A Biometric Authentication Scheme to Enhance Access Integrity of Higher Education Institutions

Boniface Mwangi Wambui[1,2]

[1]School of Computing and Informatics
Mount Kenya University,
Thika, Kenya.
Email: bonniemwangi91 [AT] gmail.com

[2]School of ICT,Media & Engineering
Zetech University,
Ruiru,Kenya.
Email: boniface.mwangi [AT] zetech.ac.ke

Abstract— **Access control and security within higher education institutions are of paramount importance in safeguarding sensitive information and resources. Conventional authentication methods, such as passwords and identification cards, have proven susceptible to security breaches and identity theft. To address these vulnerabilities, this paper presents a novel biometric authentication scheme tailored to the unique needs of higher education institutions. Deploying a trustworthy user authentication system became a key responsibility for both access control and securing user's private data with the rapid rise of electronic crimes and their connected difficulties. For both private and public use, human biometric features including voice, finger, iris scanning, face, signature, and other features offer a solid security level. This paper provides a comprehensive overview of the biometric authentication scheme, outlining its architecture, functionality, and security measures. We also present the results of a pilot implementation within a higher education institution, demonstrating improved access security and user satisfaction. Ethical considerations and privacy safeguards are discussed to ensure responsible biometric data handling. For a long time, numerous biometric authentication solutions have been considered. owing to the distinctiveness of human biometrics, which was important in thwarting imposters' attacks. Only a few of the key issues endangering system integrity and impeding effective service delivery include identity theft, spoofing, and the reliability of authentication systems in higher education institutions. From the experiment the total number of tests was 15, as the threshold was one attempt. While fingerprint authentication typically took 2.67 seconds, palm vein authentication often took 9.15 seconds. Therefore, the palm vein was slower than the fingerprint in terms of speed. The structure of the hand and the distance between the palm and the scanner were the determining elements in pal's slow authentication speed. The palm vein system has a 93.33% accuracy rate compared to the fingerprint system's 60% accuracy rate, making it the preferable model to use in a higher education setting. A biometric system's success or failure is influenced by a variety of variables and application domains. The purpose of this work is to discuss an appropriate biometric authentication model that may be used to improve the reliability of biometric systems in institutions of higher learning. The proposed biometric authentication scheme offers a forward-looking solution to the access integrity challenges faced by higher education institutions. By adopting this technology, institutions can bolster their security posture, protect sensitive data, and provide a more convenient and secure access experience for students, faculty, and staff.**

Keywords--- Authentication, integrity, security, accuracy, attacks

I. INTRODUCTION

In order to ensure that organizational and/or private data is well maintained and accessed only by the designated party, it is essential to implement a secure biometric infrastructure. It is crucial that there be a way to validate only those people who are listed as students at a prestigious college or university. The science of biometrics, which uses a person's physiological attributes or behavioral characteristics to identify them, has made considerable strides in a number of fields, including access control, authentication, security, and surveillance. Biometric features are more difficult to forge or lose than traditional authentication methods like tokens or passwords, and they are not as prone to loss or oblivion. Uni-biometric systems, which rely solely on a single biometric attribute for recognition, are frequently plagued by problems such biometric data variability, a lack of distinctiveness, poor recognition accuracy, and spoof assaults. In order to solve these issues, a multi-biometric system that combines various biometric features from two or more sources, such as a person's fingerprint, finger vein, iris, and face, not only increases recognition accuracy but also makes it harder to trick or impersonate the system.

According to Yang et al. (2018), The finger vein biometric is theoretically resistant to spoofing since finger-veins are implanted inside a finger and must be recorded by an infrared sensor. Fingerprints are one of the most frequently used and thoroughly researched biometric features. In order to spoof a biometric system, an adversary must normally get a biometric sample to utilize as the foundation for the spoofing effort. The finger-vein biometrics is very resistant to spoofing since it cannot be seen or traced, unlike the face or fingerprint, which can be seen or traced. Compared to a fingerprint- or finger-vein-based uni-biometric system, the multi-biometric system based on fingerprints and finger veins holds more and more discriminative information. The purpose of this work is to discuss an appropriate biometric authentication model that may be used to improve the reliability of biometric systems in institutions of higher learning

According to Wambui et al. (2022), One solution to the aforementioned issues is the use of contactless security technologies. A new technology that takes advantage of the shortcomings in the fingerprint method is palm vein recognition. Vein innovation is appealing in nature since users do not need to make touch with the scanner, reducing the risk of sickness (Martin, 2007). The majority of businesses have given up on biometrics because touch-based surface transmission of the Covid-19 pandemic rendered them useless. Biometric gadgets may also transmit other diseases. According to, this kind of identification could soon become the norm (Jacobsen & Sandvik, 2018). Now that most transfers and swaps take place online, a person must demonstrate to a computer that they are who they say they are.

