Security and Privacy Determinants in Biometric Application in Cyber Security in Banks in Eldoret Town, Kenya

Misoi K. Thomas, James Ogalo, Ben Maake

Abstract: ***Biometric technology has been seen as a driving force for the future direction of strong authentication. Although Biometric has been deemed by many scholars as secure method of identification and verification, few banks in Kenya have implemented the use of biometric features such as fingerprints for customer and systems user identification. There are some that put in place the system but failed to fully utilize the system. What could be the key determinants to successful implementation or adoption of the biometric systems for identification and verification. What are the elements that makes it possible for a banking institution to effectively adopt and use the biometric systems for identification and verification. The study sought to determine the effect of security and privacy in biometric application for authorization and identification in cyber security in banks in Eldoret Town. The study was guided by the contingency theory, diffusion innovation theory, and unified theory of acceptance and use of technology. A descriptive survey design was used. The study comprised of 548 employees from 30 commercial banks in Eldoret Town. The study concludes that security and privacy influence biometric application in authorization and identification in cyber security in banks in Kenya. The study recommended that banks should provide convenient and more secured banking services to customers. Additionally, the study recommended a model for evaluation of biometric system before its implementation. The model will be used to ensure successful implementation and application of the system. The determinants are: security and privacy. Biometric technology in banks needs to integrate with the existing traditional security system which will help the banks the level of authorization and identification cyber security.***

Keywords: ***Biometric Systems, System Security, Data Privacy, Technology Adoption***

I. INTRODUCTION

Biometric use in many platforms for authentication and authorization of access and systems login has gathered momentum since late 20th century up to date. Since its introduction, biometric has seen tremendous growth in the enhancement of security and other mechanisms deployed to tackle the menace of cyber security and unauthorized access to vital information of an individual [1]. Thus, this study seeks to find out determinants of biometric application for authorization and identification on cyber security in banks. A 2003 survey by Richardson found that since 1997, the frequency of computer security incidents had grown rapidly, with around 90% of large firms reporting such occurrences every year [2]. Regarding security, biometrics is a term used to describe authentication methods that rely on the measurement of physical and behavioral characteristics [3].

Manuscript received on 16 June 2022 | Revised Manuscript received on 26 June 2023 | Manuscript Accepted on 15 July 2023 | Manuscript published on 30 July 2023.
*Correspondence Author(s)

Misoi K. Thomas*, Student (M.Sc Information Systems) Department of Computing Sciences, School of Information Science and Technology, Kisii University Kenya. E-mail: tmisoikip@gmail.com, ORCID ID: 0009-0004-3231-8221

Dr. James Ogalo, Lecturer, Department of Computing Sciences, School of Information Science and Technology, Kisii University, Kenya. E-mail: jogalo@gmail.com ORCID ID: 0000-0002-9275-4963

Dr. Ben Maake, Lecturer, Department of Computing Sciences, School of Information Science and Technology, Kisii University, Kenya. E-mail: benmaake@gmail.com, ORCID ID: 0000-0002-5148-8662

Biometric technology utilizes biological and behavioral characteristics to automatically identify individuals. This technology has been acknowledged as a tool for natural identity management that provides greater security and convenience when compared to traditional methods of personal identification [4].

A. The research question:

To examine how security and privacy determinants in biometric application for authorization and identification in cyber security in banks in Eldoret Town.

II. REVIEW OF RELATED LITERATURE

Fingerprint, iris, and voice-based biometric technologies are currently the most mature and widely adopted techniques in commercial settings. However, vein patterns have shown promise as they are more difficult to forge than external hand geometry. Despite this potential, there has been limited research published on vein pattern technology. Similarly, there is also a lack of sufficient research on retinal technology. As such, further research is necessary to fully understand and develop these biometric technologies for widespread adoption in commercial and security settings.

