing security systems in Higher learning institutions

Coefficients					
Model	Unstandardized Coefficients B	Std. Error	Standardized Coefficients Beta	t	Sig.
(Constant)	1.984	1.601		1.240	.000
How regularly do use biometric Technology	-.228	.315	-.081	-.724	.471
Which Biometric Technologies has your university before (mark all applicable)	.161	.376	.050	.427	.670
How long has your organization invested on the use of biometric technology?	.514	.374	.166	1.376	.173
Which biometric technologies is your organization still investing on? Mark all applicable	-.274	.360	-.089	-.760	.449
Do you think the current biometric system can be hacked?	.182	.365	.065	.498	.620
Have you heard of cyber-attacks?	.269	.705	.043	.381	.704
Do the current biometric system have weaknesses	.639	.385	.228	1.657	.101

Will the proposed palm vein security technology help to enhance the data integrity in service delivery?	.005	.432	.002	.013	.990
Is there a scenario when the current biometric system had failed to authenticate you? Does the current biometric system have weakness?	-.409	.392	-.145	-1.043	.300
Do you think the current biometric system has been integrated well with MIS to support all the services?	-.105	.314	-.038	-.335	.738
Do you think we can have biometric cyber spoofing a form of hacking where someone may use fingerprint information copied in artificial silicon finger in order to access the system?	-.248	.358	-.086	-.691	.492

Source: Field data (2021)

Because the p-value of 0.000 was less than p = 0.05, the multiple linear regression equation revealed there was statistical significance in the investigation of the existing security measures in higher education institutions.

The following multiple linear regression was formulated from the questions associated with the sub variables;

Equation 1: Sub variables for objective 1

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 \beta_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \beta_8 x_8 + \beta_9 x_9$$

$$+ \beta_{10}x_{10} + \beta_{11}x_{11} + \beta_{12}x_{12} + \varepsilon$$

$$y = 1.984 - 0.228x_1 + 0.161x_2 + 0.514\beta_3 - 0.274x_4 + 0.182x_5 + 0.269x_6$$

$$+ 0.639x_7 + 0.05x_8 - 0.409x_9 - 0.105x_{10} - 0.248x_{11} + \varepsilon$$

The equation 1 above showed the relationship between the various sub variables in order to determine whether they are statistically significant in informing the correlation for a better security model.

X1 = How regularly do use biometric Technology\

X2 = Which Biometric Technologies has your university before (mark all applicable)

X3 = How long has your organization invested on the use of biometric technology?

X4 = which biometric technologies is your organization still investing on? Mark all applicable

X5 = Do you think the current biometric system can be hacked?

X6 = Have you heard of cyber-attacks?

X7 = Do the current biometric system have weaknesses

X8 = Will the proposed palm vein security technology help to enhance the data integrity in service delivery?

X9 = is there a scenario when the current biometric system had failed to authenticate you? Does the current biometric system have weakness?

X10 = Do you think the current biometric system has been integrated well with MIS to support all the services?

x11 = Do you think we can have biometric cyber spoofing a form of hacking where someone may use fingerprint information copied in artificial silicon finger in order to access the system?

High number of respondents indicated that there were high chances of current biometric system have weaknesses with a coefficient of + 0.639, followed by how long has your organization invested on the use of biometric technology with positive 0.514, while some factors like how respondents thought of the current biometric system has been integrated well with MIS to support all the services and regularly do use biometric Technology had lesser impact with -0.105 and -0.228 respectively.

4.3.2 Objective 2: To assess the IT Security factors that influences the integrity of biometric systems in higher learning institutions

The researcher analyzed the security policy, academic policy, integrity and the security infrastructure. Under security policy the constructs consisted of the following Security policy Components, Security Procedures, Audit Trails & Controls, Disaster Recovery Plan, Physical Security and Training. The academic policy consisted of the following constructs, administrative controls, Classroom environment, and Preventive strategies, risk Management controls, security and management Controls.

4.3.2.1 Regression Results assess the factors that influences the integrity of biometric systems in higher learning institutions

The assessment of IT security parameters that affected the integrity of biometric systems in higher education institutions was done using a linear regression. Regression coefficients, an ANOVA summary, and the results of the model were shown.

Table 13 Model Summary on the assess the factors that influences the integrity of biometric systems in higher learning institutions

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.486[a]	.734	.112	1.31585

Source: Field data (2021)

The data on the factors that affected the integrity of biometric systems in higher education institutions fit the model well, as shown in Table 13 above, with an R^2 of 73.4 percent. As a result, other variables not considered by the study only had a 26.6 percent impact on examination malpractice in public and private universities.

Table 14 ANOVA on the assess the factors that influences the integrity of biometric systems in higher learning institutions

ANOVA[a]

Model		Sum Squares	of df	Mean Square	F	Sig.
1	Regression	49.373	15	3.292	1.901	.033[b]
	Residual	159.294	92	1.731		
	Total	208.667	107			

Source: Field data (2021)

An F value of 1.901 in table 14 was obtained in the ANOVA model summary this was less than the table value at (15,92) which is 0.032818 at 95% confidence interval this indicating that there was a statistical significance on the on the assess the IT security metrics that influences the integrity of biometric systems in higher learning institutions.

Table 15 Regression Coefficients on the assess the security factors that influences the integrity of biometric systems in higher learning institutions

Coefficients

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	4.817	1.468		3.281	.001
	IT security policy is a priority within your organization?	-.440	.271	-.187	-1.623	.108
	Cyber Security risks assessments are performed periodically?	.059	.204	.035	.289	.773
	The university has implemented various administrative controls to ensure data integrity?	-.643	.241	-.372	-2.668	.009

There is public awareness in cyber security within the university	.465	.198	.308	2.346	.021
The university management has the responsibility to ensure the organization administrative controls are enforced?	.057	.239	.026	.240	.811
There is investment in cyber security research & development	.189	.196	.109	.963	.338
There is adequate training on ensuring data security	.318	.206	.227	1.540	.127
The university has implemented effective security mechanisms in class signing up	.343	.184	.264	1.867	.065
The university has a disaster recovery plan to restore systems after security attack	-.230	.216	-.140	-1.063	.291
The university support the development of professional training courses in cyber security	.023	.190	.015	.119	.905
I feel that the university has implemented physical security measures	-.081	.047	-.169	-1.722	.088

The university has a log file to conduct audit trails	.190	.211	.109	.901	.370
There are preventive strategies laid upon to prevent attacks	.014	.191	.008	.072	.943
Individuals within the company are at risk of manipulation from confidence tricksters	-.007	.104	-.007	-.068	.946
I feel that information systems provide all the protection a university requires	-.636	.169	-.450	-3.762	.000

Source: Field data (2021)

The multiple linear regression equation showed a statistical significance towards investigation on the IT security metrics that effects the integrity of biometric systems in higher education institutions since the p-value of 0.001 was less than p = 0.05

The following multiple linear regression was formulated;

Equation 2: Subvariables for objective 2

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 \beta_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \beta_8 x_8 + \beta_9 x_9 + \beta_{10} x_{10} + \beta_{11} x_{11} + \beta_{12} x_{12} + \beta_{13} x_{13} + \beta_{14} x_{14} + \beta_{15} x_{15} + \varepsilon$$

$$y = 4.817 - 0.440 x_1 + 0.059 x_2 - 0.643 x_3 + 0.465 x_4 + 0.057 x_5 + 0.189 x_6 + 0.318 x_7 + 0.343 x_8 - 0.230 x_9 + 0.023 x_{10} - 0.081\ x_{11} + 0.190 x_{12} + 0.140 x_{13} - 0.007 x_{14} - 0.636 x_{15}\ \varepsilon$$

Where the x includes questions used to represent the variables; x1 = IT security policy is a priority within your organization? x2 = Cyber Security risks assessments are performed periodically?

x3 = The university has implemented various administrative controls to ensure data integrity?

x4 = There is public awareness in cyber security within the university x5 = The university management has the responsibility to ensure the organization administrative controls are enforced?

x6 = There is investment in cyber security research & development x7 = There is adequate training on ensuring data security x8 = The university has implemented effective security mechanisms in class signing up x9 = The university has a disaster recovery plan to restore systems after security attack x10 = The university support the development of professional training courses in cyber security x11 = I feel that the university has implemented physical security measures

x12 = The university has a log file to conduct audit trails x13 = There are preventive strategies laid upon to prevent attacks x14 = Individuals within the company are at risk of manipulation from confidence

tricksters x15 = I feel that information systems provide all the protection a university requires The equation 2 above showed the relationship between the various sub variables in order to determine whether they are statistically significant in informing the correlation for a better security model. It was based on the academic and IT security policies.

Given that people are the weakest link in any security chain, the findings on Table 15's findings indicated that public awareness was crucial in order to understand how cyberattacks happened and the various mitigation strategies the institution should implement. It was evident that the security policy was not a priority within the university since the coefficient was at -0.440. It was evident that the university had not laid effective administrative controls to restore systems after a cyber-attack since there was a correlation of -0.23.

4.3.3 Objective 3: To develop a logical security model that enhances integrity access of biometric systems in higher learning institutions.

The purpose was to develop a contactless security model that was more secure and efficient.

Table 16 Loop holes in current biometric system

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	52	42.3	44.4	44.4
	No	34	27.6	29.1	73.5
	Not sure	31	25.2	26.5	100.0
	Total	117	95.1	100.0	
Missing	System	6	4.9		
Total		123	100.0		

Source: Field data (2021)

According to table 16 above 42.3% of the respondents claimed that the biometric system has loopholes that could allow illegitimate personnel access the data.27.6% reject the above narrative.25.2 were not sure while 4.9% never responded to the question.

Table 17 Authentication Failure of biometric system

		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)

According to Table 17, 59.3 percent of respondents had encountered a circumstance in which the present biometric technology failed to verify 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.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.

Table 18 Hacking of the current biometric system

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	76	61.8	63.3	63.3
	No	42	34.1	35.0	98.3
	Not Sure	2	1.6	1.7	100.0
	Total	120	97.6	100.0	
Missing	System	3	2.4		
Total		123	100.0		

Source: Field data (2021)

From table 18 above 61.8% of the respondents suggested that the current biometric system can be hacked which was more than 50% of the respondents.34.1% of the respondents ascertained that there was no way in which it could be hacked which was 34.1%.1.6% were not sure whether it could be hacked while 2.4% never responded to the question.

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

Table 19 Level Security of the proposed security system

		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 19 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. With a high percentage of 83.7% this demonstrated the need for having a better model that can be better for enhancing the security of the data.

4.3.3.1 Regression Results on implementing a logical security model using biometric systems for higher learning institutions

A linear regression was performed on the application of a biometric security model for academic institutions. Table 20 below displays regression coefficients, an ANOVA summary, and the model's outcomes.

Table 20 Model summary on the implementation of a logical security model using biometric systems for higher learning institutions

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.264[a]	.70	-.034	1.43407

Source: Field data (2021)

Table 20 shows that the data matched the model well on the creation of a security model employing biometric technologies for higher learning institutions, with an R2 of 70.0 percent.

Table 21 ANOVA implementation of a logical security model using biometric systems for higher learning institutions

ANOVA[a]						
Model		**Sum Squares**	**of df**	**Mean Square**	**F**	**Sig.**
1	Regression	15.147	11	1.377	.670	.764[b]
	Residual	201.544	98	2.057		
	Total	216.691	109			

Source: Field data (2021)

We reject the null hypothesis that there was statistical significance in the design of a security model using biometric systems for higher education institutions because a F value of 0.670 was obtained at (11,98) at 95 percent confidence interval, which is less than the table value of 0.763534 at 95 percent confidence interval according to table 21 above.

Table 22 Regression coefficient on the implementation of a logical security model using biometric systems for higher learning institutions

Coefficients						
Model		**Unstandardized Coefficients B**	**Std. Error**	**Standardized Coefficients Beta**	**t**	**Sig.**
1	(Constant)	3.020	1.184		2.551	.012
	I feel the university is ready to counter cyber attacks	.140	.185	.091	.760	.449
	I feel that the organization do not have adequate firewalls to counter attacks	.085	.125	.075	.677	.500
	I think that management have the responsibility to ensure the organization has implemented encryption techniques	.170	.219	.087	.776	.440

The university has a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure	-.177	.228	-.098	-.776	.439
There are adequate backup methods to restore data in case of attacks	.096	.228	.053	.419	.676
I feel that the university is using cloud servers or databases for backups	-.152	.231	-.083	-.660	.511
The university has updated the software's to ensure there are no loop holes	-.396	.212	-.225	-1.869	.065
The biometrics being used in the university are failing to verify users	.011	.120	.010	.089	.929
I feel that malicious attacks can be detected by intrusion detection systems installed by the university	.107	.186	.071	.573	.568
I feel that the biometrics systems and MIS have been integrated well	-.021	.178	-.017	-.118	.907
Computer systems provide all the protection a company needs	.112	.165	.089	.680	.498

Source: Field data (2021)

Equation 3: Subvariables for objective 3

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 \beta_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \beta_8 x_8 + \beta_9 x_9 + \beta_{10} x_{10} + \beta_{11} x_{11} + \beta_{12} x_{12} + \varepsilon$$

$$y = 1.984 + 0.140 x_1 + 0.085 x_2 + 0.170 x_3 - 0.177 \beta_4 + 0.096 x_5 - 0.152 x_6 - 0.396 x_7 + 0.11 x_8 + 0.107 x_9 - 0.021 x_{10} + 0.112 x_{11} + \varepsilon$$

x1 = I feel the university is ready to counter cyber-attacks x2 = I feel that the organization do not have adequate firewalls to counter attacks x3 = I think that management have the responsibility to ensure the organization has implemented encryption techniques.

x4 = The university has a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure x5 = There are adequate backup methods to restore data in case of attacks x6 = I feel that the university is using cloud servers or databases for backups x7 = The university has updated the software to ensure there are no loop holes x8 = The biometrics being used in the university are failing to verify users.

x9 = I feel that malicious attacks can be detected by intrusion detection systems installed by the university. x10 = I feel that the biometrics systems and MIS have been integrated well . x11 = Computer systems provide all the protection a company needs.

