Facial Authentication as A Bank Security Measure in Zimbabwe

Margaret Mashizha*
Department of Finance and Accounting, University of Zimbabwe,
margretmashizha@gmail.com

Englon Kavhuru
Department of Finance and Accounting, University of Zimbabwe
ekavhuru96@gmail.com

Abstract
This paper reports on the findings of a research that was conducted in an endeavour to improve security within the banking sector. The research was triggered by an increase in the number of cyber-attacks on personal bank accounts resulting in the loss of huge sums of money and hence eroding bank confidence among customers. The main objectives of the study were to determine whether customers were aware of facial authentication as a bank security and to assess whether customers would accept facial authentication as a bank security measure. Further, the study was carried out to establish whether it was feasible for banks to implement such a biometric system as part of enhancing bank security and determine the extent to which customers are prone to cyber-attacks. Finally, the research aimed to outline the probable challenges that may be encountered in implementing facial authentication in the banking system. A survey of 70 bank employees and 200 bank customers were selected from two commercial banks using a purposive sampling method. Data was collected using interviews, questionnaires, and an experiment conducted to establish the vulnerability of customers to cyber-attacks. Findings revealed that customers and employees were aware of facial authentication as a measure of bank security and it was a preferred method for bank security in this digital transformation age. Customers were highly prone to attacks as they just clicked links to websites without a second thought. The technology was recommended for the possibility of improving bank security and hence boosting customer confidence and enhancing the security of customer data. However, whilst it was feasible for banks to implement the technology as they have adequate finances, likely challenges to be encountered included a lack of expertise to set up the system and a lack of knowledge on its use amongst customers. The study recommended banks consider facial authentication due to its advantages over other non-biometric methods. The technology is safer especially as it reduces human contact and does not depend on the need for customers to memorise passwords or codes nor does it require them to possess something like smart cards.

Keywords
facial authentication; password; bank security; personal identification number; customer confidence

Introduction

The global pandemic COVID-19 has brought some changes in the banking sector notably an increase in doing business online thus leading to a corresponding embracement of e-banking (World Bank, 2017). However, the security of bank clients' accounts has become a challenge since almost every country both in developed and developing countries is facing a surge in cyber-attacks which have led to a global loss of about $100 billion annually in financial institutions (Oliviera et al., 2020). This has been attributed to the fact that most Financial Institutions are still using a legacy digital system for which their defense parameters are now defenseless in the face of an attack (Marinela, 2010).

*) Corresponding Author

Conducting business transactions by unauthorised persons results in significant financial losses, and a corresponding increase in reputational risk and breach of bank secrecy (Oliviera et al. 2020; Srinivasan & Chowdhury, 2015) thus ensuring the security of transactions has become one of the major challenges that banking systems deal with (Oliviera et al., 2020).

Regionally, African banks cannot be spared from cybersecurity risks on their digital platforms. Banks have been attacked and significant losses have been encountered. In South Africa, an approximated loss of ZAR50 billion in 2014 was realised as a result of cyber incidents in banks and about 500 million online user records were accessed illegally by cyber-criminals in 2015 (Desai, 2018). Nigerian Banks have lost about NGN159 Billion in the period 2000 to 2013 to cyber-attacks (Stephen et al., 2017) and also in Ghana banks have reported around 400 000 cases of cyber-attacks (Kshetri, 2019). Zimbabwe has not been spared from these cyber-attacks as well.

Historically in Zimbabwe, all banks irrespective of the market served, have adopted digital systems that support e-banking. There has been a notable adoption of mobile banking and this has paved the way for increased hacking of personal accounts. As such there is also a growing need to secure customer data as the country is experiencing a surge in financial fraud-related cyber-attacks. According to Fosse et al. (2017), financial institutions must have robust security measures to authenticate their customers. An effective authentication system will protect customer data, prevent money laundering and terrorist financing, reduce fraud, inhibit identity theft and promote the legal and enforceability of the agreements on electronic transactions (Federal Financial Institutions Examination Council, 2005). In Zimbabwe, there is a case where fraudsters used Africom line to make calls to Econet Zimbabwe Agent lines requesting PIN and merchant identification numbers and they pretended as if they were calling from the Econet IT Department (Rupapa, 2021; Muhamba, 2021). Apart from that, they also hijacked Econet phone numbers and resultantly their WhatsApp accounts and then went to WhatsApp group chats where they offer forex deals at abnormally high rates. The criminals managed to steal up to about USD100 million (Rupapa, 2021; Muhamba, 2021). This shows the existence of phishing and vishing hacking in Zimbabwe which is a special type of hacking that is associated with username and pin-based authentication.

Several researches established that the adoption of digital banking has been hampered by security concerns, yet in light of the pandemic virtual banking has taken over and should be embraced fully. Based on the existing empirical evidence on losses related to cyber activities, the need for robust security systems has gained attention from every industry (Meval & Kumbharana, 2014). The common method of authentication is the username and password (Barkadehi et al., 2018, Bani-hani et al., 2019). Nevertheless, the usage of single-factor authentication is considered poor in securing digital systems as it has proved to be inefficient (Bani-hani et al., 2019, Barkadehi et al., 2018; Majdalweich et al., 2022). The basic username and pin/password have presented a lot of security loopholes (Bani-hani et al., 2019, Barkadehi et al., 2018; Ometov et al., 2018) probing computer scientists and software engineers to start coming up with new interesting verification methods such as facial authentication, virtual keyboards, partial password, secrete image, smart card, USB token, OTP (One-Time Password) secrete questions and bookmark authentication among many others (Bani-hani et al., 2019)). Recently, OTP authentication has gained popularity as it seems to be more secure than a one-factor password (Han et al., 2016; Huang et al., 2014). The OTP lifetime is usually 60 seconds but this poses a challenge to the old age bank user as their typing speed is very slow and this has forced banks to increase their OTP lifetime but this has a detrimental effect as it increases the chances of hacking. Citibank in South Korea has encountered hacking as a result of increasing its OTP life span from 60 seconds to 3 minutes for the convenience sack of its users (Han et al., 2016). Although it has been proven to be more secure than a one-factor password and username authentication, there still exist security vulnerabilities, especially where the timeframe for the OTP is protracted.

