HB100/G/8062/19

NGUNZA RICHARD WAMBUA

BACHELOR OF SCIENCE IN FORENSIC SCIENCE

A RESEARCH PROPOSAL ON THE RISKS OF USING FINGERPRINT

RECOGNITION SYSTEM DURING THE COVOD-19 PERIOD AT KIRINYAGA UNIVERSITY.

A RESEARCH PROPOSAL SUBMITTED TO THE DEPARTMENT OF FORENSIC

SCIENCE IN SCHOOL OF HEALTH SCIENCE IN THE PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF

SCIENCE IN FORENSIC SCIENCE IN KIRINYAGA UNIVERSITY.

# DECLARATION

I declare that this project is my original work and has not been presented in any other university for consideration of any certification.

Signature……………………………………………. Date………………………………………

NGUNZA RICHARD WAMBUA.

This research project was submitted for examination with my approval as the university supervisor.

Signature……………………………………………Date……………………………………….

DR. WANJIKU NJOROGE.

School of Health Science.

Kirinyaga University.

# DEDICATION

I dedicate this work to my family, especially my parents, for their everlasting love and support during my studies. I’d also like to thank my friends, course-mates, and all my lecturers, including my supervisor Dr. Wanjiku Njoroge for their aid in completing this project successfully. Many thanks to everyone.

# ACKNOWLEDGEMENT.

I wish to thank the Almighty God for putting in me the desire to further my studies to this level and for enabling me accomplish the studies successfully.

I would also like to thank my lecturers for their guidance and commitment to this effort. Their guidance has been quite beneficial to me in ensuring that I complete the assignment on schedule and to the needed standards. Second, I want to express my gratitude to the kirinyaga university for providing the opportunity and resources required for this study. Finally, I congratulate myself on my effort to ensuring the project’s success.

# ABSTRACT

Biometric recognition is a technique that identifies based on their unique physical or behavioral traits. It is gaining popularity due to security worries about identity theft and cyber crime. Biometric solutions are utilized for forensics, access control, financial fraud detection, and border security. Biometric identification technologies, such as fingerprint, iris scans, facial recognition, and voice recognition, are becoming increasingly used in a variety of industries, including government, healthcare, and finance. However, during COVID-19 pandemic, the usage of fingerprint identification system put the organization and its staff at risk of infection owing to physical contact between users and machines.

For instance in Kirinyaga University the use of fingerprint scanning was a great risk for students due to different factors such as population of the students. The adoption of new technologies during the corona pandemic to curb the spread of the virus also put the users at risk of infection.

This proposal explores the dangers of utilizing fingerprint recognition systems during the pandemic, highlighting concerns related to the potential transmission of the virus through surface contact. Additionally, it discusses the implications for Kirinyaga university students, staffs and the community at large, and offers recommendations for alternative access control measures to mitigate the risks associated with fingerprint recognition systems during that public health crisis.

# 

# Table of Contents

[DECLARATION 1](#_Toc163378183)

[DEDICATION 2](#_Toc163378184)

[ACKNOWLEDGEMENT. 3](#_Toc163378185)

[ABSTRACT 4](#_Toc163378186)

[Table of Contents 5](#_Toc163378187)

[TABLE OF FIGURES 9](#_Toc163378188)

[ACRONYMS AND ABBREVIATION 10](#_Toc163378189)

[OPERATIONAL DEFINITION OF TERMS 11](#_Toc163378190)

[CHAPTER ONE: INTRODUCTION 12](#_Toc163378191)

[Background 12](#_Toc163378192)

[Problem Statement 14](#_Toc163378193)

[Objectives 14](#_Toc163378194)

[General Objective 14](#_Toc163378195)

[Specific Objectives 14](#_Toc163378196)

[Research Questions. 15](#_Toc163378197)

[Scope of the Study 16](#_Toc163378198)

[CHAPTER TWO: LITERATURE REVIEW 17](#_Toc163378199)

[Theoretical Frame 17](#_Toc163378200)

[Biometric System. 17](#_Toc163378201)

[Requirements for biometric identification system. 18](#_Toc163378202)

[Conceptual Framework 22](#_Toc163378203)

[Research Gaps 25](#_Toc163378206)

[CHAPTER THREE: RESEARCH METHODOLOGY 25](#_Toc163378207)

[Introduction 25](#_Toc163378208)