Table 22 above showed the regression parameters on the design a security model using biometric systems for higher learning institutions and their respective coefficients. It was found out that there were adequate backup methods to restore data in case of attacks and

how they feel that the university is using cloud servers or databases for backups had the lowest contribution towards design a model using biometric systems for higher learning institutions since they had the lowest coefficient of -0.152 and 0.396 respectively while those contributed highly where computer systems provided all the protection a company needs with a coefficient of 0.112.

4.3.3.2 Experimental Results

The controlled group consisted of 15 students randomly selected from the university. During the experiment some participants had their palms and fingerprints wet and dirty while some were worn out.

Demographic information of the group

Table 23 Gender of the control group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	9	60.0	60.0	60.0
	Female	6	40.0	40.0	100.0
	Total	15	100.0	100.0	

Source: Field data (2021)

From the experiment that was conducted using a control group, 60% of the participants were males while 40% were females. Both participants used the fingerprint and palm vein authentication systems according to table 23 above.

Table 24 Control Group Participant's level of education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Master's Degree	2	13.3	13.3	13.3
	Bachelor's Degree	13	86.7	86.7	100.0
	Total	15	100.0	100.0	

Source: Field data (2021)

From table 24 above 86.7% were degree students while 13.3% were master's students within the university.

Table 25 Duration of the control Group in the university

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1 year	2	13.3 53.3	13.3 53.3	13.3 66.7
	1-2 years	8	26.7	26.7	93.3
	3-5 years	4			
	Above 5 years	1	6.7	6.7	100.0
	Total	15	100.0	100.0	

Source: Field data (2021)

According to table 25 above, 53.3% had been in the University for 1-2 years, 26.7% between 3-5 years, 13.3% less than a year while 6.7% more than 5 years. The control group was suitable since more than 80% had been within the university more than one year thus they had used the current fingerprint system that was being used.

Table 26 Biometric technologies used by control group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Fingerprint several	12	80.0	80.0	80.0
		3	20.0	20.0	100.0
	Total	15	100.0	100.0	

Source: Field data (2021)

According to table 26 above 80% of the participants had used fingerprint system while 20% had used more than one technology.

Table 27 Suitable authentication system

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

Source: Field data (2021)

Table 27 above shows that 93.3 percent of the participants ascertained the palm vein (contactless) system was superior to the existing fingerprint system, which only received 6.7 percent of the vote. 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 28 Experimental Performance accuracy analysis of Palm and fingerprint biometric scheme using FAR and FRR

User:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Palm Vein	P	P	P	P	P	F	P	P	F	P	P	P	P	P	P
FAR Cases	0								**FAR**= (0/15) *100=0%						
FRR Cases	1								**FRR**= (1/15)*100=6.67%						
Verification Time (sec)	7	15	7	8	9		6	8		5	12	9	6	11	16
Fingerprint	P	P	F	F	F	F	P	P	P	P	F	P	F	P	P
FAR Cases	2								**FAR**= (2/15)*100=13.3%						
FRR Cases	6								**FRR**= (6/15)*100=40%						
Verification Time: (sec)	2	4					3	2	2	3		3		4	1

Key: P=Pass;F= Fail

FAR = (Number of False Acceptances / Total Number of Tests) x 100

FRR = (Number of False Rejections / Total Number of Tests) x 100

By calculating both FAR and FRR, we can determine the accuracy of the fingerprint system and fine-tune the system parameters to improve accuracy. From the data in table 28 above the palm vein system had a FAR of 0% indicating that no false user was authenticated to the system as compared to the fingerprint which had to 2 cases which

represented 13.3% of the test items which were 15 users in the control environment. An FRR of 40% was obtained from the fingerprint system compared to 6.67% obtained from the palm vein system. From the results above, it showed that the palm vein scanner was better in authentication as compared to the existing fingerprint system. The threshold was only one attempt therefore the total number of tests were 15.

The average authentication time for palm vein was 9.15 seconds while Fingerprint was 2.67 seconds. Therefore, with respect to speed fingerprint was better as compared to the palm vein. The factors that necessitated low authentication speed in pal was the structure of the hand and the distance between the palm and the scanner.

To calculate the accuracy rate of each system, we need to subtract the error rate (FRR) from 100%.

For the fingerprint system:

Accuracy rate = 100% - FRR

= 100% - 40% = 60%

For the palm vein system:

Accuracy rate = 100% - FRR

100% - 6.67% = 93.33%

Therefore, the accuracy rate of the fingerprint system is 60%, while the accuracy rate of the palm vein system is 93.33% thus palm vein was the better model to be implemented in the higher education institution.

Table 29 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)

The replies from the participants in the control group are displayed in Table 29 above, while 9.3% were neutral, 93.3% strongly agreed that the palm vein contactless security system is more accurate and secure in authentication than the fingerprint system. 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. 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 5 Palm Device Scanner (2021)

Figure 5 above shows the scanner scanning the palm of the user. The hybrid scanner contained the finger print, palm vein and access card.

4.3.3.3 Model Implementation

The logical model was implemented to enhance the current security system. The researcher analyzed the existing model components and identified a component that was missing which was used to extended the existing model and formed a key component in the extended integrated system theory. It had the following components (features); image acquisition, image processing, feature extraction, **feature transformation**, database and feature matching. A new component was added to the existing models which was the feature transformation which represented the infrastructure variable in the conceptual framework. Feature transformation is an important component in biometric systems as it

is responsible for converting the raw input biometric data into a new representation that is more suitable for processing and comparison. These techniques aim to reduce the dimensionality of the data while preserving important biometric features and enhancing discriminative power between individuals. Feature transformation is essential for effectively processing biometric data and for improving the accuracy, speed, and reliability of biometric systems.

Scale-invariant feature transform (SIFT) should be used to transform the extracted features into a better image component. The components of the present models included picture acquisition, feature extraction, image processing, and image storage. Random Sample Consensus (RANSAC) may be used to enhance the integrity of the recovered characteristics. The method is used to determine the number of outliers that fall within the parameters of a predetermined threshold distance within a predetermined number of computing iterations. This component should be added and made mandatory in all palm vein authentication systems since it can enhance more integrity during verification.

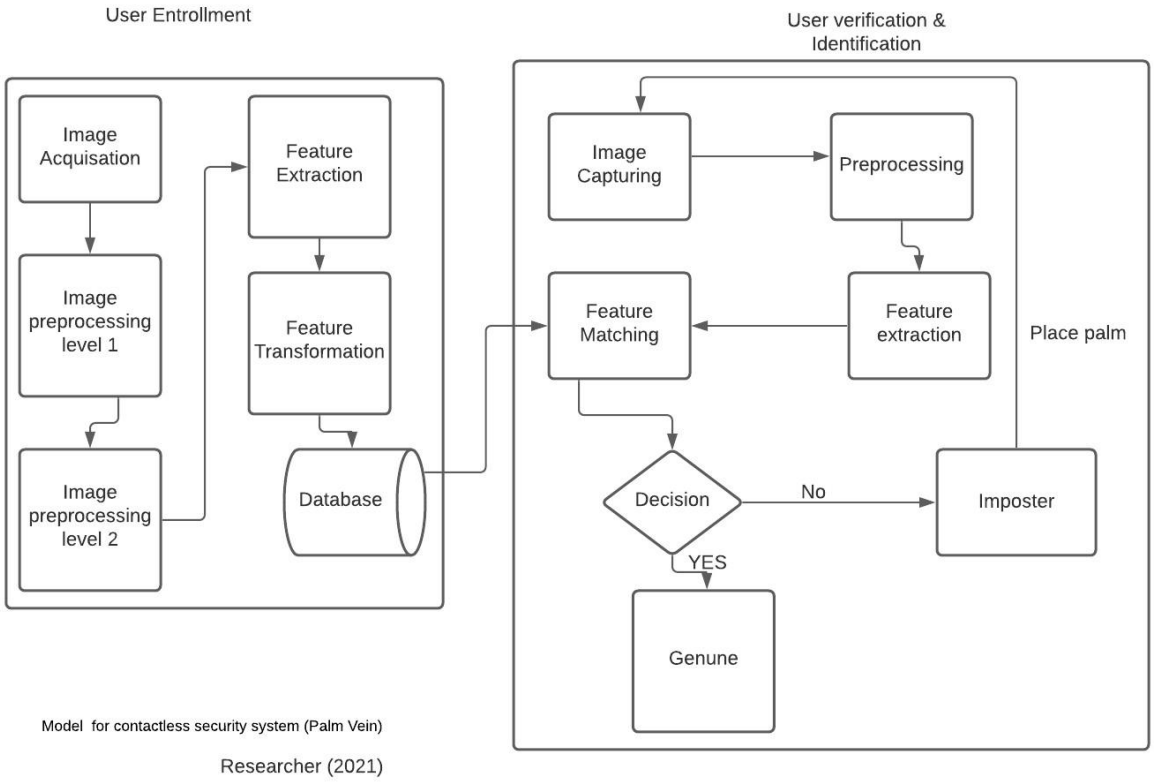


Figure 6 Implemented Logical Model for contactless security system (palm vein)

The model components have been discussed below.

a) **Image acquisition-** The device's CCD camera, which is near the bottom and surrounded by LEDs with different frequency spectra, is used to extract the image. Additionally, two models of contactless palm vein collecting devices were put forth by (Sierro et al., 2015). Both make use of reflected or mirrored light and have ultrasonic sensors that determine how far the camera is from the hand.

b) **Preprocessing (1) –** It entailed capturing of the images by using a camera. The collected image is converted into a grayscale version. This is essential since grayscale images can readily be edited after they are taken. The contrast in the image is also increased using histogram equalization. This facilitates the details' precision and clarity.

c) **Preprocessing (2) -** The NIR or CCD camera's images might or might not have no noise. To obtain a distinct vein pattern, noise must be eliminated. A median filter is used to do this. The foreground and background are then seen clearly thanks to thresholding. This is accomplished using the Otsu approach. It is a method of global thresholding that turns a grey image into a binary image by applying a threshold value.

d) **Feature extraction** - Several methods, including Gabor filters and geometricbased algorithms, are utilized to extract features. The image is first binarized, then skeletonized, and then line segments are produced. After preprocessing, the image quality is improved, but the vein pattern is still surrounded by a number of brittle white patches.

e) **Transformation**-The extracted features should be transformed into a better image component by using Scale-invariant feature transform (SIFT). The current models consisted of the following components, Image acquisition, feature extraction, image processing and storage. Random Sample Consensus (RANSAC) may be used to enhance the integrity of the recovered

characteristics. In a set number of computing iterations, the approach is used to count the number of outliers that fall inside the bounds of a predetermined threshold distance. In order to build a consensus, set, a sample of key point pairs is randomly selected from the SIFT matching results and its constituents are assessed to see if they are closer together than the threshold distance. Following the removal of an outlier, the procedure is repeated until the consensus set has the greatest number of outliers that satisfy the criteria (C. Vi, 2015). This component should be added and made mandatory in all palm vein authentication systems since it can enhance more integrity during verification.

f) **Storage**- According to the findings of the comprehensive literature study, CASIA is the most widely used database (Chinese Academy of Science Institute of Automation). The features of the photographs that were extracted were stored in the database. The closet decomposition approach is used to encode (or encrypt) the palm vein feature vectors, which are then recorded as registered templates in the system database (called encoded feature vectors).

g) **Template matching**- Template matching is the process of comparing an image to a base image. After iterating through numpy arrays with the image, the ratio of similarity is determined. This system uses TM CCOEFF NORMED template matching to match source and destination images. (Min Peng, 2016). PCA was used to compare the user-submitted palm prints to the stored template in order to verify the veracity of the prints.

Table 30 Logical Model components analysis

Table 30 below shows 20 of the 50 Google Scholar publications that were chosen at random and used to determine which parts or elements of the created Model were most popular.

	DATABASE			FEATURE EXTRACTS			MATCHING	DECISION	Sensor	
	CASIA	PUT	Poly U multi spectral palp m print	Gabor Filter	LBP Local Approa bina ry patt ern	Geometric ches	HAMMING DISTANCE	PCA	CCD Cam era	NI R
No of Papers	8	3	4	7	5	4	4	5	10	8

Source: Field data (2021)

The results of Table 30 demonstrate that CASIA (Chinese Academy of Science Institute of Automation) is the most often used database for security systems. Out of 20 journal publications, CASIA is used in 40%, PUT in 15%, Poly u Multispectral Palm print database in 20%, and CASIA in the remaining 25%. 20% of people use Hamming distance, 20% use geometric approaches, 25% use LBP, and 35% use Gabor filters for feature extraction. CCD cameras (50%) and NIR cameras (40%) are the most widely used cameras for sensors, with low cost usb cameras accounting for the remaining 10%. The application of Principle Component Analysis (PCA) in decision-making helps to validate and authenticate the user.