II. LITERATURE REVIEW

2.1 Overview of biometric systems

The origin of biometric technology dates back a few thousand years. Authentication and enrollment are two examples of the two sorts of biometric system modes that can be used. In the latter, the biometric system converts the person's biometric characteristics into a digital form and stores the outcome in a different storage system. However, the biometric technology is intended to be utilized in authentication mode for an identification or confirmation process. The biometric system compares the recorded features with the template during the confirmation process to authenticate the user's identification (Abdulrahman et al,2023). Biometric systems are a type of technology that utilizes unique physiological or behavioral characteristics of individuals to verify their identity. These systems have gained significant popularity in recent years for various applications, including security access, authentication, and identity verification. Here's an overview of biometric systems:

a) **Fingerprint Recognition:** This is one of the most common biometric modalities. It involves capturing and analyzing the unique patterns of ridges and valleys on an individual's fingertips. Without saving the image or even allowing for its reconstruction, fingerprint recognition creates a unique template from the fingerprint's characteristics. The first image for fingerprint identification is obtained through a live finger scan performed when the finger is in close proximity to a reader device that can also check for validating characteristics like temperature and pulse. Since the user's finger really contacts the scanning device, the surface might eventually become oily and foggy, which lowers the sensitivity and dependability of optical scanners. Since the covered silicon chip itself serves as the sensor, solid state sensors get beyond this and other technical challenges. Because the covered silicon chip is the sensor, solid sensors get around these and other technical challenges. Solid state devices are less sensitive to dirt and grease because they build a compact digital image by sensing the ridges of the fingerprint via electrical capacitance. There is a general consensus that fingerprint recognition is trustworthy enough for commercial use, and several suppliers are aggressively marketing readers as part of Local Area Network login methods (Phadke, 2013).

b) **Palmprint Recognition:** According to Parihar (2019), Vascular biometrics is another name for vein recognition. Many studies discovered in the early years that deoxidized hemoglobin in the vein vessels absorbs light at a wavelength between 750 and 960 nm, which reduces the veins' ability to reflect light back and causes them to appear black. Then, in order to verify the subject, this vein design is compared to an already-enrolled sample. The vein recognition method makes this possible. Because the authentication information is present beneath a person's skin, vein-based recognition techniques are significantly more secure and one of a kind than other techniques. Since other methods like palm prints, facial expression, skin, voice, and DNA recognition cannot distinguish between identical twins, vein-based identification systems are now primarily used. With the help of contemporary technology, a person can store their personal information anywhere, at any time, and an unauthorized person cannot access it. There are numerous uses for this technology, including in banks, government offices, and the issuance of passports.

c) **Iris Recognition**: Iris recognition technology identifies individuals by analyzing the unique patterns in the colored part of their eyes, known as the iris. Because it is shielded inside the eye itself, retinal recognition develops a "eye signature" from the retina's vascular structure that is incredibly consistent and trustworthy (Cook et al., 2019). By having the subject look through a lens at an alignment target, a picture of the retina is taken. The feature often remains constant and continuously available since conditions or injuries that might affect the retina are rather uncommon in the general population.

d) **Face Recognition**: Face recognition systems capture and analyze facial features, such as the distance between the eyes, nose shape, and jawline. Utilizing this technique, the distinguishing features of the face are captured. Since no interaction is necessary, it is non-intrusive. The human face may vary over time, and using glasses or having hair can impair this technology. Face recognition is more ideal for safety and security applications now that it can be used to identify a target from a distance using high-resolution cameras with zoom capabilities. Software for facial recognition can be built up quickly (Cook et al., 2019).