[Research Designs 26](#_Toc163378209)

[Target Population 26](#_Toc163378210)

[Sample and Sampling Techniques 27](#_Toc163378211)

[Data Collection Procedure 27](#_Toc163378212)

[Secondary Data (existing information): 28](#_Toc163378220)

[Pilot Study 28](#_Toc163378223)

[Validity Test 28](#_Toc163378224)

[Reliability Tests 29](#_Toc163378225)

[Data Analysis Procedure 29](#_Toc163378226)

[CHAPTER FOUR: FINDINGS AND RESULTS 30](#_Toc163378227)

[Table 3:Year of study Frequence % of respondents 30](#_Toc163378231)

[Table 4:Gender Frequency % of respondents 30](#_Toc163378232)

[Table 5:Factor Frequency % of respondents 31](#_Toc163378233)

[Table 6:Factor Frequency % of respondents 31](#_Toc163378234)

[CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION 32](#_Toc163378235)

[5.1 Introduction 32](#_Toc163378236)

[5.2 Discussion 32](#_Toc163378237)

[References 34](#_Toc163378238)

[APPENDIX 36](#_Toc163378239)

# TABLE OF FIGURES

Table 1:Target population ............................................................................................................. 25

Table 2: sample size ..................................................................................................................... 26

Table 3:Year of study Frequence % of respondents ..................................................................... 29

Table 4:Gender Frequency % of respondents ............................................................................. 29

Table 5:Factor Frequency % of respondents ................................................................................30

Table 6:Factor Frequency % of respondents ................................................................................ 30

# ACRONYMS AND ABBREVIATION

**WHO:** World Health Organization?

**Covid-19**: Corona Virus

**ID:** Identification

# OPERATIONAL DEFINITION OF TERMS

## 

**Voice recognition:** it is a deep learning technique used to identify, distinguish, and authenticate a particular person’s voice. It evaluates an individual’s unique voice biometrics, including frequency and flow of pitch, and natural accent.

**Biometrics:** It is the measurement of physical, biological or behavioral traits that can be added to a database to then authenticate an individual’s identity.

**Fingerprint recognition:** It is the verification of a person’s identity by comparing their fingerprints with previously recorded samples, typically by means of a computerized system in which the person presses a finger against a sensor that scans a fingerprint.

**Facial recognition**: is a category of biometric software that maps an individual’s facial features mathematically and stores the data as faceprint. The software uses deep learning algorithms to compare a live capture or digital image to the stored faceprint in order to verify an individual’s identity.

# CHAPTER ONE: INTRODUCTION

## Background

The sudden emergence of COVID-19 in late 2019 forced the world into a scramble for solutions. With limited resources and a looming fear of the unknown, governments turned to emerging technologies to combat the pandemic (Adey et al., 2021).

Nearly three and a half years later, the need for safe practices and technological advancements to survive future outbreaks remains ever-present. The rapid evolution of COVID-19 highlighted the crucial role of technology in managing pandemics effectively.

A report by Agarwal et al. (2020) paints a grim picture of the pandemic's early days, with over 81 million confirmed cases and 1.7 million deaths globally by December 2020. The lack of treatment and immunity left populations vulnerable, sparking a global search for solutions. Industries like tourism, transportation, healthcare, and IT faced immense pressure, driving a constant push for innovation.

The pandemic became a breeding ground for new technologies. As the virus itself evolved, so too did the solutions. Emerging technologies like contactless fingerprint scanners, iris scanners, and vein authentication emerged to address the challenges posed by physical contact. However, with new technology comes new risks. We must carefully consider how to implement these advancements to ensure both security and public health.

In simpler terms, the pandemic exposed limitations in fingerprint scanners and other touch-based security systems (Adey et al., 2021). This highlighted the need for contactless solutions, forcing institutions to rethink their strategies. The key takeaway? We need safe and innovative technologies to navigate this new reality of frequent pandemics.

## 

## Problem Statement

This project seeks to investigate the risks of employing fingerprint geometry during the COVID19 pandemic. Due to the rapidly increasing number of corona virus cases in the country, and the primary mode of transmission being physical contact with infected people or surfaces, I would like to propose that the use of fingerprint geometry puts students or individual at very high risk of contracting this deadly corona virus at Kirinyaga University, and thus an alternate approach should be implemented in the events of future occurrences. When the alternate technique is put into place, it would lessen the vulnerability of students within the university to the corona virus.