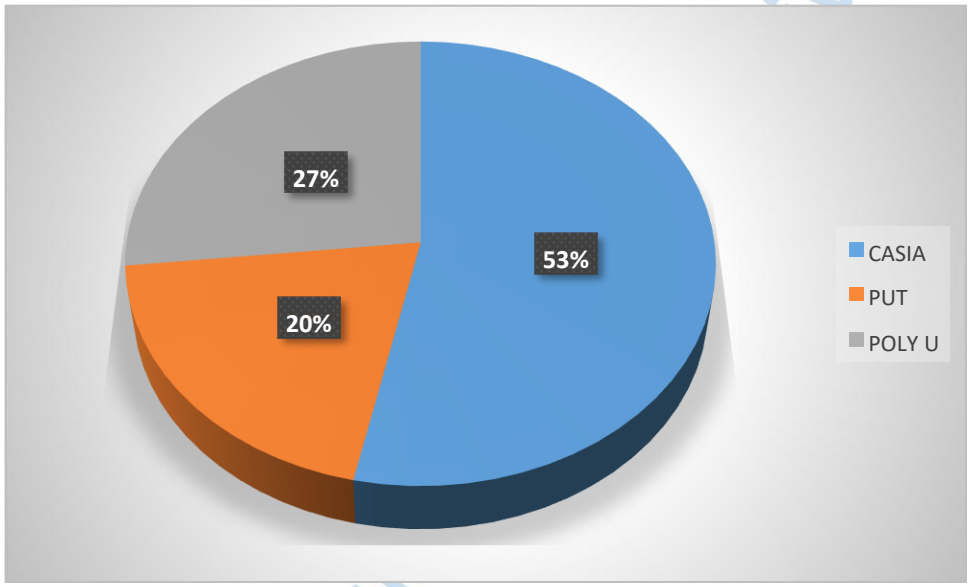


Figure 7 Databases

A depiction of well-known databases is shown in Figure 7 above, with CASIA leading with 53% of the total, PUT with 27%, and Poly U with 20%. According to the information above, the Pam vein device most frequently uses the CASIA database.

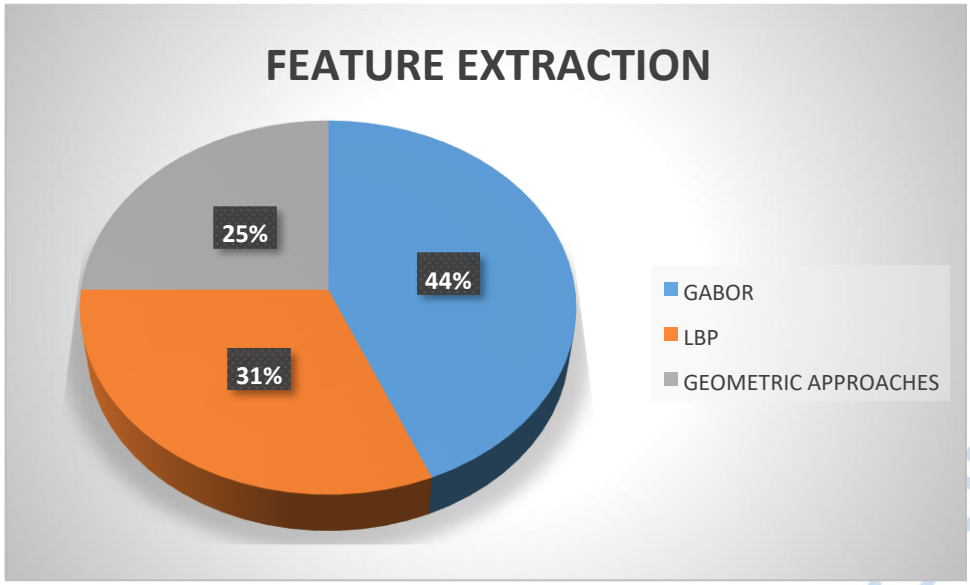


Figure 8 Methods for feature extraction

Figure 8 above shows the different feature extraction methods. The most widely used techniques include Gabor filter methods (44% of all usage), LBP (Local Binary Pattern) (31%), and geometric approaches (25%).

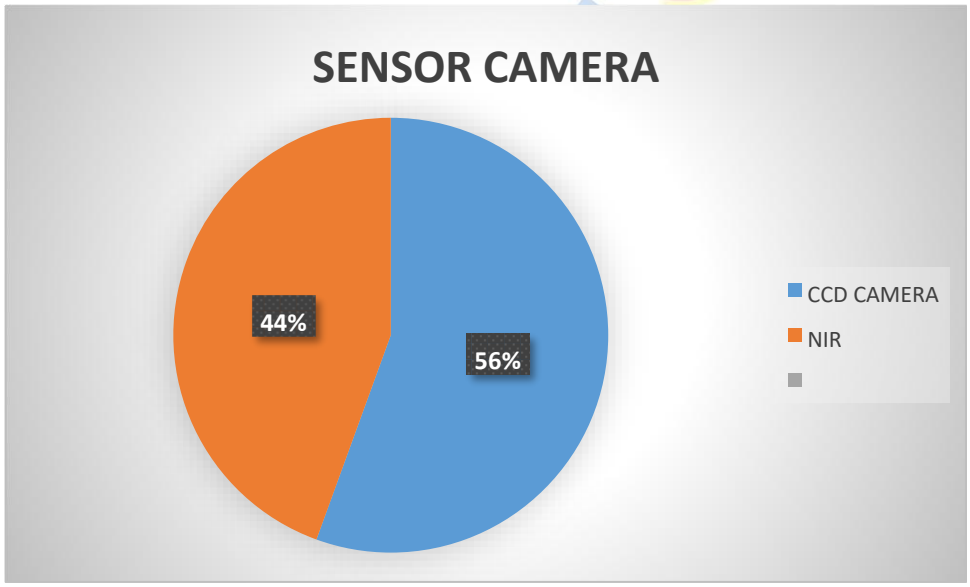


Figure 9 Model sensors

The many sensors employed are shown in Figure 9 above. 56 percent of cameras are CCD cameras, whereas 44 percent are NIR cameras.4.3.4 Objective 4: To validate the Model that will help enforce integrity by using palm vein biometric authentication system.

4.3.4 Objective 4: To validate the developed logical model that will help enforce integrity by using palm vein biometric authentication system.

4.3.4.1 Findings on the integrity issues

The researcher focused on the integrity issues and then validated the model by using expert.

Table 31 Model Summary for the model that will help enforce integrity by using palm vein biometric authentication system.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.329[a]	.108	-.043	1.37243

Source: Field data (2021)

Table 32 ANOVA for the model that will help enforce integrity by using palm vein biometric authentication system.

ANOVA[a]

Model		Sum Squares	of df	Mean Square	F	Sig.
1	Regression	13.455	10	1.345	.714	.708[b]
	Residual	111.131	59	1.884		
	Total	124.586	69			

Source: Field data (2021)

F value of 0.714 was obtained on the integrity by using palm vein biometric authentication system this is less than the table value at (1.70) degree of freedom (10, 59) which demonstrated that there was statistical significance.

Table 33 Regression Coefficient Results for the model that will help enforce integrity by using palm vein biometric authentication system.

coefficients

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	2.448	1.014		2.413	.019
	Do you feel that the university has utilized the levels of security products	-.215	.186	-.153	-1.157	.252
	Are login passwords deactivated immediately once an employee leaves the university	-.184	.227	-.118	-.813	.420
	Do you believe that the university sensitive data is protected by using strong passwords or other types of access controls	.313	.213	.216	1.468	.147
	Does the university maintain written policies or procedures related to the security controls over access to the system?	.074	.221	.047	.334	.739
	Are the scenarios where the integrated (MIs) has been hacked?	-.111	.231	-.076	-.482	.632
	If student and staff data is maintained on the servers, is security over the data sufficient to ensure with the university data security policy	-.002	.204	-.001	-.010	.992

Is the current biometric system consistent in validating and authenticating the users	-.493	.389	-.184	-1.268	.210
Does the current biometric system have loop holes that could allow unauthorized personnel modify existing data?	.283	.225	.182	1.258	.213
Does the current biometric system have the security features to detect fake login credentials of unauthorized modified data	.334	.295	.146	1.133	.262
Do you think the integration of biometric system and MIS will change the security dynamics	.416	.722	.087	.575	.567

Source: Field data (2021)

The following multiple linear regression was formulated based on the questions used for the variable;

Equation4: Subvariables for objective 4

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 \beta_4 + \beta_5 x_5 + \beta_6 x_6 + \beta_7 x_7 + \beta_8 x_8 + \beta_9 x_9 + \beta_{10} x_{10} + \varepsilon$$

$$y = 2.448 - 0.215 x_1 - 0.184 x_2 - 0.313 x_3 + 0.074 x_4 - 0.111 x_5 - 0.002 x_6 - 0.493 x_7 + 0.283 x_8 + 0.334 x_9 + 0.416 x_{10} + \varepsilon$$

X1 = Do you feel that the university has utilized the levels of security products.

x2 = Are login passwords deactivated immediately once an employee leaves the university

x3 = Do you believe that the university sensitive data is protected by using strong passwords or other types of access controls.

x4 = Do the university's security measures for system access have written rules or procedures in place? x5 = Are the scenarios where the integrated (MIs) has been hacked?

x6 = Is the protection over the data sufficient to ensure compliance with the university's data security policy if student and staff data is kept on the servers?

x7 = Is the current biometric system consistent in validating and authenticating the users.

x8 = Does the current biometric system have loop holes that could allow unauthorized personnel modify existing data?

x9 = Does the current biometric system have the security features to detect fake login credentials of unauthorized modified data.

x10 = Do you think the integration of biometric system and MIS will change the security dynamics

The equation 3 above showed the relationship between the various sub variables in order to determine whether they are statistically significant in informing the correlation for a better security model. A significant portion of respondents believed that the integration of the biometric system and MIS would change the security dynamics, as indicated by the coefficient of 0.416, according to the results of the multiple linear regression used to estimate the integrity of the palm vein biometric authentication system. Strong passwords were then found to be the most effective method of protecting university-sensitive data. With a coefficient of -0.002 and a low contribution based on student and staff data kept

on the servers, it can be inferred that the university's data security policy is not sufficient to ensure data security. However, other types of access controls were highly sensitive among the respondents, with a positive coefficient of

0.313.

4.3.4.2 Expert validation findings

The researcher sent 20 questionnaires to experts who were familiar with security issues regarding biometric systems.16 questions were answered which attributed to 80% questionnaire response rate. The researcher sought to determine whether the developed palm vein model covered all the needs.

Table 34 Expert Demographic information

			Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Valid	Male	13	81.3	81.3	81.3
		Female	3	18.8	18.8	100.0
		Total	16	100.0	100.0	
Education level	Valid	Degree	8	50.0	50.0	50.0
		Masters	8	50.0	50.0	100.0
		Total	16	100.0	100.0	
Specialization	Valid	Security Specialist	6	37.5	37.5	37.5
		Lecturer	8	50.0	50.0	87.5
		Administrator	1	6.3	6.3	93.8
		other	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
Years of experience	Valid	0-2 years	2	12.5	12.5	12.5 68.8
		3-5 years	9	56.3	56.3	75.0
		6-8 years	1	6.3	6.3	100.0
		Above 8 years	4	25.0	25.0	
		Total	16	100.0	100.0	

Source: Field data (2021)

According to table 34 above based on the expert gender 81.3% represented the male while 18.8% were females. Based on the level of education 50% had masters while 50% were degree holders. In specialization 37.5% were security specialists, 50% were lecturers, 6.3% administrator while other fields represented 6.3%. On the years of experience 56.3% had 3-5 years, 25% above 8 years, 0-2 years were 12.5% while the lowest was 6-8 years with 6.3%.

Table 35 Security Model needs coverage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes no	14	87.5	87.5	87.5
		2	12.5	12.5	100.0
	Total	16	100.0	100.0	

Source: Field data (2021)

According to table 35 above ,87.5% of the experts agreed that the security systems met the threshold of a system that can enhance the integrity of the data while 12.5% suggested that it had not meet the required threshold.

Expert knowledge of a secure control Model that guides companies to design and maintain secure processes, systems and applications

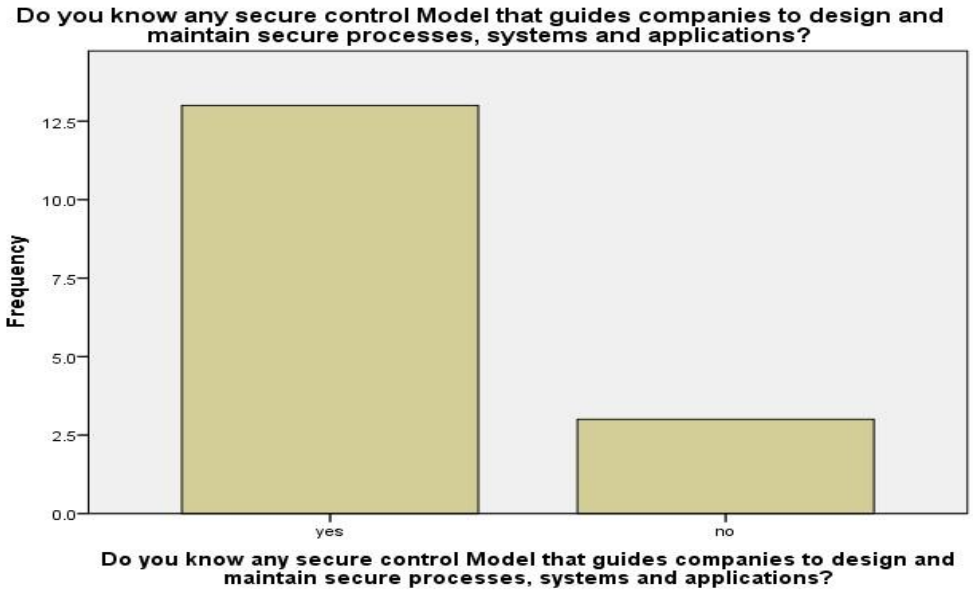


Figure 10 Expert knowledge of other se cure control Model

According to figure 10 above majority of the experts represented a frequency of 12.5 suggested that they are aware of other secure control models that guided organizations in the designing and maintaining secure processes of their systems and applications.

