South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Biometric technology in banking institutions: 'The customers' perspectives'

Authors:
Abraham Morake[1]
Lucas T. Khoza[1]
Tebogo Bokaba[1]

Affiliations:
[1]Department of Applied Information Systems, College of Business and Economics, University of Johannesburg, Auckland Park, South Africa

Corresponding author:
Lucas Khoza,
lucask@uj.ac.za

Dates:
Received: 13 May 2021
Accepted: 28 Sept. 2021
Published: 10 Dec. 2021

How to cite this article:
Morake, A., Khoza, L.T. & Bokaba, T., 2021, 'Biometric technology in banking institutions: "The customers' perspectives"', *South African Journal of Information Management* 23(1), a1407. https://doi.org/10.4102/sajim.v23i1.1407

Background: Over the years, attention has been focused on digital banking and financial technology with little or no attention being paid to biometric banking technology.

Objective: The study aimed to investigate the need for security and simplicity in the authentication of retail payments, digital banking and financial technology through the application of biometric systems.

Method: The study employed quantitative research methodology and a response rate of 52% was achieved. A set of questionnaires was distributed for data collection.

Results: The study's findings indicated it is imperative for all businesses that participate in financial businesses to fully implement the best possible security measures or systems to ensure or enhance security for financial business activities.

Conclusion: Based on the findings of the study, it is recommended that businesses must adopt the new innovative and secured mechanisms of financial dealings to enhance innovation, security and flexibility.

Keywords: biometrics; financial technology; security; authentication methods; digital banking.

Introduction

There are increasing concerns related to the security in authenticity and integrity of banking systems (De Souza Faria & Kim 2013; Petrlic & Sorge 2013). The weakness of the current verification or authentication methods such as pin numbers and passwords contributes significantly towards information leakage stored in Automated Teller Machine (ATM) smartcard which results in loss of money in bank account (Jaiswal & Bartere 2014). The word biometrics originates from ancient Greek and implies measures – bios mean life, whilst metrics mean measuring, therefore in full it means measuring life (Prabhakar, Pankanti & Jain 2003). It can be described as the process of identifying human uniqueness employing physical traits that include the face, fingerprint, iris and behavioural traits (Jain, Flynn & Ross 2007). There are various biometrics classifications: fingerprint scrutiny, face examination, hand geometry, iris observation, voice recognition, and signature acknowledgement (Clodfelter 2010).

The birth of biometrics can be traced back to the 19th century where it mainly focused on gaining knowledge of people's physical traits to secure their identity (Maguire 2009). Earlier biometrics was mainly applied within high-security applications. However, it is currently applied within a wider variety of public-facing applications, for example, in prisons, by police for drivers' license verification, canteen administration, payment systems, in the borders for verification control, including electoral system (Ashbourn 1999). Since the late 1990s, there have been changes in biometrics as a primary security replacement technology from an older form of identification such as passwords and security pin-codes (Maguire 2009). Biometrics initially was used to measure the physical and behavioural features of a person (Galton 1901). Upcoming biometric verification applications comprise ATM use, workplace authentication, network access, travel and tourism, world wide web connections, and mobile connections (Ashbourn 1999).

Over the last few years, more studies have been done on digital banking, financial technology and other areas rather than the impact of biometrics within banking and retailing in South Africa. Digital is the separation of information from physical data storage to the technical potential or digital (Legner et al. 2017). There are various characteristics of digitisation, namely collaboration, sharing, co-creation, connectivity, communication, mobility, and flexibility (Syler & Baker 2016). Digital networks started to join retailers together with traders, clients and customers to develop the identified needs for the first online connected catalogues and inventory software systems (Kelman

2016). Digital banking refers to the process of shifting into online banking and the digitisation of the entire outdated banking activities, including plans that were historically offered to the bank customers and required customers to physically visit the bank to do specific activities such as money deposit, withdrawals, money transfers and account management (Coetzee 2018). Digital banking has facilitated customers to overcome controlled time banking and local area operations (Das 2018). Digital banks use advanced banking systems that can swiftly implement new services allowing for seamless mobility for bank users (Varga & David 2017).

The main problem with this research is that there is a demand for more innovative and secured banking systems that will enable customers to access their money at any given time and location. In this fourth industrial revolution (4IR) era and the need for transformation within the banking sectors, technological advancement has provided better opportunities for financial institutes to tap. In contrast, many financial institutions have conformed to the traditional digital banking platforms as a mode of operation. This digital banking platform enables customers to make money deposits, withdrawals, transfers and account management without physically visiting the bank. However, none of these banking sectors have been able to take full advantage of the capacity and possibilities of the 4IR for a more innovative and simplified banking platform.