## Objectives

### General Objective

The main objective of this proposal is to determine the risks of using fingerprint geometry during the time of covid-19 pandemic.

### Specific Objectives

1. To assess the risk of potential viral transmission through shared fingerprint scanning devices.

2.To evaluate the frequency and adequacy of cleaning and disinfection protocols for fingerprint scanning devices

1. To establish the efficiency and how fast the machine work.
2. To explore the feasibility and effectiveness of implementing contactless biometric identification system as an alternative to traditional fingerprint scanning technology.
3. To investigate the potential impact of fingerprint scanning devices on the spread of COVID-19 within the university community.

## Research Questions.

1. How does the use of fingerprint scanning at university gates impact the risk of viral transmission during the COVID-19 pandemic.
2. Did the speed of machine contributes to students’ vulnerability to covid-19?
3. How do cleaning and disinfection protocols for fingerprint scanning devices at university gate impact the mitigation of COVID-19 transmission.
4. What measures can be implemented to mitigate the potential health risks associated with using fingerprint scanning at Kirinyaga University gate incase of COVID-19 pandemic again. How does the frequency of fingerprint scanning at Kirinyaga University gate affect the potential spread of COVID-19 within the university and the community at large.

**Justification**

This research aims at determining the risk of using fingerprinting geometry approach as identification and security enhancement tool in Kirinyaga University during the period of covid 19, this was due to rapid increased number of covid -19 cases in the country and if this was established it would reduce the vulnerability of Kirinyaga University students and even the resident against exposure to covid-19. By doing so this would guarantee the health of students and the residents as far as covid-19 was concern at the same time enhances the economy of the location hence improving the residents’ living standard.

## Scope of the Study

## 

This research proposal focuses on the determining the risks of using fingerprint geometry as biometric approach of individual identification by enhancing the security matters in Kirinyaga University. The target population being the students in general and some residents who might have felt that effect when the students were affected.

# CHAPTER TWO: LITERATURE REVIEW

## 

This chapter views the literature in connection with the risk of using fingerprint geometry as identification tool of biometric approach to enhance security in various places within the globe more so the institutions and organizations. It views the theoretical framework pertaining to the study, conceptual framework and the summary of the reviewed literature.

## Theoretical Frame

The study finds some of the theories that are relevant in analyzing the concept of the risks resulting from the use of fingerprint scanning as one of the biometric approaches in identifying the individuals who are the students in Kirinyaga University as per this study.

## Biometric System.

A 2015 article by Abhilash Sharma explores biometrics, a technology used to identify individuals based on their physical or behavioral characteristics. Biometrics, as defined by Monrose and Rubin (2000), automates this process, offering a reliable method for user authentication in an increasingly security-conscious world (Bikos and Sklavos, 2001). Jain, Bolle, and Pankanti (2006) further emphasize biometrics as a legitimate science for identity determination.

Sharma categorizes biometrics into two main groups: physiological and behavioral. Physiological biometrics rely on physical attributes like fingerprints, facial features, or retinal patterns. These are unique physical markers captured directly from the body. Behavioral biometrics, on the other hand, focus on actions and habits, such as voice patterns or typing rhythms (Dewangan, 2015). This distinction is crucial when evaluating biometric technologies, as it impacts both performance and privacy considerations.

Fingerprint identification, a well-established biometric approach, compares the unique ridges and valleys on fingers, palms, or toes. Facial recognition technology uses digital images or video to identify or verify individuals by comparing them against a database of known faces (Thorat, Nayak, and Dandale, 2010). Hand geometry, a less common method, relies on the unique shape of an individual's hand for recognition. While popular a decade ago, it's rarely used today.

Sharma's article offers a valuable overview of biometrics, highlighting its role in addressing security concerns through reliable user authentication. It explores both physiological and behavioral characteristics, along with common biometric methods like fingerprint identification, facial recognition, and hand geometry. Understanding these concepts is essential for evaluating the effectiveness and potential privacy concerns associated with biometric technologies.