However, 2.5 of the respondents were not aware of any model.

4.3.4.3 Experts findings on usage dynamics of the contactless security systems

Table 36 Expert validation Model Summary

Model Summary

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

Source: Field data (2021)

From the table 36 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.

Table 37 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)

An F value of 1.671, which was smaller than the table value at (3.50) degree of freedom (8,7), was reached on the model validation with experts about the integrity by employing palm vein biometric authentication system, as shown in table 37 above. This showed that there was statistical significance. Therefore, we reject the null hypothesis.

Table 38 Regression Coefficient Results from experts for the model that will help enforce integrity by using palm vein biometric authentication system.

Model		Unstandardized Coefficients		Standardizedt Coefficients		Sig.
		B	Std. Error	Beta		
1	(Constant)	-3.751	2.834	-.010	-1.324	.227
	The contactless security model (palm vein) is more secure than the existing security technologies such as fingerprint authentications?	-.015	.434	-.341	-.035	.973
	I feel the security model will be more accurate	-.694	.750		-.926	.385
	The developed contactless security model will be the best suitable in enhancing data integrity	.482	.458	.333	1.054	.327
	I think the developed security model will reduce the False Rejection & False Acceptance Rate (FRR) & False Acceptance Rate (FAR)?	-.304	.482	-.180	-.630	.549
	The developed security model will be more efficient inservice delivery such as authentication?	.003	.545	.002	.005	.996

	The security system will counter cyberattacks	.509	.393	.445	1.294	.237
	The integration of Palm vein contactless technology and MIS will change the security dynamics	.493	.601	.273	.820	.439
	The model adequately addresses the tasks of developing contactless security systems	1.522	.708	.730	2.151	.069

Source: Field data (2021)

Table 38 above demonstrated the Regression Coefficient Results from experts for the model that will help enforce integrity by using palm vein biometric authentication system

4.3.4.4 Experts findings on components of the contactless security systems

Table 39 Expert findings on model components

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.995[a]	.989	.978	.15861

Source: Field data (2021)

From the table 39 above, it indicated an R^2 of 98.9 % indicating the data fitted the model well on the expert validation of the model using biometric systems for higher learning institutions.

Table 40 Anova for components expert validation

Model	Sum of Squares	df	Mean Square	F	Sig.

	Regression	15.929	7	2.276	90.458	.000[b]
1	Residual	.176	7	.025		
	Total	16.105	14			

Source: Field data (2021)

An F value of 90.458 was reached on the model validation with experts concerning the integrity by employing palm vein biometric authentication system, as shown in table 40 above. This was higher than the table value at (3.79) degree of freedom (7, 7) and showed that there was statistical significance.

Table 41 Expert validation coefficients on the components

Model		Unstandardized Coefficients		Standardizedt Coefficients		Sig.
		B	Std. Error	Beta		
1	(Constant)	.587	.572	.801	1.025	.339
	I think the database will be more efficient in storing the palm templates	.065	.007	.205	9.817	.000
	Feature methods are efficient in extracting the features from the users	.284	.128	.161	2.214	.062
	Sensor will be essential to capture images	.291	.127	.052	2.288	.056
	The decision algorithm will be suitable to validate and authenticate the users	.079	.088	.200	.898	.399
	The preprocessing will be suitable to remove noise and improve image's contrast	-.002	.224	-.001	-.009	.993
	Feature transformation will be essential	-.032	.111	-.020	-.143	.890
	The combination of all the selected components will change security dynamics in the university	.178		.106	1.605	.153

Source: Field data (2021)

According to table 41 above a correlation coefficient of 0.587 was obtained that demonstrated that the proposed database was suitable to store the palm templates. Based on component combination a coefficient of 0.178 was obtained that demonstrated that the selected components were effective.

4.3.5 Regression

Table 42 Combined Regression

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.164	15	.344	36.173	.000[b]
	Residual	.876	92	.010		
	Total	6.039	107			

Source: Field data (2021)

An f-statistics of 36.173 was achieved which is at (15,92) which is less than the f table value at 95% level of degree of freedom which was 40.563 indicating the good model fitting of the parameters of the study.

Table 43 Regression model summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.925[a]	.855	.831	.09755

Source: Field data (2021)

An R squared of 85.5% was achieved which indicated that the parameters used to develop the model of palm vein biometric technology were valid in order to enhance integrity in learning institutions in Kenya. This indicated positivity on the achievement of the model.

4.4 Discussions on individual objectives

4.4.1 Discussion on objective one

Its objective was to examine the security systems in place at higher education facilities. It was evident from the results of the respondents that fingerprint security systems, which accounted for 68.3 percent, are the most extensively utilized security systems. The University had been using the system for the last four years in authenticating students before they access the university premises, lecturer clock in and clock out as well as 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. In terms of technological applications, biometric systems are gaining popularity. Every biometric technique has a unique set of benefits and drawbacks. Finding a recommended practice for all applications is likewise impossible. Its own utilization aims may be different. According to (Bilal & Khaled, 2010), the iris- and fingerprint-based procedures are more precise than the voice-based technique. The biometric market has begun to increase as biometrics become more frequently employed in a range of applications.

The R^2 value for the relationship between the dependent and independent variables was $R^2 = 0.792$, according to the model summary in Table 9, suggesting an acceptable fit of the model because more than 50% of the test items included in the case study contributed to 79.2 percent. This demonstrated a strong correlation coefficient between the variables and a good security system the value of r is supposed to be close to positive 1. The null hypothesis that there was no statistical difference between the existing security systems was not rejected by ANOVA because the F-value at (12, 81) was 0.763, which was lower than the table value of 1.95. Since the variables matched the model well, there was statistical significance. Since 82.9 percent of respondents said that the institution was

utilizing a fingerprint biometric system, it was clear that the university had concentrated on just one type of biometric technology. Theft or publication of template information is the biggest threat to fingerprint biometric technology. A breach of the fingerprint biometric poses a lifetime risk to an individual's security and privacy because each person has a limited-edition, one-of-a-kind fingerprint that is consistent over the course of their lifetime (Onifade, 2020).

Since 66.7 percent of users concurred that the current fingerprint method had flaws that allowed for data manipulation and compromised the data's integrity, it was clear that the system had several vulnerabilities. It was evident that the Management information system was integrated well to support the various services provided such as students and staff registration. Concerning the cyber spoofing of biometric system by intruders 64.2% agreed that someone may use artificial silicon finger to access the system. In light of its failure to successfully authenticate users, 66.7 percent of respondents agreed that the present fingerprint authentication solutions have flaws. The university has a responsibility to guarantee the security of user data.

4.4.2 Discussions on objective two

To assess the IT security factors that influences the integrity of biometric systems in higher learning institutions.

The objective was analyzed by using a likert scale that consisted the constructs of the conceptual framework. They represented the independent variables and constituted of Academic policy and Security policy. Because people are the weakest link in any security chain, the universities public awareness score was 0.465, underlining the importance of understanding how cyber-attacks work and the different mitigation measures the institution should use. The findings of this study, however, demonstrated that security awareness training was beneficial. Security awareness and training improves people's

comprehension of the privacy strength of biometric security, which leads to biometrics' confidence. To put it another way, security awareness could help people comprehend how biometrics can secure personal information, so improving biometrics' reliability will boost their willingness to use them. Last but not least, it is crucial to keep educating users at all levels on security awareness because it is the first step in information security management (Chen et al., 2018). If the HEIs are unable to effectively handle the user's information, the organization's records of users may be mismatched and misidentified, leading in severe loss and financial impact. Furthermore, finding a solution to the problem of securely storing biometric data would be a big difficulty if biometrics are to become more widely used.

Given the results, it was concluded that the security model was efficient and successful in strengthening the integrity because the variables had a good correlation (r = 0.734), indicating that they were related. The R^2 of 73.4% indicated the data fitted the model well on the assessment the IT security metrics that influenced the integrity of biometric systems in higher learning institutions since it was greater than 50% therefore, other variables not assessed by the study only influenced examination malpractices within public and private universities by 26.6%.

An F value of 1.901 in table 13 was obtained in the ANOVA model summary which was less than the table value at (15,92) which was 0.032818 at 95% confidence interval this indicating that there was a statistical significance on the assessment of IT security metrics that influenced the integrity of biometric systems in higher learning institutions. The coefficient was 0.138 in terms of data security training that was satisfactory. This showed that, as far as the university was concerned, more than half of the respondents had received training on the procedures for ensuring confidentiality, integrity, and personal security. With regards to class signup for students and lecturers where class attendance

was done using the current finger print system and there was a correlation of 0.343. The researcher noted that individuals within the university were at risk of manipulation from confidence tricksters since most individuals agreed with a coefficient of -0.440. Although employees are frequently regarded as the weakest link in information security, many companies are aware that they could be useful allies in the fight against threats and cyber-attacks. Employees that obey the laws and regulations of information security are rewarded. The university should pay much attention to this since individuals are the weakest link to any security chain and it could be done through social engineering or spoofing attacks (Bulgurcu, 2010).

Hackers take advantage of employee vulnerabilities by using social engineering strategies (Symantec, 2011), using unsecure password habits (Vaas, 2016), and using personal devices at work (Symantec, 2011) and (Olavsrud,2014). As a result, it is critical for businesses to inform their staff about how they may contribute to the security of their organizations. Management must invest money on "making good security behaviors part of the business process, converting humans from risks into the first line of defense in the organization's security posture" in addition to infrastructure and technical protections (Olavsrud, 2015). Leaders must first comprehend the full range of human security risks and how they will impact their personnel before they can take this step.

It was evident that the university had not laid effective administrative controls to restore systems after a cyber-attack since there was a correlation of -0.23. Technical security precautions are necessary to protect exam confidentiality and integrity. All of the following are impacted: software, hardware, networks, data sources, computers, and physical space. There are two types of technical controls for online exam proctoring: static and dynamic. Data in storage devices should be secured using encryption and hash functions, as well as well-developed technical controls like digital certificates, digital

signatures, cryptographic software, secure protocols (like SSL), and others. Digital certificates, digital signatures, and cryptographic software should be employed over networks when the data is being transported to increase security (Slusky, 2020).

4.4.3 Discussions on objective three

To develop a logical security model using biometric systems for higher learning institutions:

Based on the experiment and according to table 27, 93.3% of the participants suggested that the palm vein (contactless) was better than the current fingerprint system 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. Based on table 29, 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. With regards to palm or finger wetness affecting the system 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.

An F value of 0.670 was obtained at (11,98) at 95% confidence interval which is less than the table value which is 0.763534 at 95% confidence interval hence we reject the null hypothesis that there was statistical significance in the design of a model using biometric systems for higher learning institutions. For the researcher to develop a better and more secure model a systematic literature review using 50 selected journals from Google scholar were obtained which had related literature about palm vein technology.20 of the selected journals were used to identify the best combination of components that would fit the new model. The components consisted of the database, sensors, feature extractions, decision making algorithms. According to the findings, CASIA (Chinese Academy of Science Institute of Automation) is the most often used database for security systems. Of the 20 journal publications that were taken into consideration, 53% used CASIA, 20% used PUT, and 27% used the Poly u

Multispectral Palm print database. 44 percent utilize the Gabor Filter, 31 percent LBP, and 25 percent use geometric techniques for feature extraction. CCD cameras (56%) and NIR cameras (44%) are the two types of cameras most commonly used for sensors. Principal Component Analysis (PCA) was used for decision-making that supports verifying and authenticating the user. To match the templates, hamming distance was employed. According to Table 27 it demonstrated how 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. From the

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

4.4.4 Discussions on objective four

The objective was to validate the implemented logical model by using experts.20 experts were randomly selected.16% of the experts provided response on the questionnaire which attributed to 80%. Based on the suitability of the security model 87.5% of the experts agreed that the security system met the threshold of a system that can enhance the integrity of the data while 12.5% suggested that it had not meet the required threshold. According to table 39, it indicated an R^2 of 98.9 % indicating the data fitted the model well on the expert validation of the model using biometric systems for higher learning institutions. A correlation coefficient of 0.587 was obtained that demonstrated that the proposed database was suitable to store the palm templates. Concerning the component validation an F value of 90.458 was obtained on the model validation with experts concerning the integrity by using palm vein biometric authentication system which was more than the table value at (3.79) degree of freedom (7,7) which demonstrated that there was statistical significance between the components in ensuring that the system was secure. Based on model fitness concerning the usage of the contactless model, the R^2 of 65.6 % indicated the data fitted the model well on the expert validation of the security model using biometric systems for higher learning institutions. Concerning the integrity of the new security model an F value of 0.714 was obtained on the integrity by using palm vein biometric authentication system this is less than the table value at (1.70) degree of freedom (10,59) which demonstrated that there was statistical significance.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The chapter featured a summary of the research results, conclusions reached based on the results, ideas for further research, and recommendations based on the results.

5.2 Summary of Findings

Concerns regarding information security and privacy have grown as the digital world has become more widespread, and biometric authentication technology has become commonly used authentication system. Despite the fact that palm vein authentication technology has been acknowledged as a viable alternative to the insecure fingerprint authentication technology, many customers are still hesitant to use fingerprint systems despite the fact that they are popular, affordable, and simple to use in businesses. As a result, the study was required to look at existing security systems as well as assess the IT security metrics that affected the integrity of biometric systems in higher education institutions. This study demonstrated that security awareness training was critical for increasing the desire to use fingerprint biometric systems while also increasing understanding of the security problem and the vulnerability of the current system. The study focused on a security model that can be used to enhance the integrity of data in Higher education institutions. The palm vein biometric technology was a contactless security model that captured individual palm prints without physical contact.