A. Fingerprint

Fingerprint recognition is a security measure that relies on the uniqueness of each individual's fingerprints. Its purpose is to verify the identity of a user and is achieved by identifying certain characteristics of the fingerprint such as ridge endings, arches, loops and whorls, which are then used to create a statistical template for comparison with future samples. To prevent fraudulent use, the technology does not store an actual physical image of the fingerprint. Various sensor technologies such as digital/optical, thermal, capacitance or ultrasonic are used to capture the print. One of the main advantages of fingerprint recognition is its widespread acceptance as a reliable and accurate security measure, which is also easy to use and install. However, there are some potential disadvantages associated with the technology, particularly when it comes to injury to the user's finger. If a finger is damaged or does not have a clear pattern, the algorithm's security may be compromised, which could impact the system's performance.

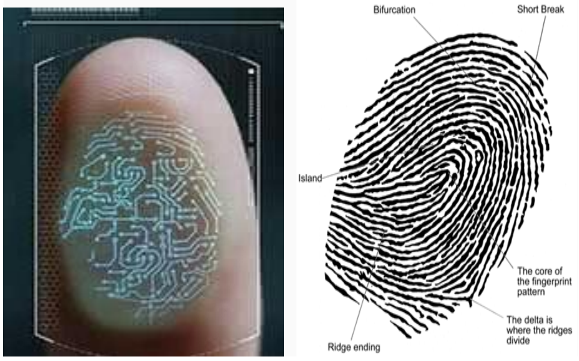
Bifurcation
Short Break
Island
The core of the fingerprint pattern
The delta is where the ridges divide
Ridge ending

Figure 1: Finger print scanning source [2]

B. Iris Recognition

Iris recognition is a method of verifying a person's identity by scanning the distinctive patterns present in the iris. To confirm the user's identity, a stereo camera is used to take a digital image of the iris, which is then compared to a template.

This technology offers several advantages, such as the fact that the iris does not change over a person's lifetime, making it a highly reliable biometric. Additionally, the iris is resistant to damage and has a high degree of randomness, making it an excellent choice for security measures. The technology also features liveliness testing through the changing pupil size and allows for contactless authentication, making it a hygienic option.

However, there are also several disadvantages to iris recognition. The nature of the iris inside the eye means that it can be obscured by eyelashes or reflections, which could affect the accuracy of the technology. The iris also deforms non-elastically with changes in pupil size and can move considerably, which could also impact its performance.

Figure 2: Iris Scanning

C. Voice Recognition

Voice recognition is a biometric technology that verifies a person's identity by analyzing their voice. The unique voiceprint is created by the influence of airways, soft tissue cavities, and the movement of the mouth and jaw on voice patterns. For speaker identification and authentication, there are several operational methods such as text-prompted response which is where the system requests the user to say a specific word or phrase. Whereas text dependent involves using a predetermined voice password that does not change, text independent involves allows the user to pronounce any passphrase.

One of the advantages of voice recognition is that it requires a lower model size since the password is not stored, making it easy to use as the user does not have to remember a password. Additionally, it is more cost-effective than other biometric systems as it does not require dedicated hardware and can be integrated into various devices such as automobiles and home appliances.

However, voice recognition can be negatively affected by poor quality hardware, such as a telephone, which can significantly decrease the performance of the system. Additionally, background noise can impact the quality of the sample and matching performance, making voice recognition less ideal for certain environments.

Figure 3: Voice input for biometric recognition source [2]

Security in biometric application for authorization and identification the biometric technology is a secure and convenient identification method and it does not need to remember complex passwords, nor smart cards, keys, and the like. Biometrics is the measurable characteristics of individuals based on their behavioral patterns or physiological features that can be used to verify or recognize their identity. Physical characteristics include fingerprints, palm or hand geometry, iris, retina, and facial characteristics. Behavioral characteristics include signature, keystroke and voice pattern. With the combination of biometric technology products and modern computer technology, it is easy to perform monitoring, management, systems integration, automated management, and security applications [5].