Owing to vulnerabilities associated with authentication by what the user knows, facial authentication has gained the interest of researchers in the field of security as it has lower intrusiveness and higher accuracy than other methods (Shang-Hung, 2000; Oliviera et al., 2020; Zulfigar et al., 2019). While other authentication systems have been used such as Optical fingerprinting, hand geometry, retinal identification, voice, and signature recognition to name but a few, these have

been associated with several flaws rendering them ineffective (Gates, 2011). The use of the eyes, both the iris and the retina was considered intrusive and uncomfortable by users, voice recognition was also associated with challenges as voice can differ depending upon the device used to record the voice tone, tempo, and stress used by the voice could also vary (Gates, 2011, Galterio et al., 2018). The use of biometric authentication has attracted huge investments in the financial sector due to their notable enhancement of security through increased convenience and acceptability by clients (Oliviera et al., 2020; Galterio et al., 2018).

The general aim of the study was to evaluate the possibility of introducing facial authentication to enhance security within the banking sector. Having noted that various flaws associated with the ownership-based models such as smart cards and physical keys and the knowledge-based models such as passwords, pin codes and lock patterns, the research seeks to assess one of the inherent based methods i.e. the face as a measure to ensure safe and secure banking experience. The research aimed to (1) assess preferences of facial authentication among bank customers and employees (2) assess the feasibility of introducing facial authentication in banks, (3) evaluate the acceptance of facial authentication by systems users (Bank account owners) and (4) to outline the challenges that may be encountered in introducing the system. The study adds to the existing body of literature by providing an assessment of the use of facial authentication as a means to enhance bank security systems and boost customer confidence. Additionally, the study makes use of a survey method that incorporates customer opinions in the study and is in line with the technology adoption model by Davies (1995).

The rest of the section is arranged as follows: The introduction provides a background of the study outlining the security measures employed in the banking sector and the challenges experienced. This is followed by the literature review which seeks to assess what is known in the subject area and hence help to identify the research gap. The methodology section outlines the methodologies used to conduct the study and the results and findings section outlines what was established in the research. The paper concluded with a summary and recommendations for further research.

Literature Review

Because of COVID-19, the usage of electronic banking has noticeably increased as it reduced human physical contact (Ndubueze, 2020; Maphosa, 2023) hence forcing the banks to upgrade and even develop new online banking systems within a very short period to remain competitive. In the banking digital platforms usage, the number of cyber-attacks has also increased exponentially both globally and locally thus putting pressure on banks on how to protect their clients and businesses against the threat (Sviantun et al., 2021). The epic researches on the use of passwords show that 86% of online system users use weak passwords which might be a dictionary word, lowercase password, digits only, or their names, consequently, the passwords can be easily attacked by brute force attack (Majdalweich et al., 2022; Bani-Hani et al., 2019). The above weakness of passwords has led to the development of more robust authentication methods that are deemed to be more secure and these are facial authentication, smart card, security questions, One-Time-Password (OTP), and secrete images among many others (Bani-Hani et al., 2019). Facial authentication is associated with quick access without the need to remember anything like a password or a username to complete the process (Oliviera et al., 2020; Chowdhury et al., 2017; Mardikar, 2017). However, the use of facial authentication has not been embraced especially in Zimbabwean banking systems. Due to this, the researcher has been prompted to carry out a study to evaluate the effectiveness of the emerging new authentication system, facial authentication compared to the most familiarly used username and password authentication method.

Literature identifies several methods that can be used to classify authentication methods in banking systems which are first, what the user knows namely the knowledge-based model such as the password, pin code, lock pattern, graphical password, rhyme-based and challenge-response, Secondly what the user has namely the ownership-based model such as physical keys, smart cards, cell phones, hardware tokens and thirdly what the user is known as the inherently based model such as fingerprints, palm, iris, voices, gestures, and face and lastly what the system can generate such as one time passwords, cryptographic credentials (Barkadehi et al., 2018, Majdalweich et al., 2022). Authentication using a username or password (something that one knows) is a single-factor authentication or multifactor authentication whilst

combining what the user knows with what the user possesses is a two-factor authentication. It has been noted that two-factor authentication and multifactor authentication provide a stronger security system as compared to the use of one-factor authentication (Barkadehi et al., 2018; Majdalwiech et al., 2022)

Theoretically, the study is informed by the technological acceptance model proposed by Davis (1995). Davis (1995) refined his conceptual model to propose the Technology Acceptance Model, as shown in Figure 1, by drawing on prior work by Fishbein & Ajzen (1975), who developed the theory of Reasoned Action and other related research studies.