### Requirements for biometric identification system.

1. Accuracy and Reliability: The system must accurately identify individuals based on their unique biometrics (Drozdowski et al., 2020). False acceptance (unauthorized access) and false rejection (denied access to legitimate users) rates should be minimal (Clarke & Furnell, 2007).
2. Security: Protecting biometric data is paramount (Habibu, 2020). Strong encryption, secure storage, and access controls safeguard user data against unauthorized access, tampering, or theft.
3. Scalability: The system should grow with user needs, adapting to accommodate more users and diverse applications without sacrificing performance or security.
4. Usability: User-friendliness is key (Ertugrul et al., 2020). Enrollment and authentication processes should be smooth and convenient, with factors like speed and ease of use being crucial.
5. Spoofing Prevention: The system should be resilient against attempts to impersonate legitimate users. Techniques like liveliness detection or other anti-spoofing measures can help mitigate this risk.
6. Ethical Considerations: Transparency in data use, protecting user privacy, and establishing clear policies for handling biometric information are all crucial ethical aspects to consider.
7. System Reliability: Built-in redundancy and fault tolerance mechanisms ensure continuous operation. Backup authentication methods can address biometric sensor failures or technical issues.

#### Common biometric technologies.

According to this article published on 1st December 2004s by these authors; Rodrigo De LuisGarcia, Carlos Alberrola-Lopez, Otman Aghzout and Juan Ruiz –Alzola. The following are common biometric technologies existed and have been functioning before corona came and were productive in terms of security of which some of them as per now they put people at more risk of contracting this deadly covid-19 virus.

* 1. Iris Identification

Iris identification is a security system that relies on the unique colored part of your eye, the iris. Each person's iris has a complex pattern of lines and swirls, like a fingerprint for your eye. To use it, a special camera takes a high-resolution image of your iris. This image is analyzed to capture these unique patterns, which are then stored in a database. When you need to be identified, the system takes another image of your iris and compares it to your stored pattern. If the patterns match closely enough, you're verified!

* 1. Facial recognition

Ever wondered how your phone unlocks with a face scan? That's facial recognition at work! This technology identifies you based on your unique facial features.

Capture: A camera (regular or specialized) snaps a picture or grabs a video of your face.

Detection: Software cleverly finds your face in the image, pinpointing key features like eyes, nose, and mouth.

Feature Extraction: Think of this as creating a digital map of your face. The software measures distances between your eyes, analyzes the shape of your face, and captures other unique details. This information is then converted into a mathematical code, like a fingerprint for your face.

1. Comparison: This code, your "faceprint," is compared against a database of stored faceprints. If there's a close enough match, voila! You're identified.

Facial recognition offers a convenient way to verify your identity in various situations, from unlocking your phone to security checks at borders.

1. Fingerprint Identification

Fingerprints are a popular biometric because they've been around for a long time and are widely used in forensics and law enforcement. Each person's fingerprint is unique due to its pattern of ridges and valleys.

To capture a fingerprint, you simply place your finger on a scanner. Traditionally, these scanners use a light-based technology called "optical frustrated total internal reflection."

The scanner then analyzes the fingerprint image, focusing on details like loops, arches, and whorls. It also looks at smaller features like ridge endings and bifurcations (called "minutiae").

Fingerprint matching can be done in three ways: comparing minutiae points, overall ridge patterns, or a correlation score that combines both factors.

Modern fingerprint scanners use optical sensors with CMOS or CCD technology. These sensors are reliable and stable, making them ideal for securing building access, computer networks, and even ATMs. Some banks now use fingerprint readers for ATM authorization.

#### Fingerprint scanning technology

They explained the many types of fingerprint technology and their benefits ( sifuzzaman, 2019). Fingerprint scanning technologies are security systems that employ biometric to identify persons based on qualities that are unique to each individual. The young wonks team presented four forms of fingerprint scanning:

1. Optical fingerprint scanning.
2. Capacitive scanning
3. Ultrasonic scanning
4. Optical-capacitive scanning

The benefits of this fingerprint technology method includes better security and the comfort of using control solutions without exposing information to outsiders. Fingerprint scanners, one of the most sophisticated biometric modalities, guarantee near-perfect accuracy during authentication.

Faster access, fingerprint scanner can lock and unlock the password as compared to typing password. Greater convenience whereby the fingerprint scanners increases device and application-level security without overburdening the user with numerous credentials.

## Conceptual Framework

The risk of employing this technology as a security enhancement tool at Kirinyaga university could stem directly or indirectly. Therefore, under the conceptual framework, the dependent variables are the effectiveness or efficiency of the machine , the time of the student reporting to school, the numbers of security cases in the school, and finally the students cooperation. The independent variable is COVID-19.