5.2.1 Summary of objectives one

From the results it was clear that the widely used security system was fingerprint system which attributed to 68.3%. The University had been using the system for the last four years in authenticating students before the access the university premises, lecturer clock in/out 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 If the HEIs are unable to effectively handle the user's information, the organization's records of users may be mismatched and misidentified, leading in severe loss and financial impact. Furthermore, finding a solution to the problem of securely storing biometric data would be a big difficulty if biometrics are to become more widely used

The R^2 value on the relationship between the analyzed dependent and independent variables was 0.792, according to the model description in Table 9, and this suggests a good fit of the model because it included more than 50% of the test items utilized in the case study. This revealed a high correlation coefficient between the variables, and a secure security system should have an R value that is close to positive one. We failed to reject the null hypothesis that there was a statistically significant relationship between the current security systems and higher education institutions, as shown by the ANOVA F-value at (12, 81), which was smaller than the table value of 1.95. As a result, the variables fit well for the model thus it was statistically significant.

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 a correlation that is above positive 0.7 which demonstrates a strong correlation coefficient. From my findings the correlation coefficient between the variables exceeded 0.675 since they were at 0.734 and

0.792 thus the researcher's model was better in-service delivery based on efficiency in regards to data integrity.

5.2.1 Summary of objectives two

The researcher noted that individuals within the university were at risk of manipulation from confidence tricksters since most individuals agreed with a coefficient of -0.440. Although employees are frequently regarded as the weakest link in information security, many companies are aware that they could be useful allies in the fight against threats and cyber-attacks. For enterprises, organizations, and government agencies, insider assaults may be the most serious cyber security threats. "Organizations claim that 42 percent of IT security vulnerabilities are caused by their employees' conduct," according to security firm Clear swift report (Clearswift, 2017). These insider threat incidents span a variety of cybercrimes, such as sabotage, espionage, and intellectual property theft, and they demonstrate how challenging it is to stop a bad actor from sharing information even when sophisticated security measures are in place (Park & Choi, 2017). Unintentional actors can also cause a massive security breach as a result of carelessness. This could cause just as much damage as intentional action. Careless activity could result in major implications for the organization, such as exposing confidential information into the public domain or on social media without recognizing it, responding to phishing attempts without realizing it, or downloading dangerous code from the Internet.

However, if the HEIs are unable to effectively handle the user's information, the organization's records of users may be mismatched and misidentified, leading in severe loss and financial impact. Furthermore, finding a solution to the problem of securely storing biometric data would be a big difficulty if biometrics are to become more widely used.

Given the results, it was concluded that the security model was efficient and successful in strengthening the integrity because the variables had a good correlation (r = 0.734), indicating that they were related. The R^2 of 73.4% indicated the data fitted the model well on the assessment the IT security metrics that influenced the integrity of biometric systems in higher learning institutions since it was greater than 50% therefore, other variables not assessed by the study only influenced examination malpractices within public and private universities by 26.6%. The 2011 hack of the American security firm RSA was a well-known example of this type of attack. A phishing email was sent to four employees, and one of them opened an attachment containing a zero-day exploit for a vulnerability. According to Zetter (2011), the burglars were able to obtain secret information about the company's Secure ID two-factor authentication solutions. Security awareness training does not only improve people's comprehension of the privacy strength of biometric security, but it also leads to biometrics' confidence. To put it another way, security awareness could help people comprehend how biometrics can secure personal information, thus improving biometrics' reliability will booster their willingness to use them. Last but not least, it is crucial to keep educating users at all levels on security awareness because it is the first step in information security management (Chen et al., 2018). If the HEIs are unable to effectively handle the user's information, the organization's records of users may be mismatched and misidentified, leading in severe loss and financial impact.

5.3.3 Summary of objective three

Based on the experiment and according to table 26, 93.3% of the participants suggested that the palm vein (contactless) was better than the current fingerprint system at 6.7%. Most of the participants selected the palm vein since it was not affected by wearing out of the hand palm or palm sensor scanner 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. Based on table 27, 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. 53.3% strongly agreed that wetness of the hand had an effect, 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. The fingerprint had an FRR of 60% while palm vein had an FRR of 93.33% based on the experiment outcomes. The accuracy rate of the fingerprint system is 60%, while the accuracy rate of the palm vein system is 93.33% thus palm vein was the better model to be implemented in the higher education institution. The average authentication time for palm vein was 9.15 seconds while Fingerprint was 2.67 seconds. Therefore, with respect to speed fingerprint was better as compared to the palm vein. The factors that necessitated low authentication speed in pal was the structure of the hand and the distance between the palm and the scanner. From the experiment it was concluded that it was essential for the university to implement the palm vein biometric technology due to its efficiency, integrity benefits, security aspects, robustness and performance. A logical model was implemented by adding security infrastructure which was represented by the feature extraction which helped to enhance the integrity of the biometric system.

5.2.4 Summary of objectives four

The goal was to use experts to validate the logical model that had been put into place.20 experts were chosen at random. 80% of the expert responses which made up 16% of the

total came from the questionnaire. Based on the adequacy of the security model, 87.5% of the experts concurred that the security system satisfied the requirement for a system that can improve the integrity of the data, while 12.5% thought it had not. Table 37 shows that the data fit the model well when it was validated by experts using biometric systems for higher education institutions, with an R2 of 98.9%. The proposed database was found to be appropriate for storing the palm templates thanks to a correlation coefficient of 0.587 that was calculated. Regarding the component validation, a model validation with experts using a palm vein biometric authentication system yielded a F value of 90.458, which was higher than the table value at (3.79) degree of freedom (7,7) and showed that there was statistical significance between the components in ensuring the security of the system. Based on model fitness for the use of the contactless model, the expert validation of the security model employing biometric systems for higher education institutions showed that the data fit the model well, as demonstrated by the R2 of 65.6%. By using a palm vein biometric authentication system, a F value of 0.714 was produced regarding the integrity of the new security model. This value is lower than the table value at (1.70) degree of freedom (10,59), which showed that there was statistical significance.

5.3 Conclusions

Finally, raising security awareness and understanding of security issues can aid consumers in avoiding data leakage and safeguarding their privacy. However, many businesses and educational institutions still lack adequate security awareness programs (Furnell & Vasileiou, 2017). As a result of this study, it is suggested that security awareness programs and training be implemented on a regular basis in both educational institutions and organizations that deal with data and information. The researcher was able to achieve all the objectives of the research. Security awareness is encouraged in terms of practical scenarios due to the following issues. To begin with, the use of digital

gadgets is getting more widespread, and security concerns are becoming more common. Security is a vital problem to consider, especially for firms that rely on all of their data and information to succeed. Companies are accountable for any damage done to their clients, including data loss and leakage, which could affect their trust in their services in the future.

Employees that pose a threat from within depict a wolf in sheep's clothing. Insider threats pose a serious risk to any firm, institution, and organization, as seen by daily, real-life examples. Theft of intellectual property, the destruction of facilities, or the disclosure of knowledge that can permanently affect the organization are just a few ways that a prospective hostile insider can cause millions of euros in damage. On the other hand, unintentional insiders can do irreversible damage. As a result, security awareness training should be performed with caution to avoid huge organizational loss and financial harm as a result of any security attack. According to the findings, the current security mechanisms were inconsistent in authenticating users and could not be trusted to improve the integrity of the system. It became clear after the COVID-19 breakout that the fingerprint mechanism was flawed as a result of direct contact with the device. The database, sensors, and feature extraction methods will be a helpful resource for enhancing palm vein recognition algorithms due to the paucity of databases and the confusing approach presented thus far in the literature. HEI, especially Mount Kenya University, could adopt palm vein recognition, a viable biometrics method that excels in terms of individuality, stability, and security. The fundamental idea of palm vein recognition was initially presented in our review. Tabulation was then used to track the advancement of the ROI approach and picture capture technologies. After considerable trial and error, a database was used to store the palm prints and fingerprints. Based on the results of our investigation, we evaluated palm vein imaging devices.

Theft or leakage of the template information is the most serious threat to the fingerprint biometric technology. Furthermore, each person 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). Therefore, due to these challenges the university should adopt the contactless security system since there is image transformation which enhances the security in a more efficient manner.

5.4 Recommendations

5.4.1 Awareness on Cyber attacks

From the findings it was evident that there was little awareness on how cyber-attacks attacks occurred and their mitigations. Employees are the weakest link in the security chain, so the university should have rules in place to train its staff. Due to the integration of biometrics with the internet there are various cyber-attacks that can occur. Through social engineering, an unforeseen insider threat could be recruited from the outside. It's critical to make all employees aware of the cyber risks and teach them how to avoid becoming a security flaw in the company's defenses.

5.4.2 User Authentication and verification

The university should consider replacing the current fingerprint security system since it was failing to authenticate legitimate users thus it was not consistent on data integrity since it had high FAR. Based on the results, 66.7% of the respondents agreed that the security measures in place today have flaws. The current system was inefficient because it took longer to validate users. The university should implement a contactless security system which is the palm vein technology which has a very low FAR.

5.4.3 Usage of fingerprint system in Covid-19 era

It was evident that the users were no longer using the fingerprint system and had resulted to card system which less secure than the fingerprint system. The university should adopt

a contactless security system that is free from physical contact which will be more useful in verifying users especially currently where there is outbreak of COVID 19 which has rendered the existing fingerprint security system un usable. The palm vein technology is currently being used in counties like USA in Carolina hospital to verify patients thus should be adopted in Higher education Institutions in Kenya especially Mount Kenya University.

5.4.4 Choice of security system

The university or any other institution should first analyze the components of the security system whether they are prone to attacks and the frequency of usage. From the findings on 50 journals analyzed by the researcher, the best and frequently used components of a contactless security system were identified. Based on the analysis, CASIA, which had 53%, is the most popular database. For decision-making, a CCD sensor camera was employed in 56 percent of cases, along with the Gabor feature extraction approach in 44 percent of cases and PCA. Therefore, Mount Kenya University should adopt the contactless security system in order to solve the current problems related to integrity and authentication. Liveness detection, watermarking, steganography and use of cancellable biometrics can be the ideal solution to overcome the various attacks on biometrics.

5.4.5 Documentation of policies and administrative controls

Policies, directives, and rules, among other administrative controls, must be well documented and implemented. It's critical to demonstrate that an organization's system, network, and information are being used responsibly. It is important to state what is expected of employees as well as the potential penalties of non-compliance. This is an effective deterrent.

5.5 Researcher's Contribution

The contribution of this thesis was implementing a contactless security model that was better than the existing models to support cyber security vulnerability based on the integrity of the data during verification and authentication. From the experiment the palm vein had an FRR of 93.33% while fingerprint had 60% which demonstrated superiority in authentication accuracy. A new logical model was produced by the addition of a feature extraction component. The retrieved features should be transformed into a better image component using the scale-invariant feature transform (SIFT). The current models' components included image processing, feature extraction, image storage, and picture capture. It is possible to improve the integrity of the recovered attributes by using Random Sample Consensus (RANSAC). inside a set number of computing iterations, the approach is used to count the number of outliers that fall inside the bounds of a predetermined threshold distance. Based on the integrated system theory the researcher extended the theory by adding security infrastructure component that was reflected in the conceptual framework. With the developed model it is essential for all security systems to have the image transformation feature which adds a layer in integrity enhancement in palm vein systems. It had a particular focus on contactless biometric systems especially in the era of COVID-19 where the fingerprint system was no longer usable to due physical contact.

The best combination of components was discovered after a thorough analysis of the literature utilizing 50 publications found on Google Scholar. From the analysis it was discovered that the best database was CASIA, Feature extraction algorithm was Gabor filters, CCD camera was the best while PCA algorithm was the best in decision making during authentication.

The researcher introduced new security levels such as double preprocessing and transformation that will provide better and secure image template. Based on the analysis

the researcher identified the suitable components that every institution should consider before implementing a security system. The researcher was able to contribute security knowledge to Higher education institutions that they should consider the components of a security system before the implementation which was guided by the integrated system theory.

5.6 Suggestions for further study Based on the findings on the research, the following areas are recommended for further

research.

a) Little research has been done on decision authentication algorithms since the commonly used was the PCA thus more research need to be carried out. Researchers should focus on identifying new algorithms that are more efficient in verifying users.

b) They are still loop holes especially based on spoofing attacks (Tome, 2015), thus more research is needed in that field.

c) More research needs to be carried out on palm vein template protection in deep learning since little research has been done in the field. The primary reason is that there isn't a sizable palm vein photo database, comparable to a face or fingerprint database. In order for palm image recognition technology to be used more frequently, a bigger database is needed.

REFERENCES

A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac.(2021). ‘‘A survey on security and privacy issues in modern healthcare systems: Attacks and defenses,’’ ACM Trans. Comput. Healthcare, vol. 2, no. 3, pp. 1–44, Jul. 2021

A. Khanna and S. Kaur. (2020). ‘‘Internet of Things (IoT), applications and challenges: A comprehensive review,’’ Wireless Pers. Commun., vol. 114, no. 2, pp. 1687–1762, Sep. 2020.

Aboalsamh, H. A. (2009). Vein and fingerprint biometrics authentication-future trends. *International journal of computers and communications*, *3*(4), 67-75.

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.

Al-Juaid, N. A., Gutub, A. A., & Khan, E. A. (2018). Enhancing PC data security via combining RSA cryptography and video-based steganography. *Journal of Information Security and Cybercrimes Research*, *1*(1), 5-13.