Davis (1985) proposed that user motivation can be explained by three factors: perceived ease of use, perceived usefulness, and attitude toward using the determinant of whether the user will use or reject the system. The user's attitudes were thought to be influenced by two major beliefs: perceived usefulness and perceived ease of use, with perceived ease of use having a direct influence on perceived usefulness. Finally, both of these beliefs were hypothesized to be directly influenced by the system design characteristics represented by X1, X2, and X3 in Figure 1 above.

Lately, Username and PIN/password Authentication were commonly used as bank security systems (Majdalweich et al., 2022). This is a validation of users according to what the user knows, that is the username which is the user's unique identifier on the system and the password which is a secret string of characters and symbols (Bani-hani et al., 2019). The strength of each password depends on the length and blending of characters' upper- and lower-case letters, numbers, and symbols (Bani-hani et al., 2019; Maddox & Moschetto, 2019). While passwords and usernames can be easily memorised and are used at zero cost (Barkadehi et al., 2018; Shen et al., 2016) they have many vulnerabilities. Passwords are weak and insufficient as they can be easily guessed and are also used across many websites in addition, they are prone to shoulder surfing and retry attacks (Alabdan, 2020; Majdalweich et al., 2022). Phishing, vishing and smashing are also commonly used to attack systems secured by this method (Alabdan, 2020). These vulnerabilities have paved the way for facial authentication to be used to enhance bank security systems and counter the weaknesses of passwords and personal identification numbers.

Facial authentication is increasingly gaining popularity as the face is an important means of identifying and authenticating a person (Zulfigar et al., 2019). Facial recognition systems are trending globally as they provide the most secure and reliable security system. It is considered the fastest biometric technology that identifies a person without their interaction (Zulfigar et al., 2019). This biometric authentication system has been widely adopted as it can be used in multifaceted areas such as in government institutions to locate criminals and extremists (Galterio et al., 2018).

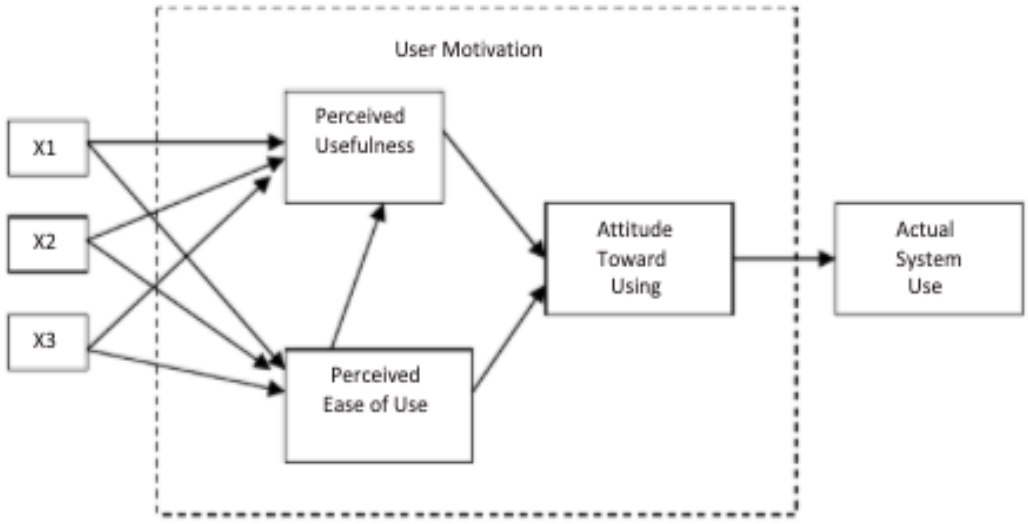

Figure 1: Original TAM proposed by Fred Davis
Source: Davis, 1985 p. 24

Facial authentication is also used in commercial sectors such as supermarkets where they can use the face to identify shoppers and study the behaviour of their customers to note impulse buyers, regular shoppers and even spot shoplifters (Galterio et al., 2018). Within the security sector, facial authentication has been extensively used in institutions, ports of entry, and border checkpoints. At border checkpoints facial authentication has been fast and reliable for verification, helping to reduce biases, misjudgments and unlawful proliferation among many other benefits. Facial authentication plays a significant role in crime prevention in offices, colleges, and universities and even in residential buildings and corporate organisations (Zulfigar et al., 2019). In schools and universities, the technology has been used to manage attendance accurately, (Zulfigar et al., 2019, Oliviera et al., 2020). In large gatherings such as Conferences and public events facial authentication has been used to deal with a large number of people in short durations at entry and exit points (Zulfigar et al., 2019). Any individual breaching the entrance rule can be easily spotted and an alert triggered (Oliviera et al., 2020). In like manner, the banking sector has also made use of the technology. ATMs, banking applications, computer and network security, and email logins are also areas in which facial authentication has been extensively and reliably used (Galterio et al., 2018). However, the use of this method seems to be of limited use within the Zimbabwean banking sector, with only manual facial verifications from photographs submitted upon opening the account instead of a facial scan each time one needs to access banking services.

Whilst facial authentication has gained popularity in many areas, it is not without its flaws. Zulfigar et al. (2019) noted that adopting this technology requires huge storage space and big data analysis hence increasing the required investment. Additionally, they note that facial images are not consistent as variations are noted in daily life, yet traditional methods will need consistency for comparisons with data sets in the system. Zulfigar et al. (2019) noted that traditional methods require input images to have facial features that can be compared to those available in the system which is not always the case. They also noted that as the data set increases the accuracy decreases if proper measures are not put in place. This then calls for measures to reduce the repercussions of facial authentication to be put in place requiring heavy financial investments.