### The effectiveness or efficiency of the machine as a risk in relation to covid-19.

This passage discusses how fingerprint scanner performance can impact student safety during COVID-19. Here's a summary:

Speed:

Faster scanners reduce queuing time, minimizing crowding and promoting social distancing.

However, speed doesn't guarantee virus-free interaction. An infected student could touch the scanner, potentially spreading the virus.

Slow scanners cause crowding, increasing infection risk, especially if not everyone wears masks.

Accuracy:

Faster fingerprint recognition reduces crowding, similar to faster scanners.

Maintenance:

Poorly maintained scanners can be slow and inaccurate, leading to crowding and higher infection risks.

Overall, fingerprint scanner effectiveness depends on speed, accuracy, and maintenance. Even a well-maintained scanner can't eliminate all risks, as a single infected student could spread the virus through contact.

**The time of students reporting to school as a risk factor in relation to covid-19.**  This element is based on the school schedule for students daily classes. Due to the limited number of machines used at the gate for fingerprint scanning, if for example, a quarter of the students in the entire school have classes schedule at the same time , the will arrive at the gate nearly the same time due to to campus students culture. This means there will be overcrowding in the gate, students waiting to clock-in order to be permitted in. Sometimes others did not have their masks on putting those who are safe at a high danger of contracting the deadly COVID-19.

## The number of security cases in the school as a risk in relation to covid-19

The number of security cases in the school as a risks of COVID-19. The number of security issues in the school will also influence the utilization of the fingerprint scanning machine/ equipment. This is clear in the scenario when there were no or few security cases in school, and while the students were congested, some may have been allowed in without clocking in, reducing crowding and thereby lowering students risk. Susceptibility to COVID-19. However, if there are many security cases, no students will be allowed in without clocking in, putting the pupils at high danger of getting corona virus while waiting to clock in, resulting in crowding without social distance ,and some may contract it only in the process of clocking to confirm their fingerprint for identification. All this is brought by use of fingerprint scanning approach.

**Student’s cooperation as a risk in relation to covid-19.**

This factor depends on the discipline of the students, the students might decide to be organized at the time of using this biometric machine at the gate during the time of entering the school. This is evident when student decide to maintain social distance during the time of clocking and also everyone wears a mask. At the same time they could do the opposite hence increasing the risks of exposing innocent and organized students to the risk of contracting covid-19.

potentially the entire nation. This is because when the risk of using this fingerprint approach is identified and controlled by implementing effective measures ,the health of students is protected, and because they interact with members of society, society is also safe and can carry on with their daily activities normally, boosting the country’s economy by a certain percentage.

## Research Gaps

This passage highlights a research gap in biometrics during COVID-19. While past research explored biometrics' role in controlling the virus spread, there's a lack of focus on the risks of fingerprint scanners specifically. Previous studies mainly emphasized the positive aspects of some biometrics (like facial recognition) in managing COVID-19. This knowledge is valuable for maintaining public health and economic activity. It also suggests contactless biometrics as alternatives for secure identification during pandemics. Existing research on fingerprint scanners often overlooks their downsides during COVID-19, focusing primarily on their advantages. This new research aims to bridge this gap by investigating the risks associated with using fingerprint scanners for identification during the pandemic. By identifying these risks and proposing solutions, the research can significantly improve safety not just for students but for society as a whole, ultimately contributing to better living standards and economic stability.

# CHAPTER THREE: RESEARCH METHODOLOGY

## Introduction

This chapter brings out the research designs and the methodology. These are the steps which will be used in data collection and analysis. The section contains the research instruments, sampling designs, data collection procedure, research design, target population and sampling methods.

## Research Designs

This research will use a descriptive approach. The students are supposed to provide feedback on how they felt when using the fingerprint scanning approach during the COVID-19 pandemic at Kirinyaga university. ( Anirudhan,2013) defines a descriptive study as one in which information is obtained without modifying the environmental using “ observational” studies. The research will be conducted utilizing questionnaires and machines swaps as primary and secondary data sources.