Almomani, I., El-Shafai, W., AlKhayer, A., Alsumayt, A., Aljameel, S., & Alissa, K. (2023). Proposed biometric security system based on deep learning and chaos algorithms. *Comput. Mater. Contin.*, *74*(2), 3515-3537.

Alpaydin, E. (2020). *Introduction to machine learning*. MIT press.

Baayen, R. H., Davidson, D. J., & Bates, D. M. (2008). Mixed-effects modeling with crossed random effects for subjects and items. *Journal of memory and language*, *59*(4), 390-412.

Babalola, F. O., Bitirim, Y., & Toygar, Ö. (2021). Palm vein recognition through fusion of texture-based and CNN-based methods. *Signal, Image and Video Processing*, *15*(3), 459-466.

Backe, A., & Lindén, H. (2015). Cloud computing security: a systematic literature review.

Beatty, R. C., Shim, J. P., & Jones, M. C. (2001). Factors influencing corporate web site adoption: a time-based assessment. *Information & management*, *38*(6), 337-354.

Bernal-Romero, J. C., Ramirez-Cortes, J. M., Rangel-Magdaleno, J., Peregrina-Barreto, H., & Cruz-Vega, I. (2023). A review on protection and cancelable techniques in biometric systems. *IEEE Access*.

Bilal, K., Muhammad, K. K., & Khaled, S. A. (2010). Biometrics and identity management for homeland security applications in Saudi Arabia. *African Journal of Business Management*, *4*(15), 3296-3306.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64-68.

Brotby, W. K. (2008). Information security metrics: *A definitive guide to effective security monitoring and measurement.* Boca Raton, FL: Auerbach.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Cai, H., Lin, J., Lin, Y., Liu, Z., Tang, H., Wang, H., & Han, S. (2022). Enable deep learning on mobile devices: Methods, systems, and applications. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, *27*(3), 1-50.

Cao, L., & Ramesh, B. (2007). Agile software development: Ad hoc practices or sound principles. *IT professional*, *9*(2), 41-47.

Chen, H. H., & Chen, S. C. (2009). The empirical study of automotive telematics acceptance in Taiwan: Comparing three technology acceptance models. *International Journal of Mobile Communications*, *7*(1), 50-65.

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312-324.

Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2019). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *1*(1), 32-41.

Dai, J., Feng, J., & Zhou, J. (2011). Robust and efficient ridge-based palmprint matching. *IEEE transactions on pattern analysis and machine intelligence*, *34*(8), 1618-1632.

Dalmarco, G., & Barros, A. C. (2018). Adoption of Industry 4.0 technologies in supply chains. In *Innovation and Supply Chain Management* (pp. 303-319). Springer, Cham.

Debrah, E., Effah, J., & Owusu-Mensah, I. (2019). Does the use of a biometric system guarantee an acceptable election's outcome? Evidence from Ghana's 2012 election. *African studies*, *78*(3), 347-369.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125128.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & security*, *25*(1), 55-63.

Drazin, R., & Van de Ven, A. H. (1985). Alternative forms of fit in contingency theory. *Administrative science quarterly*, 514-539.

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.

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

Effah, J., & Debrah, E. (2018). Biometric technology for voter identification: The experience in Ghana. *The Information Society*, *34*(2), 104-113.

Evrensel, A. (2010). Voter Registration in Africa a Comparative Analysis.

Fang, Y., Wu, Q., & Kang, W. (2018). A novel finger vein verification system based on two-stream convolutional network learning. *Neurocomputing*, *290*, 100-107.

Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, *11*(7), 4332-4340.

Furnell, Steven, and Ismini Vasileiou. "Security education and awareness: just let them burn?." *Network Security* 2017, no. 12 (2017): 5-9.

Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. *Center for Global Development Working Paper*, (315).

Giri, S. (2019). Cybercrime, cyber threat, cyber security strategies and cyber law in Nepal. *Pramana Research Journal*, *9*(3), 662-672.

Grijpink, J. (2005). Two barriers to realizing the benefits of biometrics–A chain perspective on biometrics, and identity fraud. *Computer Law & Security Review*, *21*(2), 138-145.

Guillen, E., Alfonso, L., Martinez, K., & Mejia, M. (2012). Vulnerabilities and performance analysis over fingerprint biometric authentication network. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 2, pp. 1-6).

Guleker, R., & Keci, J. (2014). The effect of attendance on academic performance. *Mediterranean Journal of Social Sciences*, *5*(23), 961.

Hao, Y., Sun, Z., Tan, T., & Ren, C. (2008, October). Multispectral palm image fusion for accurate contact-free palmprint recognition. In *2008 15th IEEE International Conference on Image Processing* (pp. 281-284). IEEE.

Hasheminasab, M., Ebadi, H., & Sedaghat, A. (2015). An integrated ransac and graphbased mismatch elimination approach for wide-baseline image matching. *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, *40*(1), 297.

Heracleous, L., & Wirtz, J. (2006). Biometrics: the next frontier in service excellence, productivity and security in the service sector. *Managing Service Quality: An International Journal*.

Hong, H. G., Lee, M. B., & Park, K. R. (2017). Convolutional neural network-based finger-vein recognition using NIR image sensors. *Sensors*, *17*(6), 1297.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*.

Hsueh, N. L., Kuo, J. Y., & Lin, C. C. (2009). Object-oriented design: A goal-driven and pattern-based approach. *Software & Systems Modeling*, *8*(1), 67-84.

Iwuoha, V. C. (2018). ICT and elections in Nigeria: Rural dynamics of biometric voting technology adoption. *Africa Spectrum*, *53*(3), 89-113.

Jack, B., & Clarke, A. M. (1998). The purpose and use of questionnaires in research. *Professional nurse (London, England)*, *14*(3), 176-179.

Jacobsen, K. L., & Sandvik, K. B. (2018). UNHCR and the pursuit of international protection: accountability through technology? *Third World Quarterly*, *39*(8), 1508-1524.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90-98.

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). *An introduction to statistical learning* (Vol. 112, p. 18). New York: springer.

Jansen, W. A. (2009). *Directions in security metrics research*. Diane Publishing.

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education.

Joshi, S. Mayur (2016). **Full Guide on Cyber Crimes in India**. Article published in "Cyber Fraud Resources*". Journal of Frauds, India Forensic Consultancy Services.*

Kamil, M. S. A., Mirza, S., Syed, A., & Bora, R. (2020). Palm Vein Technology.

Kark, K., Stamp, P., Penn, J., Bernhardt, S., & Dill, A. (2007). Defining an effective security metrics program. *Forrester Research*.

Katz, D. (1978). *Social psychology of organizations*.

Kaur, M., Kaur, N., & Singh, B. (2017). Comparative Study of Different Cryptoghraphic Algorithms. *International Journal of Advanced Research in Computer Science*, *8*(4).

Kavitha, S., & Sripriya, P. (2018). A review on palm vein biometrics. *Int. J. Eng. Technol*, *7*, 407.

Lee, J. C. (2012). A novel biometric system based on palm vein image. *Pattern Recognition Letters*, *33*(12), 1520-1528.

Lloyd, R., & Mertens, D. (2018). Expecting more out of expectancy theory: History urges inclusion of the social context. *International Management Review*, *14*(1), 28-43.

Lu, L., Fu, R., Yuan, L., Chen, W., & Liu, Y. (2019). Palm vein recognition based on end-to-end convolutional neural network. *Nan fang yi ke da xue xue bao= Journal of Southern Medical University*, *39*(2), 207-214

Lu, W., Li, M., & Zhang, L. (2016). Palm vein recognition using directional features derived from local binary patterns. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *9*(5), 87-98.

Luan, S., Min, Y., Li, G., Lin, C., Li, X., Wu, S., ... & Hill, J. C. (2014). Cross-cultural adaptation, reliability, and validity of the Chinese version of the STarT Back Screening Tool in patients with low back pain. *Spine*, *39*(16), E974-E979.

Luna, J., Ghani, H., Germanus, D., & Suri, N. (2011, July). A security metrics framework for the cloud. In *Proceedings of the international conference on security and cryptography* (pp. 245-250). IEEE.

MacAskill, E., Thielman, S., & Oltermann, P. (2017). WikiLeaks publishes 'biggest ever leak of secret CIA documents. *The Guardian*, *26*.

Maranga, M. J., & Nelson, M. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. *International Journal of Computer Science and Network*, *8*(4), 371-379.

Martin, Z. (2007). A new application for biometrics. *Health data management*, *15*(12), 46-48.

Mbogo, S. (2011). Health insurers tap bio-card to stem surging fraud cases. Business daily.

Meng, X., Xi, X., Yang, G., & Yin, Y. (2018). Finger vein recognition based on deformation information. *Science China Information Sciences*, *61*(5), 1-15.

Mishu, T. I., & Rahman, M. M. (2018). Vulnerabilities of fingerprint authentication systems and their securities. *Int. J. Comput. Sci. Inf. Secur*, *16*,

Mondal, S., & Bours, P. (2017). A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomputing*, *230*, 1-22.

Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. *Information & management*, *38*(4), 217-230.

Mugenda, O., & Mugenda, A. (2003). Research Methods, Qualitative and Quantitative Approach Acts. *Press Nairobi*.

Mulumba, M. A. (2012). *Biometric authentication systems and service delivery in healthcare sector in Kenya* (Doctoral dissertation).

N. Soliman, A. Algarni, W. El-Shafai, F. Abd El-Samie and G. El Banby, (2021). "An efficient GCD-based cancelable biometric algorithm for single and multiple biometrics,"CMC-Computers Materials & Continua, vol. 69, no. 2, pp. 1571–1595.

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.

Olavsrud, T. (2015). information security trends that will dominate.

Onifade, O. F., Olayemi, K. B., & Isinkaye, F. O. (2020). A Fingerprint template protection scheme using Arnold transform and bio-hashing. *Int J Image Graph Signal Process*, *12*, 28-36.

Park, R. K., Lim, J. I., Kwon, H. Y., & Choi, J. Y. (2017). A study on Korea's information security management system: an insider threat perspective. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 61-67). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and security for cloud computing* (pp. 3-42). Springer, London.

Peng, M., Wang, C., Chen, T., & Liu, G. (2016, May). A methodology for palm vein image enhancement and visualization. In *2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS)* (pp. 57-60). IEEE.

Pflug, A., Hartung, D., & Busch, C. (2012). Feature extraction from vein images using spatial information and chain codes. *Information security technical report*, *17*(1-2), 26-35.

Pironti, J. P. (2007). Developing metrics for effective information security governance. *Information Systems Control Journal*, *2*, 33.

Pooe, A., & Labuschagne, L. (2011). Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation. *Southern African Business Review*, *15*(1).

Ranjith Kumar, M., Deepika, G., & Meenakshi Krishnan, K. B. (2017). An OpenSource Contact-Free Palm Vein Recognition System.

Raut, S. D., & Humbe, V. T. (2015, December). Palm vein recognition system based on corner point detection. In *2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 499-502). IEEE.

Ringheim, K. (1995). Ethical issues in social science research with special reference to sexual behaviour research. *Social Science & Medicine*, *40*(12), 1691-1697.

Robbins, S. P., & Judge, T. (2009). *Organizational behavior*. Pearson South Africa.

Roberts, C. (2007). Biometric attack vectors and defences. *computers & security*, *26*(1), 14-25.

Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, *39*(4), 774-784.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Sater, M. H. A., Kanaan, H., & Ayache, M. (2019, October). Identification of individuals using palm vein classification. In *2019 Fifth International Conference on Advances in Biomedical Engineering (ICABME)* (pp. 1-4). IEEE.

Saunders, M., Lewis, P. H. I. L. I. P., & Thornhill, A. D. R. I. A. N. (2016). Research methods. *Business Students 4th edition Pearson Education Limited, England*.

Schuckers, S. A. (2002). Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4), 56-62.

Selvarani, P., & Natarajan, S. (2013). Face Recognition Using a Coarse-to-Fine Level Set Scheme. *Research Journal of Applied Sciences, Engineering and Technology*, *5*(3), 760-766.

Serianu, (2020). Cybersecurity Report 2020.

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.

Sherwood, J. (1996). SALSA: A method for developing the enterprise security architecture and strategy. *Computers & Security*, *15*(6), 501-506.

Slusky, L. (2020). Cybersecurity of online proctoring systems. *Journal of International Technology and Information Management*, *29*(1), 56-83.

Soh, S. C., Ibrahim, M. Z., & Yakno, M. (2018). A review: Personal identification based on palm vein infrared pattern. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1-4), 175-180.

Stone, J. (2020). Ransomware strikes biotech firm researching possible COVID-19 treatments.

Sullivan, G. M. (2011). A primer on the validity of assessment instruments. *Journal of graduate medical education*, *3*(2), 119-120.

Swanson, M. M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. (2003). Security metrics guide for information technology systems.

Symantec, W. (2011). Advanced persistent threats: A Symantec perspective. *Symantec World Headquarters*.

T. Putte and J. Keuning. (2000). “Biometrical fingerprint recognition: don’t get your fingers burned”, Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App., pp. 289-303.

Thakral, P., Rai, M., & Thakral, R. (2012). Issues of biometric for disabled. *International Journal of applied Engineering research*, *7*(11).

Thakur, K., & Vyas, P. (2019). Social Impact of Biometric Technology: Myth and Implications of Biometrics: Issues and Challenges. *Advances in Biometrics*, 129155.

Thorsen, L. T. (2016). *Multi-factor Authentication using Secure Elements: Enhancing the Usability with new Web APIs* (Master's thesis).

Tome, P., & Marcel, S. (2015, May). On the vulnerability of palm vein recognition to spoofing attacks. In *2015 International Conference on Biometrics (ICB)* (pp. 319-325). IEEE.s

Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, SatoshiN Hoshino. (2002). "Impact of artificial 'gummy' fingers on fingerprint systems." Proc. SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, April 2002.