The major concern of privacy issues observed by researchers in organizations, people demand strong authentication and focus on suggesting biometrics because biometrics could provide advantages to recipients, staff and providers. The combination of smart card with biometrics could provide considerable advantages in sense of ease of use, speed of transaction, personal use without compromising privacy and security. There is a need of biometrics technology as the security cannot be assured with user ID and password in public places [5]. According to [5], there is a privacy concern using biometric system.

Many respondents have confidence on the privacy of their current healthcare information systems and on the other hand, half of the respondents have little doubt about the privacy of their current health information system [6]. [7] argue that at base, people distrust biometric authentication systems. Civil libertarians often oppose biometrics as being a potential tool for demographic profiling, intrusive, and a means of eroding patient privacy. Further biometrics are unlike conventional identifiers such as PINs or passwords because they are linked to a specific person and cannot be replaced, changed, or modified. It is anticipated that users will need help to understand and experience the biometric technology and overcome their concerns about security and privacy. They identified that biometric technology still seems to be too intrusive to many people.

[8] did a study on ease of use of Gaze-Based biometric authentication system in verification and intrusion detection. The study used census design. The findings of the study revealed that the ease of use and superior functionality of Gaze-Based biometric Authentication System has increased significantly as a result obits higher ability to protect users' confidential and private information. The results of the study showed that the use of gaze-based authentication system helps tackle with the challenges such as spoofing, video analysis and shoulder surfing attacks.

[9] did a study on the factors influencing adoption of electronic payments in banks in Mexico. The study objectives were to identify how cost, information security, technology infrastructure and top management affects adoption of electronic payments in banks in Mexico. A descriptive survey design was used while 112 IT staff of commercial banks were targeted. Census sampling technique was used to select 112 respondents. Questionnaire and interview schedule were used as data collection instruments. Both qualitative and quantitative analysis was used in analyzing of data with the help of descriptive statistics. The study found out that the major factor affecting adoption of electronic payments in commercial banks are information security. The results indicated that hardware malfunctioning, transaction errors, and information security affects adoption of electronic payments in banks in Mexico. The study recommended that the banks IT practitioners should monitor the quality of the systems in order to detect attacks, attempt attacks and check intrusion of customer information in the systems.

[10], investigated determinants of adoption of biometric application for authorization and identification among patients in public hospitals in Ghana. A descriptive survey design was used while 509 employees were targeted. Sample random sampling technique was used to select 213 respondents. Questionnaire and interview schedule were used as data collection instruments. Both descriptive and inferential statistics were used in analyzing, presentation and interpretation of data. [10] found out that system errors and specifically false rejection error was the main factor adversary affecting the performance of biometric system. As such the healthcare facilities may wish to deployment of a multi-biometrics solution. This will ensure that the patients are not denied services due to inadequacies of the unidiomatic system.

Privacy in biometric application for authorization and identification

[11] did a study on the factors influencing adoption of mobile banking in banks in Uganda. The main study objective was to determine factors influencing adoption of mobile banking in banks in Uganda. A descriptive survey design was used while 189 IT staff of banks were targeted. Census sampling technique was used to select 189 respondents. Questionnaire and interview schedule were used as data collection instruments. Both qualitative and quantitative analysis was used in analyzing of data with the help of descriptive statistics. The results indicated that security of information and transactions ranks high among the factors that banks in Uganda grapple in adoption of mobile banking. The study recommended that the banks in Uganda need to evaluate and assess before implement mobile banking system in order to reduce occurrence of transaction issues and fraudness.

[12] assessed on the factors contributing to occurrence of cybercrime on E-banking in commercial banks in Nairobi Kenya. A case study design was used while 41 ICT experts were targeted from 14 commercial banks. Census sampling technique was used to select 41 respondents. Questionnaire was used as data collection instruments. Quantitative analysis was used in analyzing of data with the help of descriptive statistics where data was presented in form of pie-charts, percentages, figures, tables and bar graphs. The study found out that in order to protect cybercrime in commercial banks the ICT experts had network security policies in place; the banks serviced their disaster recovery site and banks used an antivirus in protecting their systems. The study recommended that the commercial banks ICT management should enhance their security by implementing timed access control mechanisms.