Historically, In the UK, Hong Kong and Shanghai Banking Corporation Limited (HBSC) was the first bank to implement facial recognition. Their Mobile Banking app is equipped with facial authentication as one of its major security schemes in its multi-factor authentication mechanism. The app is used to acquire a 6-digit PIN from the bank securely by using facial recognition or figure print and this ensures it is only the bank account holder who has access to the account. In the United States of America, a multinational investment bank JPMorgan & Chase has installed facial recognition in all ATMs across the world (Hollinger, 2020) which allows consumers to get their funds and even deposit them using just a face scan (Hollinger, 2020).

Facial recognition, which is the pillar of facial authentication, is the most successful application in the area of image processing (Al-Allaf, 2014, Oliviera et al., 2020). The availability of modern mobile technology has paved the way for advancement in security (Albalooshi et al., 2018) and according to Albalooshi et al. (2018) and Zulfigar et al. (2019) facial authentication is believed to bring more secure banking systems. The use of facial authentication utilises neural networks and the procedure is believed to increase mobile banking which is one of the effective tools to enhance financial inclusion in many economies (Albalooshi et al., 2018; Oliviera et al., 2020, Zulfigar et al., 2019). The risk of banking fraud is believed to be reduced by using the Deep Belief Network when implementing facial authentication (Hinton et al., 2006) hence the need to adopt the technology in many banking systems.

Various researchers have worked around the area of authentication schemes. Bani-hani et al. (2019) conducted research in the United Arab Emirates (UAE) and sought to find the most commonly used authentication methods in UAE banks. A sample of six banks was taken for UAE and a comparison matrix was used to rank the methods that were being used to ensure security and enhance confidence in the banking sector. The researcher only considered virtual keyboard, partial password, secret image, smart card, USB token, OTP (One-Time Password) manual, OTP automatic, OTP synchronous, secrete questions and bookmark authentication and provided a ranking of these methods. The matrix used the factors of additional hardware, additional software, complexity, scalability, portability, and system requirements. The findings of the research revealed that banks

employ a variety of measures to enhance security and strengthen online authentication systems. It was also established that employing only one method resulted in a weak security system which has to be replaced by more robust security, to make it difficult for attackers. The main limitation of the research was that it did not cover all authentication methods especially where banking services are obtained via the use of mobile phones. Additionally, the study excluded the use of facial authentication which then is the focus of the current study.

Majdalweich et al. (2022) studied commonly used authentication methods using a comparison matrix with 11 characteristics. Data was collected from 25 respondents in 16 international banks in different countries including China and the USA. The research established common authentication methods to be security questions, smart cards, personal identification numbers and virtual keyboards. The researchers cite the limitations of the study to be the use of observation methods to collect data and thus recommend the use of surveys to gather customer opinions. They also noted the need to evaluate authentication methods using another matrix namely user acceptance. Additionally, the limitation of the study was the exclusion of other methods especially those that can be used on a mobile device. The current study focuses on facial authentication which was not part of this study and also makes use of questionnaires to gather customer opinions and capture data to address user acceptance.

Szczodrak & Czyzewski (2017) carried out research on face detection algorithms evaluation for verifying the identity of bank clients. The main goal of the research was to test the face detection method's practical usability in a biometric bank user verification system. The researchers used videos that were taken from three bank branches captured from four different types of operating rooms and thereafter, an analysis of the facial recognition algorithm was then done. They discovered that for system optimum operation, additional illumination should be provided. They concluded that the detection precision is sufficient to make a critical component of the system for visual bank customer verification. However, the analysis did not consider the level of acceptance by users, a gap to be filled by the current research.

In Zimbabwe, Zimucha et al. (2012) have done research that evaluates the effectiveness of e-banking security strategies in Zimbabwe Commercial Banks. The study focused on the risks of bank accounts being tampered with through phishing or identity theft. Fifteen commercial banks in Zimbabwe were considered for the research. The aims of the research were: to examine the security methods employed by Zimbabwean commercial banks, to see how different integrated security banking systems affect security strategies, to create a standard metric for measuring the effectiveness of e-banking security strategies, to assess the efficacy of various e-banking security strategies in Zimbabwe and to recommend solutions to improve the evaluated e-banking security strategies. The researchers established that banks were using four to five security strategies which included passwords, virtual keyboards, pins, access codes firewalls and secure socket layers. The study recommended further research that captures the customer perspective concerning bank security. This research gap is being addressed in the current research.

This research sought to determine the level of awareness and preference for facial authentication as a bank security measure among customers. Further, the research sought to assess whether customers would accept facial authentication as a bank security measure and whether it was feasible for banks to implement such systems. Finally, the research aimed to outline the probable challenges that may be encountered in implementing facial authentication in the banking system. The study is of importance in light of the increasing use of the Internet and let alone the need to enhance digital banking in light of the objectives of the Zimbabwe National Financial Inclusion Strategy 11 which seeks to enhance an inclusive financial sector and promote financial innovation and the adoption of more digital financial services. The study will also address the Sustainable Development Goals where the creation of an inclusive financial sector will help promote sustainable livelihoods, create wealth and employment, and facilitate gender equality in line with Vision 2030 of an Upper Middle Income Economy. Further, the study will add to the dearth of literature in the area.