Vijayalakshmi, P. S. (2015). Palm vein recognition using ındependent component analysis and gabor texture patterns IJARCET.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104.

von Solms, R., Van Der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, *26*(3), 143-153.

Watanabe, M. (2008). Palm vein authentication. In *Advances in biometrics* (pp. 75-88). Springer, London.

Xie, C., & Kumar, A. (2017). Finger vein identification using convolutional neural network and supervised discrete hashing. In *Deep Learning for Biometrics* (pp. 109-132). Springer, Cham.

Yan, X., Kang, W., Deng, F., & Wu, Q. (2015). Palm vein recognition based on multisampling and feature-level fusion. *Neurocomputing*, *151*, 798-807.

Yang, W., Hu, J., Fernandes, C., Sivaraman, V., & Wu, Q. (2016, December). Vulnerability analysis of iPhone 6. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 457-463). IEEE.

Yang, W., Hui, C., Chen, Z., Xue, J. H., & Liao, Q. (2019). FV-GAN: Finger vein representation using generative adversarial networks. *IEEE Transactions on Information Forensics and Security*, *14*(9), 2512-2524.

Zang, W. L. (2014). Research of information security quantitative evaluation method. In *Applied Mechanics and Materials* (Vol. 513, pp. 369-372). Trans Tech Publications Ltd.

Zetter, K., Matsakis, L., Lapowsky, I., Graff, G., Dreyfuss, E., & Newman, L. (2011). Researchers uncover RSA phishing attack, hiding in plain sight. *WIRED Magazine*.

APPENDICES

Appendix I: Staff Research Questionnaire

I humbly take this opportunity to pass my appreciation for taking your time to complete this questionnaire. The objective of this questionnaire is to assist research being carried

out on" **A model of palm vein biometric technology to enhance integrity in learning institutions in Kenya** a case Study of Mount Kenya University Thika**.**". I assure you that the information will be kept confidential kindly answer the questions as truthfully as possible.

Thank you.

SECTION A: Demographic Information Kindly

check in the boxes provided.

1. What is your gender? Male ☐ Female ☐

2. What is your Marital Status?

a) Single ( )

b) Married ( )

c) Divorced ( )

d) Widowed ( )

3. What is your age?

18-25 ( ) 26-30 ( ) 31-35 ( ) 36-40 ( ) 41-45 ( ) Above 45 ( )

4. Which department do you work in?

a) Finance ( )

b) ICT ( )

c) Human Resource ( )

d) Business ( )

e) Security ( )

f) Accommodation ()

g) Examinations ()

h) Administration ( )

i) Other Specify……..

5. Which is the highest Level of Education you have attained?

a) Certificate/Diploma ( )

b) Bachelor's Degree ( )

c) Master's Degree ( )

d) Phd ( )

e) Other ( )

6. How long have you worked in this University?

1 month -4 years ( ) 5-8 years ( ) 9-12 years ( ) above 12 years ( )

7. What is your career?

a) System Administrator ( )

b) Database Administrator ( )

c) Lecturer ( )

d) Administrative Assistant ( )

e) Customer Care Representative ( )

f) Security Officer ( )

g) Any other Specify…… **SECTION B: BIOMETRIC SYSTEM USAGE**

1. Which biometric technologies have you used before?

Fingerprint ( ) Voice Recognition ( ) Iris Recognition ( ) Face Recognition ( )

Palm Vein Recognition ( ) None ( )

2. How regularly do you use biometric Technology?

Often ( ) Always ( ) Seldom ( ) Never ( )

3. Which biometric Technologies has your University Invested before? Mark all applicable.

Fingerprint ( ) Voice Recognition ( ) Iris Recognition ( ) Face Recognition ( )

Palm Vein Recognition ( ) None ( )

4. How long has your organization invested on the use of biometric technology?

1 month -3 years ( ) 4-7 years ( ) 8-12 years ( ) above 12 years ( )

5. Which biometric technologies is your organization still investing on? Mark all applicable.

Fingerprint ( ) Voice Recognition ( ) Iris Recognition ( ) Face Recognition ( )

Palm Vein Recognition ( ) None ( )

6. Do you think the current biometric system can be hacked?

Yes ( ) No ( )

7. Have you heard of cyber-attacks?

Yes ( ) No ( )

8. Do the current biometric system have weakness?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

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

Yes ( ) No ( )

If yes, elaborate

……

……

……

10. Which channels (areas) use biometrics in your university? Specify three……

……

……

11. Is there a scenario when the current biometric system had failed to authenticate you? Does the current biometric system have weakness?

Yes ( ) No ( )

If yes, elaborate

……

……

……

12. Do you think the current biometric system has been integrated well with Management information system (MIS) to support all the services?

Yes ( ) No ( )

If yes, elaborate

……

……

13 Do you think we can have biometric cyber spoofing a form of hacking where someone may use fingerprint information copied in an artificial silicon finger in order to access the system?

Yes ( ) No ( )

If yes, elaborate

……

……

14. List at least three recommendations that can be used to improve biometric system.

a) ……

b) ……

c) ……

d) ……

…

SECTION C: ITS SECURITY POLICY AND ACADEMIC POLICY

Please read the statement carefully and tick appropriately.

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

	Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
IT security policy is a priority within your organization.					
Cyber security risks assessments performed periodically					
The university has implemented various administrative controls to ensure data integrity.					
There is public awareness in cyber security within the University					
The university management has the responsibility to ensure the organization administrative controls are enforced.					
There is investment in cyber security research & development programs					
There is adequate training on ensuring data security.					
The university has implemented effective security mechanisms in class during signing up.					
The university has a disaster recovery plan to restore systems after security attack.					

The university support the development of professional training courses in cyber security					
I feel that the university has implemented physical security measures.					
The university has a log file to conduct audit trails.					
There are preventive strategies laid upon to prevent attacks.					
Individuals within the company are at risk of manipulation from confidence tricksters.					
I feel that Information systems provide all the protection a university requires.					

SECTION D: IT'S SECURITY INFRASTRUCTURE

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

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I feel the University is ready to counter cyber attacks					
I feel that the organization do not have adequate firewalls to counter attacks.					
I think that management have the responsibility to ensure the organization has implemented encryption techniques.					
The university has a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure.					
There are adequate backup methods to restore data in case of attacks.					
I feel that the university is using cloud servers or databases for backups.					
The university has updated the software's to ensure there are no loop holes.					
The biometrics being used in the university is failing to verify users.					
I feel that malicious attacks can be detected by intrusion detection systems installed by the university.					
I feel that the biometric system & MIS have been integrated well.					
Computer systems provide all the protection a company needs.					

SECTION E: INTEGRITY

1. Do you feel that the university has utilized the levels of security products?

   Yes ( ) No ( )

   If yes, elaborate

   ……

   ……

   ……

   ……

2. Are logins passwords deactivated immediately once an employee leaves the university?

   Yes ( ) No ( )

   If yes, elaborate

   ……

   ……

   ……

   Do you believe that the university sensitive data is protected by using strong passwords or other types of access controls?

   Yes ( ) No ( )

   If yes, elaborate

   ……

   ……

   ……

3. Does the university maintain written policies or procedures related to the security controls over access to the system?

   Yes ( ) No ( )

If yes, Elaborate

……

……

……I

s the system security administrator designated to control password and biometric system security?

Yes ( ) No ( )

If yes, Elaborate

……

……

……I

f student and staff data is maintained on the servers, is security over the data sufficient to ensure compliance with the university data security policy?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

4. Is the current biometric system consistent in validating and authenticating the users?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

Does the current biometric system have loop holes that could allow unauthorized personnel modify existing data?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

Does the current biometric system have the security features to detect fake login credentials of unauthorized modified data?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

5. Does you think the integration of biometric system and MIS will change the security dynamics?

Yes ( ) No ( )

If yes, Elaborate

……

……

……

……

Appendix II: Expert Research Questionnaire

I humbly take this opportunity to pass my appreciation for taking your time to complete this questionnaire. **The purpose of the questionnaire is to validate the palm vein model that will be more efficient and secure in enhancing the integrity of the data.**

It will assist on research being carried out on" **A model of palm vein biometric technology to enhance access integrity in learning institutions in Kenya.** "I assure you that the information will be kept confidential kindly answer the questions as truthfully as possible.

Thank you.

SECTION A: General Information Kindly

check in the boxes provided.

1. What is your gender? Male ☐ Female ☐

2. Which is the highest Level of Education you have attained?

f) Bachelor's Degree ( )

g) Master's Degree ( )

h) Phd ( )

i) Other ( )

5. What is your field of specialization?

h) System Analyst ( )

i) Security Specialist ( )

j) Lecturer ( )

k) Administrator ( )

l) Any other Specify……

4. Please state your years of experience?

0 -2 years ( ) 3-5 years ( ) 6-8 years ( ) above 8 years ( )

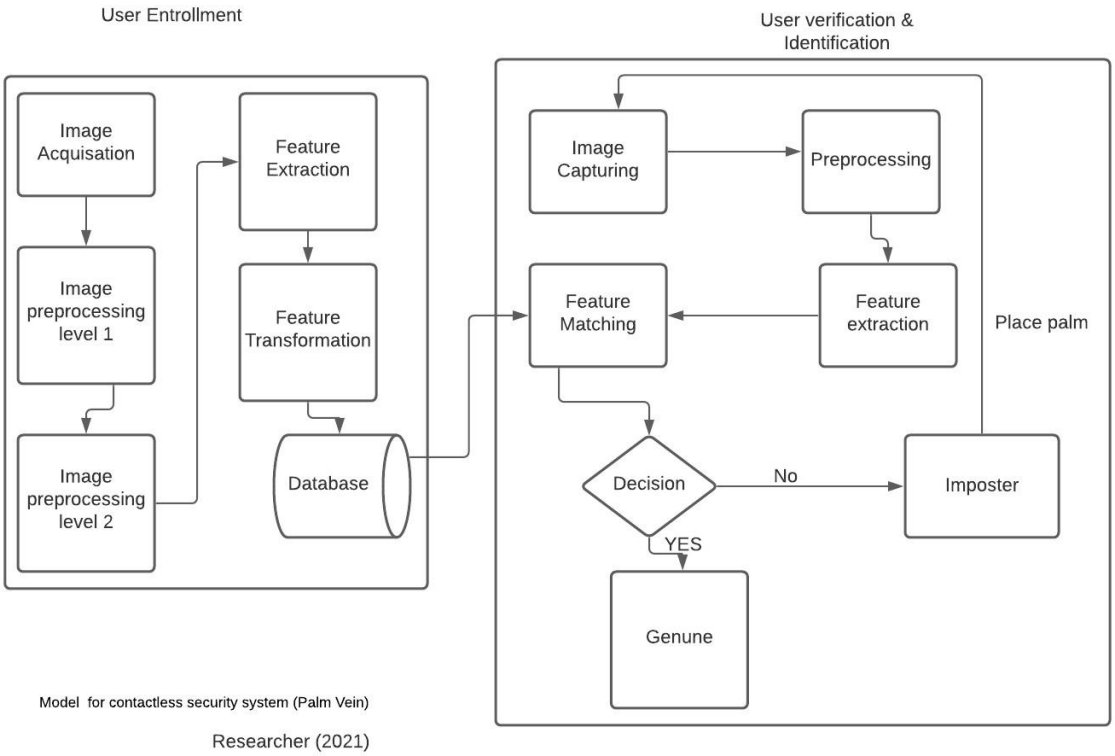
5. Do you know any secure control model that guides companies to design and maintain secure processes, systems and applications?

Yes ( ) 3-5 No ( )

SECTION B: RELEVANCE AND COMPLETENESS OF CONTACTLESS SECURITY MODEL

6. The following model constructs represents important aspects which must be precisely be determined in the development of secure contactless models. Please state your agreement with this statement by selecting appropriately.

The following image demonstrates the developed model



Model for contactless security system (Palm Vein)

Researcher (2021)

SECTION B: MODEL SECURITY DYNAMICS

Please read the statement carefully and tick appropriately.

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

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The contactless security model (palm vein) is more secure than the existing security technologies such as fingerprint authentications?					
The security model will be more accurate					
The developed model will be the best suitable in enhancing data integrity					
The developed security model will reduce the False Rejection Rate (FRR) & False Acceptance Rate (FAR)?					
The developed security model will be more efficient in-service delivery such as authentication?					
The security system will counter cyber-attacks					
The integration of Palm vein contactless technology and MIS will change the security dynamics					
The model adequately addresses the tasks of developing contactless security systems					

7. SECTION C: COMPONENTS OF THE SECURITY MODEL

Please read the statement carefully and tick appropriately.

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

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The database will be more efficient in storing the palm templates					
Feature methods are efficient in extracting the features from the users					

Sensor will be essential to capture images					
The decision algorithm will be suitable to validate and authenticate the users					
The preprocessing will be suitable to remove noise and improve image's contrast					
Feature transformation will be essential					
The combination of all the selected components will change security dynamics in the university					

8. In your opinion, do you think the model has covered all the needs of developing a contactless security system?

Yes ( ) 3-5 No ( )

Appendix III: User Experiment Questionnaire

I humbly take this opportunity to pass my appreciation for taking your time to complete this questionnaire. **The purpose of the questionnaire is to validate the contactless security model that will be more efficient and secure in enhancing the integrity of the data.**

It will assist on research being carried out on" **A model of palm vein biometric technology to enhance access integrity in learning institutions in Kenya.** "I assure you that the information will be kept confidential kindly answer the questions as truthfully as possible.

Thank you.

SECTION A: General Information Kindly

check in the boxes provided.