e) **Hand Vein**: Infrared imaging is used to measure the changes in the subcutaneous features of the hand in an effort to identify individuals. Similar to facial recognition, it has additional considerations for three-dimensional space and hand position. Similar to retinal scanning, it creates a template from the pattern of the veins in the hand and then compares that template to templates kept in a database. In manufacturing or shop-floor applications where hands might not be clean enough to effectively scan using a normal video or capacitance technique, the use of infrared imaging gives some of the same advantages as hand geometry over fingerprint identification.

f) **Voice Recognition:** Voice recognition systems analyze the unique characteristics of an individual's voice, including pitch, tone, and speech patterns. Automatic Speaker Verification (ASV) and Automatic Speaker Identification (ASI) are the two main ways used to classify voice recognition techniques. In a two-factor scenario, speaker verification uses speech as the authenticating property. Speaker identification tries to determine a person's identity using voice (Cook et al., 2019). Voice recognition recognizes a person by comparing specific voice characteristics against templates kept in a database. At the time of enrollment, voice systems must be tuned to the enrollee's voice, and many enrollment sessions are frequently required. In feature extraction, formants or sound qualities particular to each person's vocal tract are often measured. The pattern matching techniques used in face recognition and voice recognition are comparable.

2.2 Attack vectors of biometric systems

According to Abdulrahman (2023), Biometric systems are designed to provide secure and convenient authentication based on an individual's unique physiological or behavioral characteristics. However, like any technology, they are not immune to security vulnerabilities and attack vectors. Here are some common attack vectors and potential security risks associated with biometric systems:

1 Spoofing Attacks:

- Presentation Attacks: Attackers may attempt to present fake or stolen biometric data (such as a fingerprint or facial image) to the system to gain unauthorized access.

- Gummy Fingers: For fingerprint recognition systems, attackers may use materials like gelatin or silicone to create fake fingerprints.

- 2D Photos or Videos: Facial recognition systems can be fooled by presenting a 2D photo or video of the authorized person's face.

2. Replay Attacks: - Attackers may record a legitimate biometric authentication session and then replay it to gain unauthorized access.

3. Template Attacks: - Biometric systems often store templates or feature vectors derived from the biometric data, which can be stolen or reverse-engineered to replicate an individual's biometric characteristics.

4. Man-in-the-Middle Attacks: - An attacker intercepts the communication between the biometric sensor and the authentication system, potentially altering or capturing the biometric data.

5. Database Breaches: - If the biometric templates or data are stored in a central database, a data breach can expose sensitive biometric information, making it available for unauthorized use.

6. Insider Threats: - Employees or individuals with legitimate access to the biometric system may misuse their privileges to compromise the system's security.

7. Biometric Enrollment Attacks: - Attackers may manipulate the enrollment process to introduce malicious biometric data into the system, making it easier for them to later gain access.

8. Biometric Spoof Detection Bypass: - If the biometric system includes anti-spoofing measures, attackers may attempt to bypass or defeat these measures using advanced techniques.

9. Environmental Factors: - Environmental conditions like lighting, noise, or sensor quality can affect the accuracy of biometric recognition, potentially leading to false positives or negatives.

10. Cross-Modal Attacks: - Attackers may attempt to use one biometric modality (e.g., voice) to impersonate another (e.g., face), exploiting vulnerabilities in multimodal biometric systems.

To mitigate these attack vectors and enhance the security of biometric systems, organizations should implement the following best practices:

a) *Use liveness detection mechanisms to detect and prevent spoofing attacks.*
b) *Encrypt biometric data during transmission and storage.*
c) *Implement robust authentication protocols to prevent replay attacks.*
d) *Protect biometric templates with strong encryption and access controls.*
e) *Continuously monitor for unusual patterns of biometric usage.*
f) *Educate users about the importance of protecting their biometric data.*

Keep in mind that no authentication system is entirely foolproof, and a layered security approach that combines biometrics with other authentication methods (such as passwords or smart cards) can provide enhanced security (Supriya,2014). Additionally, regular security audits and updates are crucial to maintaining the integrity of biometric systems. Biometric systems offer a convenient and secure way to verify identities and grant access, but they also raise ethical and privacy considerations that need to be carefully addressed as these technologies become more prevalent.