Methodology

A mixed-method research approach was adopted and due to the emergence of the COVID-19 epidemic, data was collected via Google Forms, with online interviews replacing in-person interviews and these were conducted via telephone

calls. Participants of the study included bank employees from selected departments (Cybersecurity, E-banking and Card Services) and customers from two of the 19 banking Institutions in Zimbabwe. Purposive sampling techniques were used to select 70 bank employees and 100 bank customers with an equal distribution between the two selected banks. These include System Developers(IT department) who provide sufficient information on what needs to be done, the resources needed and recommendations when facial authentication is to be implemented, IT technicians(IT department): who provide information related to the computing servers for which the authentication applications needs, the forecasted expense if facial authentication is to be implemented, and their recommendations on the future of e-banking security: Cyber analyst (IT department): provide information on system security, Project manager (Finance department): provide information on project feasibility when banks decide to go for facial authentication. An experimental approach was also conducted to test the probability of customers being prone to social engineering attacks. Semi-structured interviews were performed to gather information from key informants. An email with a link that redirects someone was mailed to 50 bank customers to check on how many would be enticed to click attachments and open links. Interviews were conducted with ten employees selected from the IT and Finance departments. Under the IT department, interviews were done with two IT department managers, two System developers, two IT technicians, and two Cyber analysts and under the Finance department, two Managers were interviewed. The Statistical Package for Social Scientists (SPSS) Version 20.0 was used to analyse quantitative data, while thematic narrative analysis was used to analyse qualitative data from interviews and open-ended questions.

Data Analysis

The researcher distributed 70 questionnaires to bank employees and 100 questionnaires to bank clients and a response rate of 86% was achieved from bank employees and a response rate of 85% from the bank customers. From the interviews, a response rate of 80% was achieved. The response rate was considered sufficient for data analysis (Rubin, 2009). For the experiment, of the ten emails that had been sent with a redirect link, six respondents (60%) clicked the link. Figure 2 shows the age distribution of respondents.

Out of 60 employees who responded, 17% were below the age of 25 years, 43% were aged between 25-35 years, 32% were aged between 36 and 45 years and 8% were above the age of 46. This shows that most of the respondents were in the youthful age group. Among the customers who were part of the study, 29% were aged below 25 years, 41% were between 26 and 35 years of age, 18% were aged 36 to 45 years and 12% were aged 46 years and above. The age distribution shows that most of the respondents were youthful, which is the targeted group in the Zimbabwe Financial Inclusion strategy framework.