## Target Population

. The expected population size is 12000 that will be drawn from students according to their year of study that is first, second, third and fourth year respectively in Kirinyaga University. The study will adopt stratified random sampling technique. This will enable the researcher to capture variations among the students in terms of use of fingerprint scanning machines.

|  |  |
| --- | --- |
| Stratum | Target Population |
| First Years | 3500 |
| Second Years | 3200 |
| Third Years | 2800 |
| Fourth Years | 2500 |
| TOTAL | 12000 |

*Table 1:Target population*

## Sample and Sampling Techniques

## 

This study at Kirinyaga University will recruit 1500 students to represent the entire student body. The researchers will ensure all student years are included (equal representation) when using fingerprint scanners. This aligns with Paton (2002) who emphasizes sample size should match the study's goals. To gather data quickly and affordably, the researchers will use quota sampling. This non-probability method combines purposive and stratified sampling for a well-rounded dataset. Quota sampling is faster and cheaper than the individual methods, according to Kombo and Tromp (2006).

*Table 2: sample size*

|  |  |  |
| --- | --- | --- |
| Stratum | Total population | Sample size |
| First year | 3500 | 460 |
| Second year | 3200 | 440 |
| Third year | 2800 | 400 |
| Fourth year | 2500 | 200 |
| TOTAL | 12000 | 1500 |

## Data Collection Procedure

## This study collected data on student experiences with fingerprint scanners at Kirinyaga University. Here's a breakdown of the data collection methods used:

## Primary Data (firsthand information):

## Questionnaires were used to gather student opinions directly. These questionnaires were:

Semi-structured: containing both closed-ended (multiple choice) and open-ended questions for detailed responses.

## Anonymous: to ensure students felt comfortable expressing their views freely.

## Distribution methods:

## In-person surveys were conducted during school registration.

## The drop-and-pick method was used for students who lacked immediate time for response (questionnaires were left and collected later).

## Secondary Data (existing information):

## Research was conducted using library resources to understand:

## General use of fingerprint scanners. Reported benefits of fingerprint scanners (during COVID-19, if available).This information was then used to identify potential risks associated with fingerprint scanners during the pandemic.

## Pilot Study

## 

To determine the accuracy and relevancy of the data collection method, the questionnaire will be pre-tested on the 10% population. These respondents will be selected using the purposive sampling from the University but are not part of the research study population.

## Validity Test

Validity may be defined as the appropriateness, meaningfulness and usefulness of inferences makes based on the collected data. Appropriate reasoning is one that is relevant to the purpose of the information obtained. The biggest challenge this research study may experience is the respondents’ biases and misinformation because respondents may fear that the information they disclose or expose may have greater negative impact on their studies since the use of fingerprint scanning was the school project and failure to follow the school protocol will be treated as indiscipline, in this case, the questions will be sent before the institution confirm. To assure them that no confidential information will be asked during the time questionnaire are being administered.

## Reliability Tests

Reliability is a measure of the degree to which research instrument yields consistent research or data after repeated trials. Reliability is influenced by a random error which is a deviation from an accurate measurement because of the factors that are not properly addressed. Thus, the reliability will be established by use of Cronbach’s alpha coefficient with the ranges between 0and 1 to ensure the values are not more than 0.7.

## Data Analysis Procedure

Data analysis will be carried out at Kirinyaga university using descriptive statistics to compute the values of the outcomes and pie charts to highlight the findings of the dangers of utilizing fingerprint scanning as an identification method to increase security during the COVID-19 pandemic. Descriptive statistics helps researchers to summarize and arrange data m a very effective and relevant style, as well as gives tools for characterizing collections of statistical observations and reducing information to an intelligible form.

# 

# CHAPTER FOUR: FINDINGS AND RESULTS

## This study at Kirinyaga University investigated the risks of fingerprint scanners during the COVID-19 pandemic. Researchers surveyed 100 students, achieving an 80% response rate (80 completed questionnaires).

## The findings highlighted the risks associated with fingerprint scanners. Participants indicated a preference for alternative strategies in case of future outbreaks. Many respondents suggested improved efficiency, accuracy, increased entry points, and better scheduling could help manage outbreaks.

## While fingerprint scanners are widely used for access control, the study suggests proper management is crucial. The research concluded that fingerprint scanners exposed Kirinyaga students to a higher risk of COVID-19 infection. It recommends alternative entry systems for future outbreaks. The study presented data in tables and analyzed it using measures of central tendency, frequencies, and percentages.