2.3 Weaknesses of Biometric Systems

Biometrics, the use of unique physical or behavioral characteristics for identification and authentication purposes, has several strengths but also comes with some notable weaknesses. Here are some common weaknesses of biometrics:

1.Immutability and Irrevocability: Biometric traits are generally considered constant and unchangeable. However, if a biometric template is compromised or stolen, individuals cannot easily change their biometric characteristics, unlike passwords or tokens which can be reset or replaced.

2.Privacy Concerns: Collecting and storing biometric data can raise significant privacy concerns. If biometric databases are breached, individuals' sensitive information could be exposed, leading to identity theft or other malicious activities.

3. Accuracy and False Positives/Negatives: Biometric systems are not perfect and can produce false positives (when an unauthorized person is authenticated) or false negatives (when an authorized person is not authenticated). The accuracy of biometric systems can be affected by factors such as environmental conditions, sensor quality, and changes in an individual's biometric traits over time.

4. Cost: Implementing biometric authentication systems can be costly. Biometric sensors and hardware are typically more expensive than traditional authentication methods like passwords or smart cards. Moreover, maintaining and upgrading biometric systems can also be costly.

5. Cultural and Societal Factors: Some biometric modalities may not be culturally or socially acceptable to all individuals or groups. For example, facial recognition technology has faced backlash due to concerns about surveillance and potential bias in its application.

6. Spoofing and Forgery: Biometric systems can be vulnerable to spoofing, where an attacker uses a replica or imitation of a biometric trait to gain unauthorized access. For instance, fingerprint sensors can be fooled with a high-quality replica of a fingerprint.

7. Lack of Standards: The absence of standardized biometric data formats and interoperability can hinder the widespread adoption and integration of biometric systems across different platforms and organizations.

8. Biometric Data Storage: Storing biometric data securely is a challenge. Biometric templates must be stored in a way that prevents unauthorized access, and this can be complex and expensive to implement.

9. Health Concerns: Some biometric modalities, like iris scanning or retinal scanning, involve exposing individuals to potentially harmful levels of light. This can be a concern for individuals with certain medical conditions or sensitivities.

10. Ethical and Legal Issues: The use of biometrics raises various ethical and legal questions, including issues related to consent, data ownership, and the potential for abuse or misuse of biometric data.

11. Lack of Universality: Not all individuals may have suitable biometric traits for authentication. Some people may have medical conditions or injuries that affect the reliability of certain biometrics.

To address these weaknesses, organizations and governments need to carefully consider the ethical and privacy implications of biometric systems and implement robust security measures to protect biometric data (Nalinakshi,2013). Additionally, the combination of biometrics with other authentication factors, such as passwords or tokens, can help mitigate some of these weaknesses.

III. METHODOLOGY & RESEARCH DESIGN

A mixed methodological approach was used in this work, and an experimental research design was used (Polit & Hungler, 1999). Experimental research design is a scientific approach used to investigate the cause-and-effect relationships between variables. It is a systematic method for studying phenomena and is commonly used in various fields such as psychology, biology, physics, and social sciences. The primary goal of experimental research is to manipulate one or more independent variables to observe their impact on a dependent variable while controlling for potential confounding variables. According to Zang (2014) Experimental research design is a powerful tool for establishing causal relationships between variables, but it requires careful planning, control, and ethical considerations to ensure the validity and generalizability of the results. Proper randomization, control of extraneous variables, and ethical treatment of participants are essential aspects of experimental research.

It was helpful in identifying the advantages and disadvantages of the services offered as well as how well the biometric system worked. It was acceptable because it gave the researcher a deeper comprehension of the study. The research was conducted at Mount Kenya university Thika with a sample of 169 staff and 123 questionnaires were filled. Faculty and students at Mount Kenya University served as the study's target population. Given that the university has been utilizing biometric technologies for over 7 years, it was chosen. They are utilized for student registration and verification, gate entry, access to particular rooms, and class attendance. Experts validated the generated model based on the results of the experiment. Regarding the biometric technologies employed in this study, the researcher's attention was drawn to the university's faculty and students. The experiment was crucial in demonstrating the superiority of the palm vein model over the fingerprint authentication technique.