1. What is your gender? Male ☐ Female ☐

2. Which is the highest Level of Education you have attained?

a) Phd ( )

b) Master's Degree ( )

c) Bachelor's Degree ( )

d) Diploma ( )

e) Certificate ( )

f) Other ( )

3. How long have you been in the university?

Less than 1 year ( ) 1-2 years ( ) 3-5 years ( ) above 5 years ( )

SECTION B: EXPERIMENT DYNAMICS

4. Which biometric technologies have you used before?

Fingerprint ( ) Voice Recognition ( ) Iris Recognition ( ) Face Recognition ( )

Palm Vein Recognition ( ) None ( )

5. From the experiment, which technology was better?

Fingerprint ( ) Palm vein (Contactless) ( )

6. Please read the statement carefully and tick appropriately.

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

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The contactless security system (palm vein) is more secure than the fingerprint system					
The contactless system was more efficient(fast) in user registration					
The palm vein(contactless) was more accurate in authentication					
The palm vein(contactless) was consistent in validation					
The palm vein(contactless) was not affected by the wearing out of hand palm during registration and verification					
Wearing out of fingerprint ridges affected the speed in which a user was registered					
The contactless (palm vein) prevented unauthorized access					
The fingerprint system should be replaced with contactless security system(Palm vein)					

Wetness of the finger affected the registration and authentication					
The palm vein was not affected by wetness or sweating of the palm					

Appendix IV: Experiment Observation Checklist

Parameters	**Tick Appropriately**
The user had wet hands	Yes ☐ No ☐
The Fingerprint scanner rejected the first thumb finger	Yes No ☐
The palm vein scanner registered a user with dirty palm	Yes ☐ No ☐
The participant had dirty fingers	Yes ☐ No ☐
The participant finger ridges were worn out	Yes ☐ No ☐
The fingerprint scanner verified the user with a single attempt	Yes ☐ No ☐
The palm vein scanner verified the user with a single attempt	Yes ☐ No ☐
Fingerprint scanner took time to register a user	Yes ☐ No ☐
Palm scanner took time to register a user	Yes ☐ No ☐
Worn out fingerprints affected authentication	Yes ☐ No ☐
	Yes ☐ No ☐

Palm vein scanner rejected unregistered or incorrect palm during authentication	

Appendix V: MKU ERC Approval Certificate

Mount Kenya University

REF: **MKU/ERC/1757** Date: 02 February 2021
TO: **BONIFACE MWANGI WAMBUI**

REG: **MSCCS/2019/39971**

Dear Sir/Madam,

RE: A MODEL OF PALM VEIN BIOMETRIC TECHNOLOGY TO ENHANCE INTEGRITY IN LEARNING INSTITUTIONS IN KENYA. A CASE STUDY OF MOUNT KENYA UNIVERSITY

This is to inform you that **Mount Kenya University** has reviewed and approved your above research proposal. Your application approval number is **830.** The approval period is **02/02/2021 - 01/02/2022.**

This approval is subject to compliance with the following requirements;

i. Only approved documents including informed consents, study instruments, MTA will be used
ii. All changes including amendments, deviations and violations are submitted for review and approval by **Mount Kenya University**
iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to **Mount Kenya University** within 72 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affect the safety or welfare of study participants and others or affect the integrity of the research must be reported to **Mount Kenya University** within 72 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal
vii. Submission of an executive summary report within 90 days upon completion of the study to **Mount Kenya University**

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology and Innovation (NACOSTI) https://oris.nacosti.go.ke and also obtain other clearances needed.

Yours sincerely,

The Chairman
Mount Kenya University
Ethics Review Committee
P. O. Box 342 - 0100, Thika

Dr. Peter G. Kirira
Chairman, Mount Kenya University IERC

Main Campus, General Kago Road, P.O. Box 342-01000 Thika. Tel: +254 67 2820 000,
Cell: +254 720 790 796, 0709 153 000
Email:info@mku.ac.ke, Web: www.mku.ac.ke
Chartered and ISO 9001 : 2015 Certified Institution.
Unlocking Infinite Possibilities

Appendix VI: Introduction Letter from Postgraduate

Mount Kenya University

DIRECTORATE OF GRADUATE STUDIES

MSCCS/2019/39971

7th April, 2021

The Director, Research Coordination Division
National Commission for Science, Technology & Innovation
Utalii House, 8th & 9th Floor
P.O Box 30623- 00100
NAIROBI

Dear Sir/Madam,

RE: BONIFACE MWANGI WAMBUI – REGISTRATION NO. MSCCS/2019/39971

The purpose of this letter is to introduce the above named student who is pursuing **Master of Science in Cyber Security** in the Department of **Information Technology** in the School of **Computing & Informatics.**

The title of his research is *"A Model of Palm Vein Biometric Technology to Enhance Intergrity in Learning Institutions in Kenya. A Case Study of Mount Kenya University."*

He has been cleared by the University's Ethics Review Committee (Certificate attached) and now has to proceed to the field to collect data for his research between **April and June, 2021.**

Any assistance accorded to him will be highly appreciated.

Thank you.

Mount Kenya University
P.O. Box 342-01000, THIKA
Office of the Director
Graduate Studies

Dr. Samuel M. Kariuki, Ph.D
Director, Graduate Studies
Enc.

Main Campus, General Kago Road, P.O. Box 342-01000 Thika. Tel: +254 67 2820 000.
Cell: +254 720 760 796, 0709 153 000
Email: info@mku.ac.ke. Web: www.mku.ac.ke
Chartered and ISO 9001 : 2015 Certified Institution
Unlocking Infinite Possibilities

Appendix VII: Nacosti Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 604679

Date of Issue: 15/April/2021

RESEARCH LICENSE

This is to Certify that Mr.. Boniface Mwangi Wambui of Mount Kenya University, has been licensed to conduct research in Kiambu on the topic: A MODEL OF PALM VEIN BIOMETRIC TECHNOLOGY TO ENHANCE INTEGRITY IN LEARNING INSTITUTIONS IN KENYA. A CASE STUDY OF MOUNT KENYA UNIVERSITY for the period ending : 15/April/2022.

License No: NACOSTI/P/21/10081

604679

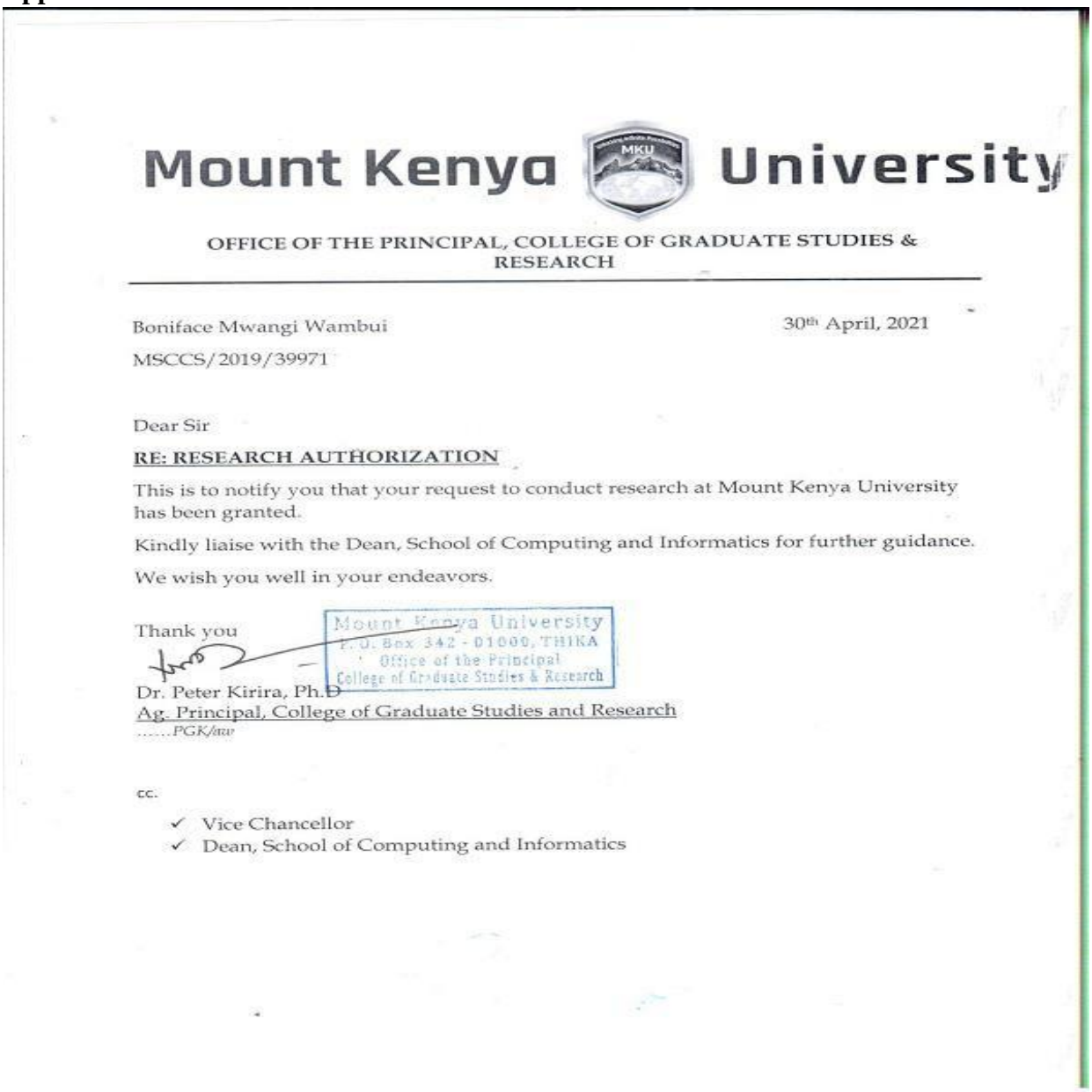
Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

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

Appendix VIII: Research Authorization Letter



Mount Kenya University

OFFICE OF THE PRINCIPAL, COLLEGE OF GRADUATE STUDIES & RESEARCH

Boniface Mwangi Wambui

MSCCS/2019/39971

30th April, 2021

Dear Sir

RE: RESEARCH AUTHORIZATION

This is to notify you that your request to conduct research at Mount Kenya University has been granted.

Kindly liaise with the Dean, School of Computing and Informatics for further guidance.

We wish you well in your endeavors.

Thank you

Mount Kenya University
P.O. Box 342 - 01000, THIKA
Office of the Principal
College of Graduate Studies & Research

Dr. Peter Kirira, Ph.D
Ag. Principal, College of Graduate Studies and Research
.....PGK/mw

cc.

- ✓ Vice Chancellor
- ✓ Dean, School of Computing and Informatics

Appendix IX: Informed Consent Form

Dear Respondents,

I humbly invite you to participate in a research study entitled "**A model of palm vein biometric technology to enhance access integrity of biometric systems in learning institutions in Kenya".**

I am currently a student undertaking Master of Science in Information Cyber Security at Mount Kenya University. This information will be of great purpose to the study since it will assist to analyze a model of palm vein technology to enhance integrity of biometric systems in learning institutions in Kenya. The study will be going to be helpful to neutral within the learning institution where the matter of identity theft has been prevailing. The proposed technology will seal prevailing loops holes that have been used by hackers or unauthorized users in compromising the security on organization. The outcomes from this study will be of beneficial to decision makers in Kenyan learning establishments in enhancing the integrity of information systems. Given the above, I am humbly requesting you to cooperate in answering the questionnaire responding to the questions which I will provide in the questionnaires attached here-with. Kindly read the accompanying instructions and respond to the questions as provided for. Your participation in this research project is completely voluntary. You may decline altogether, or leave blank any questions you don't wish to answer. There are no known risks to participation beyond those encountered in everyday life. Your responses will remain confidential and anonymous. Data from this research will be kept under lock and key and reported only as a collective combined total. No one other than the researchers will know your individual answers to this questionnaire. There are no direct benefits to you for participating in this research.

However, you may find it interesting to talk about the issues addressed in the research and it may be beneficial to the field and to future clients or individuals who have experienced similar concerns. Please return the questionnaire as soon as possible to enable me complete the project report.

If you have any questions about this project, feel free to contact the INVESTIGATOR:

BONIFACE MWANGI WAMBUI: Tel 0716540697 or my supervisors Dr. Joyce Gikandi: Tel 0707252342 or Dr.Mariga Tel: 0722440677. If you have questions about your rights as a research participant, please be in touch with the Chairman, Mount Kenya University, Ethical Review Committee, P.O Box 342-01000, and Thika

Thank you very much for your assistance in this important exercise.

Participant's statement

I have read and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I voluntarily agree to take part in this study

Participant signature ---------- Date…….

Investigator's signature ---------- Date…….

Appendix X: Similarity Index

A PALM VEIN AUTHENTICATION IMPLEMENTATION MODEL FOR ENHANCED ACCESS OF BIOMETRIC SYSTEMS: A CASE OF MOUNT KENYA UNIVERSITY MAIN CAMPUS

ORIGINALITY REPORT

14%	12%	5%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	erepository.mku.ac.ke Internet Source	1%
2	ijcit.com Internet Source	1%
3	umispace.umi.ac.ug Internet Source	1%
4	erepository.uonbi.ac.ke Internet Source	1%
5	docplayer.net Internet Source	<1%
6	doczz.net Internet Source	<1%
7	www.researchgate.net Internet Source	<1%
8	Juan Carlos Bernal-Romero, Juan Manuel Ramirez-Cortes, Jose De Jesus Rangel-Magdaleno, Pilar Gomez-Gil et al. "A Review	<1%

Dr. G. Maina
20/6/2023

Dr. Gwendi Gw
20/06/2023