[11] proposed that many biometric technologies are capable of operating as stand-alone systems, in reality their accuracy and performance levels would be greatly improved by combining them with more conventional authentication methods such as passwords and keys. [5] asserted that passwords need to be renewed within a certain period of time to maintain a high level of security. Moreover, it might be copied and used by unauthorized users. To fix that problem, biometrics security system can be applied. The most use of biometrics security system in network is the logical access control method. It will verify person's identification for secure workstation logon or network logon to get access control to the system.

III. METHODOLOGY

If you This study adopted descriptive survey research design where the study was carried out in commercial banks in Kenya. [13] asserted that descriptive survey design is adopted in studies whose objective is to determine and describe different variables in a situation. This is where there were attempts to describe, explain and interpret conditions of the current biometric application for authorization and identification in cyber security in banks in Kenya

From secondary data available in the Central Bank of Kenya Bank Supervision Department Annual Report (2017), there are 30 commercial banks in Eldoret town. The target population included bank managers, head of departments, tellers, personal bankers, credit officers and customer care employees. The study comprised of 528 employees.

Simple random sampling technique was used to select the 272 respondents. In simple random sampling technique, each member of the population has an equal chance of being selected as a sample for use in the study. The entire process of sampling is done in a single step with each subject selected alongside the other members of the population.

The sample of this research was calculated using Nassiuma's (2000) method as shown below.

$$\frac{NC^2}{C^2+(N-1)e^2}$$

Where

n = Sample size

N = population size

C = Coefficient of variation (30%)

e = Error rate (0.03)

The formula was used to select 22 bank managers, 59 heads of departments, 53 tellers, 35 personal bankers, 57 credit officers and 46 customer care employees. The sample size was 272 respondents.

Table 1: Sample Size

Respondents	Target population	Sample size
Bank managers	28	22
Heads of department	140	59
Teller	110	53
Personal bankers	56	35
Credit officers	130	57
Customer care employees	84	46
Total	548	272

Source: (Researcher, 2019).

IV. RESULTS

Be The study sought to determine the effect of security and privacy in biometric application for authorization and identification in cyber security in banks in Eldoret Town.

Table 2: Effect of security and privacy in biometric application for authorization and identification in cyber security in banks

Statements		1	2	3	4	5	Total	Mean	Std
Poor biometric applications hardware is inefficient enhancing insecurity issues	Freq	79	79	40	15	8	221	2.07	1.07
	%	35.7	35.7	18.1	6.8	3.6	100	41.4	
Proper biometric application hardware and software installed enhance securing of banks information	Freq	30	27	44	89	31	221	3.29	1.25
	%	13.6	12.2	19.9	40.3	14	100	65.8	
Biometric applications offers correct information	Freq	36	11	36	89	49	221	3.47	1.33
	%	16.3	5	16.3	40.3	22.2	100	69.4	
Biometric applications software installed reduces banking errors by employees	Freq	36	13	32	78	62	221	3.53	1.38
	%	16.3	5.9	14.5	35.3	28.1	100	70.6	
Biometrics application maintains data integrity	Freq	28	10	36	85	62	221	3.65	1.28
	%	12.7	4.5	16.3	38.5	28.1	100	73	
Biometrics application maintains data confidentiality	Freq	25	4	20	75	97	221	3.97	1.28
	%	11.3	1.8	9	33.9	43.9	100	79.4	

The results indicate that 35.7% of the participants strongly disagreed, 35.7% disagreed, 18.1% were neutral, 6.8% agreed and 3.6% strongly agreed that poor biometric applications hardware install in banks is inefficient where they are not secure enhancing insecurity issues such as fraud, cybercrime among others (mean= 2.07 and Std=1.07). The data had low standard deviation indicating that the data points tend to very close to the mean hence indicating the data was normally distributed.