IV. FINDINGS

4.1 Demographic Information

4.1.1 Questionnaire Response Rate

During the actual data collection, the researcher distributed 169 questionnaires to the participants; 123 of them or 73% of the completed questionnaires were returned. According to Mugenda & Mugenda (2003), a response rate of 50% is seen as sufficient for analysis and reporting, a rate of 60% is regarded as good, and a rate of 70% or higher is regarded as outstanding. Based on this claim, the response rate was excellent. Everyone who worked in the study's target industry got a chance to take part. The demographic information was based on the participants' ages, genders, marital statuses, departments in which they worked, levels of education, length of time spent working at HEIs, and career paths.

Table 1: Demographic Information

	Demographic Information					
			Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Age		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
	Valid	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		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
	Valid	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			6	4.9	4.9	4.9
		1month-4years	38	30.9	30.9	35.8
	Valid	5-8 years	55	44.7	44.7	80.5
		9-12 years	22	17.9	17.9	98.4
		Above 12 years	2	1.6	1.6	100.0

Source: Field data (2021)

The educational backgrounds of the respondents were displayed in Table 1 above. Degree holders accounted for the majority with a frequency of 62, or 50.4% of the total questionnaire answer rate. With a frequency of 36, or 29.3%, master's holders came in second. Certificate/diploma holders came in third, with a frequency of 17, or 13.8%. PhD and other respondents who did not state their educational level had a frequency of 3, or 2.4%. Two respondents (1.6% of the total) never chose any of the available options in the survey.t

Table 1 above shows the respondents' academic backgrounds at Mount Kenya University Thika. With a frequency of 38, the bulk of respondents (30.9 percent) were lecturers. There were just 2 system administrators, or 1.6%, according to the analysis above. There were 7 customer service agents, or 5.6% of the workforce, 24 administrative assistants, or 19.5%, and 9 security officers, or 7.3%. Due to their strategic placement at the entry points, where students must utilize biometric systems in order to access the university's facilities as well as the library, security officers were extremely important.24.4% of respondents chose the other option, which asked about their professional backgrounds, such as accountant or procurement officer.

4.2 Biometric technologies used by the respondents

Table 2: Type of biometric used

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

Table 2 above shows that 68.3 % of respondents had only ever utilized finger prints as a biometric identification method. According to usage, some people have combined several biometric technologies, such as fingerprint, face, and iris detection with voice recognition. This was responsible for 31.7%. The study deduced from this that the fingerprint was the most widely used, affordable, and accessible biometric technology.

4.3 Biometric Technologies Investment in the University

Table 3: Types of biometric invested 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)

The type of biometric system that the university had previously purchased is shown in Table 3 above. According to the analysis, 102 respondents, or 82.9%, said that only one type of fingerprint system had been used in the past. In contrast, 17 respondents, or 13.8%, said that several types of technologies, including face and fingerprint recognition, were in use. Meanwhile, 2.4% said that none had been used in the past, and 0.8% had never suggested.

4.4 Weaknesses of biometric systems

Table 4: Weaknesses of biometrics

		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)

Table 4's findings show that 66.7 percent of respondents agreed that the present security measures are flawed, 30.1 percent disagreed, 0.8 percent were undecided, and 3.4 percent did not respond to the question. To address these weaknesses, organizations and governments need to carefully consider the ethical and privacy implications of biometric systems and implement robust security measures to protect biometric data. Additionally, the combination of biometrics with other authentication factors, such as passwords or tokens, can help mitigate some of these weaknesses. Studies on the usage of biometrics have revealed that the bulk of the systems are prone to multiple errors and hacking. The biometric authentication used by smartphone devices like the iPhone and some Android handsets is an excellent example. False acceptance and rejection are frequent occurrences that raise serious concerns about the viability of the technology (Das, 2014). On the other side, the public is reluctant to use the technology because they believe it is ineffective because these systems are readily breached and information was taken. The designers and developers must refocus and correct the mistakes in order to solve this problem.