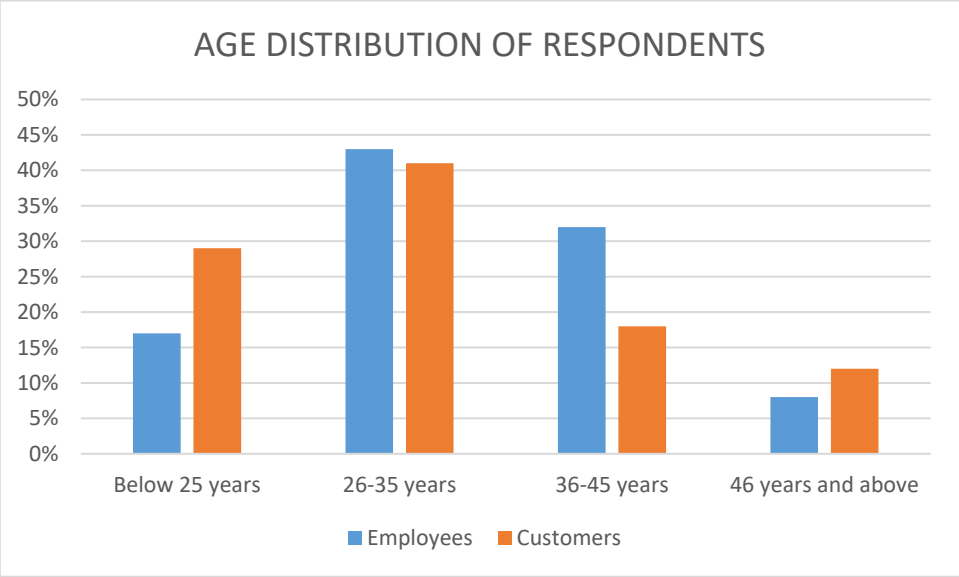

Figure 2. Age distribution of respondents
Source: Analysis of Primary Data

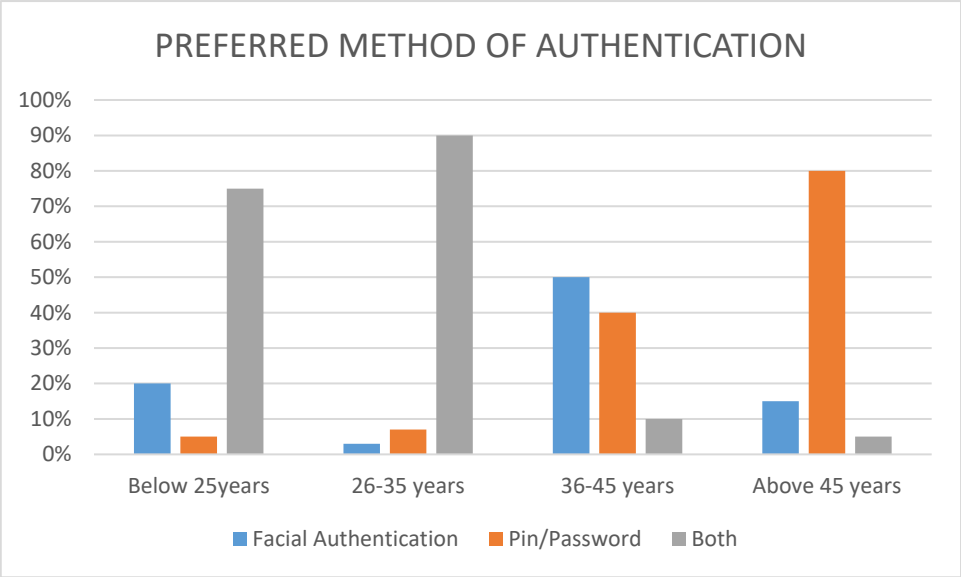

Figure 3. Preferred Method of Authentication
Source: Analysis of Primary Data

One of the objectives of the study was to assess awareness and preference for facial authentication as a bank security measure among bank customers and employees. Respondents were asked whether they had knowledge of facial authentication and to indicate whether they preferred facial authentication as opposed to the use of passwords when conducting bank transactions. Results from the study are presented in Figure 3.

For the age group below 25 years, 20% preferred to use facial authentication only, 5% preferred the use of pins and passwords and 75% wanted the use of both facial authentication and passwords and pins. In the 26 to 35 years category, 3% preferred the use of facial authentication, 7% indicated pins and passwords whilst 90% wanted to use both methods. In the 36 to 45 years category 50% preferred the use of facial authentication, 40% the use of pins and passwords whilst only 10% wanted to use both methods. In the above 45 years category, 15% wanted to use facial authentication, 80% wanted the use of pins and passwords whilst 5% preferred the use of both methods. The results show that the youthful population prefers the use of facial authentication combined with passwords and pins as they are aware of increasing cases of cybercrime. The older generation shows a preference for the more traditional methods as they may be reluctant to change to newer methods. This may also indicate a lack of appreciation of increasing cybercrime in the financial sector as well as resistance to change.

Overall, from the data collected from both bank customers and employees, the findings are that respondents who are less than 45 years old are aware of facial authentication as a security measure and show a preference for it as compared to PIN/password authentication. For the customer age group of 45 and above they showed that they know less or even nothing about facial authentication and hence less preference for it as compared to PIN/password. In light of these findings, the research concluded that most of the stakeholders who disagree with the idea of facial authentication are those who lack knowledge and education about the invention. Findings revealed that respondents who are 45 years old and working are more knowledgeable about facial authentication and show a preference for it. Overall, if facial authentication is going to be implemented the probability that the users will accept the system is high.

From the interviews conducted with the Cyber Analyst, the following was obtained:

"*…. Facial authentication is highly recommended since there is no room for attacking methods such as shoulder surfing attack, especially on our ATMs where people will be crowded…"*

The cyber analyst also highlighted that several bank account holders faced some attacks mainly from stripe card cloning and PIN theft. The analyst also explained the rising concern of vishing attacks where the hackers just use phone calls to obtain

bank account credentials from bank customers. The cyber analyst indicated that if financial institutions were using facial authentication, such attacks could have been avoided. The cyber analyst recommended the upgrading of bank software in the hope that it would reduce digital fraud within banks.

The cyber analyst further argued that although facial authentication is more expensive to implement than PIN/password because of its need for computing servers with more processing power, it will be profitable in the long run since anticipated losses due to password-based hacking outweigh the initial outlay for setting up facial authentication schemes.

Another respondent 2 indicated that…
"…The advantage of facial authentication is that it is fast and more reliable and does not require the participation of the customer as in the input of passwords and PIN….".

Respondent 3 indicated that
"…. the younger generation have already adopted facial authentication as evidenced by their use on smartphones…"

The Impact of Facial Authentication on bank Security

Another objective of the research was to assess customer perception of whether facial authentication could improve bank security as compared to other methods. Findings from the study are presented in Figure 4.

Findings revealed that in the 25 years and below category 50% felt that facial authentication would improve bank security, 20% thought that bank security would not improve and 30% indicated that facial authentication would partly improve bank security. In the age group 25 to 35 years about 35% of the respondents indicated that facial authentication would result in improved security, 25% indicated that it would not improve and 40% felt it would partly improve. In the 35 to 45 years category, 47% agreed that facial authentication improves bank security, 31% said it would not improve bank security and 22%. In the above 45 years category, 40% agreed that facial authentication would improve bank security, 40% indicated that it would not improve and 20% indicated partial improvement. Overall a majority of the respondents thought that facial authentication would bring an improvement in bank security.

Feasibility of Facial Authentication Implementation

The research sought to assess the feasibility of facial authentication in banks and so interviews were conducted with the IT managers and Project Managers for the two banks. Responses revealed that they can implement facial authentication effectively in terms of financial resources and human capacity.