The findings indicate that 13.6% of respondents strongly disagreed, 12.2% disagreed, 19.9% were neutral, 40.3% agreed and 14% strongly agreed that proper biometric application hardware and software installed enhance securing of banks information reducing fraud by tellers, cybercrime among others (mean= 3.29 and Std=1.25). The data had slightly low standard deviation indicating that the data points tend to very close to the mean hence indicating the data was normally distributed.

According to table 4.6, 16.3% of participants strongly disagreed, 5% disagreed, 16.3% were neutral, 40.3% agreed and 22.2% strongly agreed that biometric applications offers correct information when customers use since there is no access of customer information by the tellers or bank management (mean= 3.47 and Std=1.33). The data had high standard deviation indicating that the data points are spread out over large range of values hence indicating the data was normally distributed due to the mean was above 2.5.

From the results 16.3% of participants strongly disagreed, 5.9% disagreed, 14.5% were neutral, 35.3% agreed and 28.1% strongly agreed that biometric applications software installed reduces banking errors by employees such as fraud by bank tellers hence increasing effectiveness and efficiency of bank operations (mean= 3.53 and Std=1.38).

The data had high standard deviation indicating that the data points are spread out over large range of values hence indicating the data was normally distributed due to the mean was above 2.5.

The findings indicate 12.7% of the respondents strongly disagreed, 4.5% disagreed 16.3% were neutral, 38.5% agreed and 28.1% strongly agreed that biometrics application maintains data integrity hence making employees cannot access the bank records easily since it is secured (mean= 3.65 and Std=1.28). The data had slightly low standard deviation indicating that the data points tend to very close to the mean hence indicating the data was normally distributed.

Moreover table 4.6 indicates 11.3% of the participants strongly disagreed, 1.8% disagreed, 9% were neutral, 33.9% agreed and 43.9% strongly agreed that biometrics application maintains data confidentiality in terms of the customers and banks records where it needs access of the customer or the bank management (mean= 3.97 and Std=1.28). The data had slightly low standard deviation indicating that the data points tend to very close to the mean hence indicating the data was normally distributed.

From the results majority of respondents with 79.4% (mean=3.97) were of the opinion that biometrics application maintains data confidentiality in terms of the customers and banks records where it needs access of the customer or the bank management.

The study is concurred by [9] who indicated that hardware malfunctioning, transaction errors, and information security affects adoption of electronic payments in banks in Mexico. Also [10] supported the findings where they found out that system errors and specifically false rejection error was the main factor adversary affecting the performance of biometric system.

V. RESULT AND DISCUSSION

The From the findings majority of the participants were of the opinion that effect of security and privacy in biometric application for authorization and identification in cyber security in banks included: poor biometric applications hardware installed in banks, where they are not secure enhancing insecurity issues such as fraud, cyber security among others; proper biometric application hardware and software installed enhance securing of banks information reducing fraud by tellers, cyber security among others; biometric applications offers correct information when customers use since there is no access of customer information by the tellers or bank management; biometric applications software installed reduces banking errors by employees such as fraud by bank tellers hence increasing effectiveness and efficiency of bank operations; biometrics application maintains data integrity hence making employees cannot access the bank records easily since it is secured; and biometrics application maintains data confidentiality in terms of the customers and banks records where it needs access of the customer or the bank management.

VI. RECOMMENDATION

The management needs to offer training programs to both the staff and customers on how to use the biometric technology hence increasing effectiveness of firm operations. The IT department before installing the biometric technology needs to assess if the biometric system is compatible with other systems used in the banks in order to reduce breakdown of operations in organization.

The IT department of the commercial banks need to use proper system tools used to in the implementation of biometric technology in the bank operations. The management needs to make sure the biometric technology used by the customers is secure and confidential.

contents of the journal are peer-reviewed and archival. The journal publishes scholarly articles of archival value as well as tutorial expositions and critical reviews of classical subjects and topics of current interest.