## Table 3:Year of study Frequence % of respondents

|  |  |  |
| --- | --- | --- |
| Year of study | Frequency | % of respondents |
| Year one | 20 | 25 |
| Year two | 19 | 24 |
| Year three | 20 | 25 |
| Year four | 21 | 26 |
| Total | 80 | 100 |

## Table 4:Gender Frequency % of respondents

|  |  |  |
| --- | --- | --- |
| Gender | Frequency | % of respondents |
| Male | 43 | 54 |
| Female | 37 | 46 |
| Total | 80 | 100 |

## Table 5:Factor Frequency % of respondents

|  |  |  |
| --- | --- | --- |
| Factor | Frequency | % of respondents |
| Affected directly | 50 | 62 |
| Affected indirectly | 30 | 38 |
| Total | 80 | 100 |

## Table 6:Factor Frequency % of respondents

|  |  |  |
| --- | --- | --- |
| Factor | Frequency | % of respondents |
| Literate | 33 | 41 |
| Illiterate | 47 | 59 |
| Total | 80 | 100 |

# CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATION

## 5.1 Introduction

The chapter aims at providing a conclusion and discussion of the about the risk of using fingerprint scanning as a recognition tool in Kirinyaga University during the corona virus pandemic. The study focused on Kirinyaga University where the biometric is entirely utilized by the students. The findings of the study on the risk of fingerprint scanning are discussed in this chapter.

## 5.2 Discussion

Gender distribution among students

In the study out of the 80 participants 43 of the total population were male accounting for 54% of the total population. On the other hand 37 of the respondents were female which represented 46% of the total population studied. The results of the study suggests that males were more affected than females.

Illiterate and literate

41% of the student under study had knowledge about the fingerprinting scanning system compared to the 59% of the students who had never encountered the fingerprint scanning system. Students without knowledge about the biometric system are more vulnerable to being infected because sometimes sanitization of hands is not a basic thing to them. The entire population can be at risk if students without knowledge of the system are affected.

Affected directly and affected indirectly

The study examined students in Kirinyaga University on the use of fingerprint scanning in relation to the effect the system causes to the students. The false reject rate of the system attributes to the students who are affected directly by the system. Students tend to spend more time at the entry station and this is a vulnerability to the students. The long time spend at the fingerprint scanner gives time for the virus to be transferred to the scanner and can infect the rest of students who are not affected by the false reject rate directly.

Based on the responses from the questionnaire filled, I can conclude that the use of fingerprint scanning recognition system impacted more risk of students being affected by its use during the Covid 19 pandemic. However it was discovered that the fingerprint scanning also had some advantages. With increased efficiency, correctness, more entry station and maintenance it can be used as a recognition tool of choice to avoid manual verification of students using convectional methods.

# References

*17*(7), 2309.

Adey, P., Hannam, K., Sheller, M., & Tyfield, D. (2021). Pandemic (Im)mobilities. *Mobilities*, *16*(1), 1–19. https://doi.org/10.1080/17450101.2021.1872871

Agarwal, S., Punn, N. S., Sonbhadra, S. K., Tanveer, M., Nagabhushan, P., Pandian, K. K., & Saxena, P. (2020). Unleashing the power of disruptive and emerging technologies amid COVID19: A detailed review. *arXiv preprint arXiv:2005.11507*.

Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., & Nagem, T. A. (2018). A multibiometric iris recognition system based on a deep learning approach. *Pattern Analysis and Applications*, *21*(3), 783-802

Andronikou, V., Demetis, D. S., & Varvarigou, T. (2005). Biometric implementations and the implications for security and privacy. *Journal of the Future of Identity in the Information Society*, *1*(1), 20-35.

Biko’s, A. N., & Slaves, N. (2012). LTE/SAE security issues on 4G wireless networks. *IEEE Security & Privacy*, *11*(2), 55-62.

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. *Ieee access*, *8*, 90225-90265.

Chew, V., Phillips, M., & Yamada Park, M. (2020). COVID-19 impacts on immigration detention: Global responses.

Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers & Security*, *26*(2), 109–119. https://doi.org/10.1016/j.cose.2006.08.008

Coronavirus disease (COVID‐19): An updated review based on current knowledge and existing literature for dermatologists. *Dermatologic Therapy*, *33*(4), e13677.

Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods.