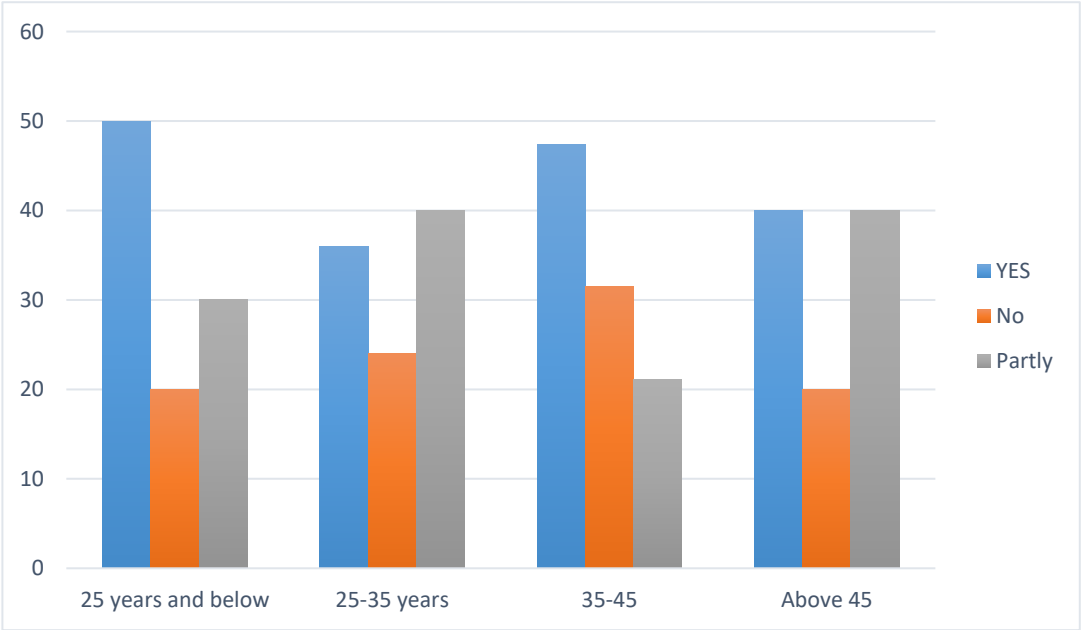

Figure 4. The impact of facial authentication
Source: Analysis of Primary Data

The IT managers and technicians further expressed that the computing servers they had were capable of handling facial authentication software programs. One of the respondents said,

"…. If our servers are overwhelmed, we can consider hiring cloud services from TelOne Data centres or Utande Datacentres which are locally available and there is no need for foreign currency to pay for the subscription hence boosting the feasibility of the facial authentication method…."

The Project Manager further contends that even though implementing facial authentication proved to be extremely costly, the project was worthwhile as it embraced technology and improved confidence in the banking system through the prevention of several cybercrimes.

An experiment was also conducted to test the probability of customers being prone to social engineering attacks. Findings from the experiment revealed that 80% of the participants visited the link. However, only 25% provided the information that was requested. According to Siadati et al. (2017), evaluating a phishing experiment must be based on the previous phishing experiment to see if the vigilance towards falling into track has changed. In this regard, key informants testified that a clicking mail phishing test was conducted in 2018 and 2019, resulting in 68 percent and 47per cent of them falling into the phishing test before training them, respectively. However, Kumaraguru et al, (2007) suggested that there is an acceptable range of falling into phishing tests that is at most 5%. Results show that of the 80% who have visited the link, only 25% provided the requested information. These findings revealed a decrease from 47% to 25%. However, these results show those bank customers who perform banking transactions online are at high risk of phishing. Interviews conducted with Managers revealed that bank systems have to be equipped with facial authentication to curb the risks associated with online transactions.

Problems associated with Facial Authentication implementation

Another objective of the research was to assess the challenges that may be encountered in implementing facial authentication banking security. Findings revealed that the lack of knowledge of facial authentication by Customers was a foreseen challenge. From the data, there are a significant number of people expressing a lack of knowledge of the technology and this is likely to present a problem when banks consider upgrading their system to facial authentication and thus uptake by the customers is likely to be low.

Technical implementation problems were also detected as implementing facial authentication needs more expertise than implementing authentication schemes based on PIN/password as revealed by one of the developers during the interview. The developer explained that for facial authentication to work, complex efficient algorithms have to be designed using deep machine learning and neural networks so that it works well. Another challenge cited was the heavy investment needed to implement the technology. This would require heavy budgets so that it becomes feasible.

Conclusion

The research concludes that a large number of customers and bank employees are aware of facial authentication as a method of improving bank security. There is mainly the young generation who have an appreciation of changing technology and the need to embrace it. The general sentiments were that facial authentication improves bank security and hence boosts customer confidence as it ensures the safety of information and customers are willing to embrace the technology Although a huge capital outlay is needed to implement facial authentication in banks adopting the technology was worthwhile in the long run and it was a feasible project for banks to undertake. Challenges likely to be encountered include lack of knowledge by the customers, lack of adequate financial resources, and lack of expertise to set up the systems. The research recommended that banks consider facial authentication to improve their security and enhance customer confidence. There is a need to budget for awareness campaigns and a budget for the setup of the system.

References

Al-Allaf, O. (2014). Review of Face Detection Systems Based Artificial Neural Networks Algorithms. *The International Journal of Multimedia & Its Applications*. 6 (1), 1.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), 168.

Albalooshi, F., Smith-Creasey, M., Rajarajan, M. & Albastaki, Y. (2018). Facial Recognition System for Secured Mobile Banking.

Sustainability and Resilience Conference: Mitigating Risks and Emergency Planning: Kingdom of Bahrain. 3(7). 92.

Bani-Hani, A., Majdalweieh, M., & AlShamsi, A. (2019). Online authentication methods used in banks and attacks against these methods. *Procedia Computer Science*, *151*, 1052-1059.

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, *35*(5), 1491-1511.

Chowdhury, M., Gao, J., & Islam, R. (2017). Fuzzy rule based approach for face and facial feature extraction in biometric authentication. *In Proceedings of the 2016 International Conference on Image and Vision Computing New Zealand (IVCNZ)*, Palmerston North, New Zealand.

Desai, A. (2018). Cybercrime, cyber surveillance and state surveillance in South Africa. *Acta*

Criminologica: African Journal of Criminology & Victimology, 31(3), 149-160.