VII. CONCLUSION

The study concludes that security and privacy influence biometric application in authorization and identification in cyber security in banks in Kenya. The study recommended that banks should provide convenient and more secured banking services to customers. Additionally, the study recommended a model for evaluation of biometric system before its implementation. The model will be used to ensure successful implementation and application of the system.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Glaser, A. (2016). Biometrics are Coming Along Serious Security Concerns. International Journal for Sucurity, 3(1), 21-34.
2. Richardson, A. (2013). Biometric Application and its Influence in the Organization Performance. International Journal on Information Security.
3. Spolaor, R., Li, Q., Monaro, M., Conti, M., Gamberini, L., & Sartori, G. (2016). Biometric Authentication Methods on Smartphones: A Survey. PsychNology Journal, 14(2).
4. Wayman, J. L. (2016). Biometrics in Identity Management Systems. IEEE Security and Privacy Magazine, 6(2), 30-37. [CrossRef]
5. Iqbal, I., & Qadir, B. (2012). Biometric technology - Attitudes & influencing factors when trying to adopt this technology in Blekinge healthcare. Karlskrona: Blekinge Institute of Technology.
6. Vijayan, J. (2014). Corporate America Slow to Adopt Biometric Technologies. 38(32), 1-2.
7. Chandra, A., & Calderon, T. (2015). Challenges and constraints to the diffusion of biometrics in information systems. Commun. ACM, 48(12), 101-106. [CrossRef]
8. Malla, A. H. (2018). A Gaze-Based Authentication System: From Authentication to Intrusion Detection. Thesis, Texas A&M University
9. Collins, D. (2016) Factors influencing adoption of electronic payments in banks in Mexico. International Journal in Information Technology, Volume 5: Pages 34-89.

10. Adebayo, T. & Olukenya, O. (2015) Determinants of adoption of biometric application for authorization and identification among patients in public hospitals in Ghana. International Journal of Computer Science and Information Security, 31(2), 56-71.
11. Amutebo, R. (2016) Factors influencing adoption of mobile banking in banks in Uganda. African Journal of Information and Communication Technology Research, 53(4), 121-142.
12. Mwai, N. M. (2015) Factors contributing to occurrence of cybercrime on E-banking in commercial banks in Nairobi Kenya. Unpublished Project, United States International University (USIU).
13. McNabb, D. E. (2015). Research methods for political science: Quantitative and qualitative methods. Routledge.

AUTHORS PROFILE

Misoi K. Thomas (MSC information systems) Department of Computing Sciences School of Information Science and Technology Kisii University. Thomas Misoi is a driven and ambitious student pursuing a Master of Science in Information Systems. With a strong passion for technology and its application in real-world scenarios, Thomas is focused on exploring the potential of biometric systems, data management, and IT systems implementation. Currently, he holds a position as the Manager of IT at AMPATH Kenya. In this role, he is responsible for overseeing the organization's IT infrastructure, managing technology projects, and ensuring the smooth operation of information systems. Thomas's dedication to his work and his commitment to leveraging technology for positive change make him a valuable asset to his organization.

Dr. James Ogalo (PhD) Lecturer Department of Computing Sciences School of Information Science and Technology Kisii University Doctor of Philosophy - Information Technology Management. Throughout his career, Dr. Ogalo has demonstrated a keen interest in exploring the potential of Information Systems to revolutionize healthcare delivery and enhance security in digital environments. His research focuses on leveraging cutting-edge technologies, such as blockchain, to design and implement secure and efficient health information systems. By integrating these systems, Dr. Ogalo aims to optimize the flow of information within healthcare organizations, ultimately improving patient outcomes and driving operational excellence.

Dr. Ben Maake, (PhD). Lecturer, Department of Computing Sciences, School of Information Science and Technology, Kisii University. Experienced Lecturer with a demonstrated history of working in the higher education industry. Skilled in Negotiation, Machine Learning, Artificial Intelligence, Programming, and English. Strong education professional who is a candidate student - Doctor of Computing - Computer Systems Engineering focused in Recommender Systems research at the Tshwane University of Technology, South Africa.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Retrieval Number: 100.1/ijitee.H96570712823
DOI: 10.35940/ijitee.H9657.0712823
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)