4.5 Authentication Failure of biometric system

Table 5: Authentication Failure

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

Source: Field data (2021)

Table 5 shows that 59.3% of respondents have experienced a situation in which the users could not be verified using the biometric technology that is currently in use. This occurred both during lecturer clocking and while personnel attempted to enter university property. When other users attempted to access the control rooms, they were refused entry.39% of the respondents said they had never had an authentication issue.1.6% of the respondents omitted their response entirely. When a user placed their finger in the sensor, these authentication issues occurred because the database template failed to compare the user's credentials with the data it had saved. The institution used biometric technology for access to the library, student registration, class attendance, exam attendance, lecturer clock-in, access to the control rooms, and access to the directorate of tests office.

4.5 Level of Security

Table 5 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)

The response from the respondents regarding the shortcomings of biometric systems is shown in Table 5 above. The proposed contactless security systems, according to 83.7% of respondents, will address the issues and improve data integrity in service delivery.6.5% said the proposed security solution won't improve integrity in any way.7.3% of respondents did not react at all, while 2.4% were unsure. It was clear from the analysis that the suggested security model will address the current security issues. This clearly showed the need for a better model that can be better for strengthening the security of the data with a high percentage of 83.7%.

4.6 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 6 below displays regression coefficients, an ANOVA summary, and the model's outcomes.

Table 6 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)

With an R2 of 70.0 percent, Table 6 demonstrates that the data and model for the development of a security model utilizing biometric technology for higher education institutions were well matched.

Table 7 ANOVA implementation of a logical security model using biometric systems for higher learning institutions

ANOVA[a]

Model		**Sum of Squares**	**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)

Because the F value obtained at (11,98) at 95 percent confidence interval, which is less than the table value of 0.763534 at 95 percent confidence interval as shown in table 7 above, was less than the table value of 0.763534 at 95 percent confidence interval, we reject the null hypothesis that there was statistical no significance in the design of a security model using biometric systems for higher education institutions.

4.7 Experimental Results

The controlled group was made up of 15 university students who were chosen at random. Some volunteers had moist, unclean palms and fingerprints during the trial, while others were fatigued

Table 8 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 9 Biometric technologies used by control group

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

Source: Field data (2021)

According to table 9 above 80% of the participants had used fingerprint system while 20% had used more than one technology.

Table 10 Suitable authentication system

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

Source: Field data (2021)

According to Table 10 above, 93.3% of respondents believed the palm vein (contactless) technology was better than the current fingerprint system, which garnered only 6.7% of the vote. The majority of participants chose the palm vein because it was unaffected by palm wear, unlike the fingerprint, which the system stopped registering or authenticating users with who had worn fingers, muddy fingers, or wet fingers.

Table 11 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
Finger print	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 11 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.

V. DISCUSSIONS

The results of the respondents clearly showed that fingerprint security systems, which accounted for 68.3 percent of the respondents, are the most widely used security systems. For the previous four years, the University has been utilizing the system to verify students' identities before allowing them entry to the campus, as well as to track lecturers' arrival and departure times, as well as student attendance in class. It was also used to enter the control room, library, and directorate of finance offices, giving proof that it was the most popular type of authentication at the university. The largest risk to fingerprint biometric technology is theft or release of template information. Because each person has a unique, limited-edition fingerprint that remains constant throughout the length of their lifetime, a fingerprint biometric breach poses a lifetime danger to that person's security and privacy (Onifade, 2020). According to table 3, the investigation showed that 102 respondents, or 82.9%, claimed that just one kind of fingerprint system has ever been used. The current security procedures are defective, according to 66.7 percent of respondents. In contrast, 30.1 percent disagreed, 0.8 percent were unsure, and 3.4 percent did not reply to the question. Organizations and governments must carefully evaluate the moral and privacy implications of biometric systems and put in place strong security mechanisms to safeguard biometric data in order to solve these flaws. People may better understand how biometrics may protect personal information with increased security awareness, which will increase their desire to employ biometrics. Last but not least, as security awareness is the initial step in information security management, it is critical to continue teaching users at all levels about security (Chen et al., 2018). According to 83.7% of respondents, the proposed contactless security technologies will address the problems and enhance data integrity in service delivery.6.5% of respondents thought the suggested security measure won't in any way advance integrity.2.4% of respondents were undecided, while 7.3% showed no reaction at all.93.3% of respondents in the experiment thought the palm vein (contactless) technology was superior to the present fingerprint technique, which received only 6.7% of the vote. In contrast to the fingerprint, which the system ceased registering or authenticating users with whether they had worn fingers, muddy fingers, or damp fingers, the majority of participants preferred the palm vein because it was unaffected by palm wear. The fingerprint system yielded an FRR of 40% while the palm vein system only yielded 6.67%. According to the aforementioned data, the palm vein scanner outperformed the current fingerprint technology in terms of authentication. The total number of tests was 15, as the threshold was one attempt. While fingerprint authentication typically took 2.67 seconds, palm vein authentication often took 9.15 seconds. Therefore, the palm vein was slower than the fingerprint in terms of speed. The structure of the hand and the distance between the palm and the scanner were the determining elements in pal's slow authentication speed. The palm vein system has a 93.33% accuracy rate compared to the fingerprint system's 60% accuracy rate, making it the preferable model to use in a higher education setting.