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. *Reading, MA:* Addison-Wesley.

Fosse, G., Leo, S., Rodriguez, C. S. & Gratao, N. (2017). FEBRABAN survey on Banking Technology, *Technical Report*.

Federal Financial Institutions Examination Council (FFIE), (2005). Authentication in an internet banking environment, *Financial Institution Letter* - FIL-103-2005.

Galterio, M. G., Shavit, S.A., & Hayajneh, T., (2018). A review of facial biometrics security for smart devices, *Computers,* 7(37).

Gates, K.A. (2011). Our Biometric Future Facial Recognition Technology and the Culture of Surveillance; *NYU Press*: New York, USA,

Han, C. K., Lee, S. K., & You, Y. Y. (2016). The effect of intension to use biometric-based non-face-to-face authentication system in financial transactions-Focusing on extended UTAUT model. *Indian Journal of Science and Technology*.

Hinton, G. E., Osindero, S., & Teh, Y.-W. (2006). A fast learning algorithm for deep belief nets. *Neural computation*,18 (7), 1527–1554

Huang, Y., Huang, Z., Zhao, H., & Lai, X. (2013). A new one-time password method. *IERI Procedia*, *4*, 32-37.

Huang, L., Song, Y., Li, J., Zhen, Z., Yang, Z., & Liu, J. (2014). Individual differences in cortical face selectivity predict behavioral performance in face recognition. *Frontiers in human neuroscience*, *8*, 483.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa, *The Journal of Global Information Technology Management.* DOI: 10.1080/1097198x.2019.1603527

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914).

Maddox, I., & Moschetto, K., (2019). Modern password security for users. User-focused recommendations for creating and storing passwords. Accessed from: https://cloud.google.com/static/solutions/modern-password-security-for-users.pdf, accessed on 6/2/2024

Maithili, K., Vinothkumar, V., & Latha, P. (2018). Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. *Journal of Computational and Theoretical Nanoscience*, *15*(6-7), 2059-2063.

Majdalawieh, M., Bani-Hani, A., Hussain, M., & Alshamsi, A. (2022, December). Assessing the Attacks Against the Online Authentication Methods Using a Comparison Matrix: A Case of Online Banking. In *2022 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 1039-1046). IEEE.

Mardikar, U. (2017). Systems and Methods for Authenticating Facial Biometric Data against Secondary Sources. U.S. Patent 20170091533 A1,

Maphosa, V. (2023). An overview of cybersecurity in Zimbabwe's financial services sector. *F1000Research*, *12*, 1251.

Meval, T. & Kumbharana, C. K., (2014). Study of different Trends and Techniques in Face Recognition. *International Journal of Computer Applications* (0975 – 8887) IV (8), 96.

Muhamba, V. (2021). Ecocash US$100 million fraudsters arrested, Techzim, accessed on 27 April 2021 05:02am. https://www.techzim.co.zw/2021/04/ecocash-us100-million-fraudstersarrested/amp/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:%20techzim%20(Techzim).

Ndubueze, P. N. (2020). Cybercrime and legislation in an African context. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 345-364.

Oliveira, J.S., Sounza, G.B, Rocha, A.R., Deus, F.E., & Marana, A.N., (2020). Cross-Domain Deep Face matching for Real Banking Security Systems, *ICEDEG Conference Proceedings.*

Ometov, A., Bezzateev, S., Mäkitalo, N., & Andreev, S., (2018). Multi-Factor Authentication: A Survey. *Cryptography.* 2(1).

Rehman, A. A., & Alharthi, K. (2016). An introduction to research paradigms. *International Journal of Educational Investigations*, *3*(8), 51-59.

Rubin, J. G., (2009). Methodological challenges in assessing general population: Reaction in the immediate aftermath of a terrorist. *International Journal of Methods Psychiatry research,* 17, 29-35.

Rupapa T. (2021), Fraudsters appear in court, The Herald, viewed at 27 April 2021 05:06 am, https://www.herald.co.zw/ecocash-fraudsters-appear-in-court/amp/.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89.

Saunders., M., Lewis, P., and Thornhill. A., (2007). Research Methods for Business Student, 4th edition.

Shang-Hung, L., (2000). An Introduction to Face Recognition Technology. Informing Science *Special Issue on Multimedia Informing Technologies*, 2 (3) 1

Srinivasan, R., & Chowdhury, A. R. (2015). Robust face recognition based on saliency maps of sigma sets, *in Proceedings of International Conference on Biometrics: Theory, Applications, and Systems*.

Stephen, A. Ojeka,1., Egbide, B., & Edara-Obong, I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness, *International Review of Management and Marketing*, 7(2), 340-346.

Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., & Kozych, I. V., (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics,* 18, 751-762.

Szczodrak, M., & Czyżewski, A., (2017). Evaluation of Face Detection Algorithms for the Bank Client Identity Verification. *Foundations of Computing and Decision Sciences*.42(2).

World Bank, (2017). The Global Findex Database 2017, available at https://globalfindex.worldbank.org/.

Zimucha, T., Zanamwe, N., Chimwayi, K., Chakwizira, E., Mapungwana, P., & Maduku, T. (2012). An Evaluation of the Effectiveness of E-banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks. *Journal of internet banking and commerce*, *17*(3).

Zulfigar, M., Syed, F., Khan. M. J., & Khurshid, K., (2019). Deep Face Recognition for Biometric Authentication, *Proceedings of the 1st International Conference on Electrical Communication and Computer Engineering.*