Dungan, S. K. (2015). Human authentication using biometric recognition. *International Journal of Computer Science & Engineering Technology (IJCSET)*, *6*(4), 240-245.

Hua, J., & Shaw, R. (2020). Corona virus (Covid-19)“infodemic” and emerging issues through a data lens: The case of china. *International journal of environmental research and public health*,

In *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine* (pp. 184193). IEEE.

Jain, A. K., Bolle, R., & Pankanti, S. (Eds.). (2006). *Biometrics: personal identification in networked society* (Vol. 479). Springer Science & Business Media. Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine* (pp. 184-193). IEEE.

Janeiro, L., & Patel, M. K. (2015). Choosing sustainable technologies. Implications of the underlying sustainability paradigm in the decision-making process. *Journal of Cleaner Production*, *105*, 438-446.

Kaur, I., Sharma, A., Jakhar, D., Das, A., Aradhya, S. S., Sharma, R., ... & Mhatre, M. (2020).

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, *16*(4), 351-359.

Morganstein, J. C., Fullerton, C. S., Ursano, R. J., Donato, D., & Holloway, H. C. (2017).

Pandemics: health care emergencies. *Textbook of disaster psychiatry*, 270-284.

Righi, G., Peissig, J. J., & Tarr, M. J. (2012). Recognizing disguised faces. *Visual Cognition*, *20*(2), 143-169.

Thorat, S. B., Nayak, S. K., & Dandale, J. P. (2010). Facial recognition technology: An analysis with scope in India. *arXiv preprint arXiv:1005.4263*.

Yoruk, E., Konukoglu, E., Sankur, B., & Darbon, J. (2006). Shape-based hand recognition. *IEEE transactions on image processing*, *15*(7), 1803-1815.

Yu, S. (2016). Big privacy: Challenges and opportunities of privacy study in the age of big data. *IEEE access*, *4*, 2751-2763.

Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., & Busch, C. (2020). Demographic Bias in Biometrics: A Survey on an Emerging Challenge. *IEEE Transactions on Technology and Society*, *1*(2), 89–103. https://doi.org/10.1109/TTS.2020.2992344

Ertugrul, E., Li, P., & Sheng, B. (2020). On attaining user-friendly hand gesture interfaces to control existing GUIs. *Virtual Reality & Intelligent Hardware*, *2*(2), 153–161. https://doi.org/10.1016/j.vrih.2020.02.001

Georgiev, M. K. (2022). *Continuous touchscreen biometrics: authentication and privacy concerns*. Ora.ox.ac.uk. https://ora.ox.ac.uk/objects/uuid:3702b4ac-7294-41b3-bfd4-6a160c3cf11a

Habibu, T. (2020, March 1). *Development of secured algorithm to enhance the privacy and security template of biometric technology*. Dspace.nm-Aist.ac.tz. http://dspace.nm-aist.ac.tz/handle/20.500.12479/900

Mbunge, E., Akinnuwesi, B., Fashoto, S. G., Metfula, A. S., & Mashwama, P. (2020). A critical review of emerging technologies for tackling COVID ‐19 pandemic. *Human Behavior and Emerging Technologies*, *3*(1). https://doi.org/10.1002/hbe2.237

# APPENDIX

1: Questionnaire

Dear Respondents,

The questionnaire is aimed at collecting information about the determination of the risk of use of fingerprint scanning during this saperiod of covid-19 in Kirinyaga University as a way of enhancing security. It will only require the participation of all your authenticity will add value to the study and your response will be used for academic purpose only. However if you are not sure of any given question or your response to the question, it is good to tick the number under neutral. Your response will be held in total confidence and only be used for the purpose of the study. Thank you in advance.

**INSTRUCTIONS**

Please do not write your name anywhere in the questionnaire.

PART A. DEMOGRAPHIC INFORMATION.

Kindly tick appropriately in the brackets provided below.

Gender: Male [ ] Female: [ ]

School

of……………………………………………………………………………………………………

.

Course………………………………………………………………………………………………

………..

Year of

study……………………………………………………………………………………………….

PART B.

How many times do you report to school daily?

How often do you report to school weekly?

Do you sanitize after and before using the machine? YES [ ] NO [ ]

Do you support replacement of fingerprint scanning with other approach that serve same purpose but less risk as compared to fingerprint scanning during this period of covid-19?

YES [ ] ( N0)