VI. CONCLUSIONS

Consumers can prevent data leaks and protect their privacy by increasing security awareness and understanding of security issues. But many companies and academic institutions still don't have enough security awareness training (Furnell & Vasileiou, 2017). This study has led to the recommendation that companies that work with data and information, including educational institutions, regularly perform security awareness programs and training. In order to strengthen current security measures that make it far more difficult for fraud to occur by prohibiting ready impersonation of the authorized user, biometrics offers a valuable method. However, in order to employ biometrics, we must first register individuals, which could be expensive and burdensome for users. Additionally, we need a socially and culturally appropriate way to verify the biometric at the point of authentication. The requirement for safeguards for the usage of the biometric may also result from these issues. We must be mindful of the operational elements that could lead to biometrics' failure while utilizing them, as they do not always measure accurately. Palm vein identification is a workable biometrics technique that excels in terms of individuality, stability, and security, and HEI, particularly Mount Kenya University, could implement it. In our review, the basic concept of palm vein recognition was first introduced. The development of the ROI technique and picture collection technology was then monitored via tabulation. The palm prints and fingerprints were kept in a database after much trial and error. Our investigation's findings led us to explore palm vein imaging technology. In conclusion, biometric authentication is a technological achievement that has not yet won the confidence of the general public. It is overloaded with flaws despite the fact that it aids in addressing the numerous drawbacks connected to conventional authentication methods like passwords and PINs. The biometric identifiers cannot be altered after they have been compromised, they are expensive, inaccurate, and vulnerable to hacking, and they are prone to malfunction when the individual undergoes a physical change. To increase the effectiveness of the technology, these flaws must be fixed.

VII RECCOMENDATIONS

The researcher’s recommendations are that 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. Palm vein authentication will be able to provide better security. Staff members are the weakest link in the security chain, so the university should have rules in place to train them. The fusion of biometrics and the internet may result in a number of cyber-attacks. Through social engineering, an unanticipated insider threat could be attracted from the outside. All employees must be made aware of the cyber risks and instructed on how to avoid compromising the company's defenses.

Among other administrative controls, policies, directives, and regulations must be properly documented and followed. It is crucial to show that a system, network, and information are being used properly by the organization. Both the requirements for employees and the potential consequences of non-compliance should be made clear. This works well as a deterrent.

REFERENCES

[1] Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, *80*, 2642-2646.

[2] 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.

[3] 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.

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

[5] Parihar, R. S., & Jain, D. S. (2019). Palm vein recognition system for human authentication: A review. *International Journal for Research in Applied Science and Engineering Technology*, *7*(2), 472-477.

[6] 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.

[7] Phadke, S. (2013). The importance of a biometric authentication system. *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)*, *1*(4), 128-132.

[8] Wambui, B. M., Gikandi, J. W., & Wambugu, G. M. (2022). A Suvery of Biometric Authentication Technologies Towards Secure And Robust Systems: A Case Study of Mount Kenya University.

[9] Wambui, B. M., Gikandi, J. W., & Wambugu, G. M. (2022). A Framework for Verification in Contactless Secure Physical Access Control and Authentication Systems.

[10] Wambui, B. M., Nyambura, H., & Muriuki, N. (2022). An Analysis on the Effectiveness of ICT Integration In Learning in Higher Education Institutions in Covid-19 Era.

[11] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2018). A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, *78*, 242-251.

[12] Zang, W. L. (2014). Research of information security quantitative evaluation method. Applied Mechanics and Materials, 513, 369–372