There are only few studies which have studies and covered biometric banking and payment systems. To bridge the gap, this study seeks to evaluate the innovative and secured methods of paying for items at retail stores and accessing money without physically having a bank card and hard cash through the application of biometrics. The study focuses on biometrics digital banking financial technology as an alternative means of authentication for mobile baking transactions such as payments and bank transfers. Current authentication methods still use traditional password authentication. In addition, this article seeks to create awareness in banks and retailers on the significant role of biometrics as an essential mechanism in providing speedy, secured, flexible and innovative authentication process to protect the funds/money of customers and the organisation, which can result in crime being lowered or prevented.

This article is structured as follows: section literature review, discusses the current knowledge and findings around biometric technology in the banking system. Section Challenges of biometrics covers the research problem that this research study attempts to address. Section Research method and design discusses the research methodology. Lastly, sections Results and analysis through 11 is the data analysis.

Literature review: Biometric technology in the banking system

As submitted by Ateba et al. (2013), for banks to remain relevant, successful and competitive in today's competitive world, they must provide innovative and best-secured services to their customers.

Customer and organisational perspectives

A customer can be described as a stakeholder of an organisation who provides payment in exchange for products or services (Ateba et al. 2013). In addition, a customer cannot only be described as a person but also an organisation (e.g. university, bank, construction company, school, legal firm and hospital) that buys goods and services from other retailers (Rahman & Safeena 2016). Organisations (banks and retail) need to understand that customers come from various occupations (Rahman & Safeena 2016). More banking and other financial transactions are being done online by customers and fraudsters have followed suit, initiating ever-more sophisticated attacks. With the risk of digital fraud and theft increasing many organisations have searched for solutions to stop fraudsters from launching ever-more sophisticated attacks. Banks cannot stop or limit the high rate of transaction scams and security breaks by using traditional security systems such as password/pin and identification cards; therefore, digital banking solutions appear to be a perfect mechanism to defeat these threats (Hosseini & Mohammadi 2012). Pin code verification alone cannot be regarded as a strong defence mechanism against security breaches. Using digital banking solutions, the operator's data or information is securely kept in an encrypted container or sandbox (Johnson 2019).

Digital perspective

Digital banking solutions have proven to be more innovative for end-users, who appreciate replacing a complicated password with a fingerprint or face scan, which features biometric technologies (Agidi 2018). By applying biometrics, traditional passwords are becoming a thing of the past; biometrics is taking over banking security. To achieve safeguarding of operations and customer transactions, one solution is to secure banking using a consistent authentication method such as biometric (Hosseini & Mohammadi 2012). Biometrics characteristics include fingerprints, veins, palm veins, iris, retina, face, voice, and handwritten signature. The patterns of blood vessels in the palm finger are so different that no two or more individuals possess the same, and this can serve as a trusted security system (Ahmad, Ali & Adnan 2012). Biometrics is still in its early stages in developing countries, but it has been developed and adopted by businesses to increase the security and efficiency of the adopter's operations (Agidi 2018).

Usage of biometrics in banking institutions is popular in developed countries thus, the adoption rate of biometrics is growing significantly (Venkatraman & Delpachitra 2008). There is no hesitation that biometrics are escalating for banking security, to an extant identifying authentication through biometric application is highly secured compared to password authentication (Liang, Samtani, Guo & Yu 2020). Biometric authentication is also coming to physical payments

cards; biometrics are progressively being used for account access, even replacing debit cards at the ATMs (Lee 2016). Biometrics provides a much more reliable and efficient method of verification than relying only on human agents. The security and efficiency principles of biometrics make the adoption of biometrics an attractive prospect to banking institutions across the world (Agidi 2018). With the average banking customer managing a broader range of financial transactions online through desktop and mobile devices, the need for simple and secured access to their banking data is becoming a top priority for banking service providers intending to differentiate themselves from the direct rivals. As the digital age expands, banks need to balance security and accessibility (Varga 2018).

Major South African banks include: ABSA, FNB, Nedbank, Standard Bank, and Capitec (Coetzee 2018). This is based on their revenue generation, large base of customers, services and products they offer and marketing strategies they deliver. Without the successful implementation and adaption of e-banking by the South African banking industry, most banks will struggle to perform optimally through the adaption of the 4IR and FinTech (Abukhzam & Lee 2010). Businesses have realised the increasing value digitisation provides towards the growth of businesses (Neumeier et al. 2017).

It is important that digital payment service providers (banks) have a comprehensive cybersecurity strategy aided by a robust framework to assist all stakeholders participating in the ecosystem (Kristensen & Solvoll 2019). There is a demand for managing service interface and customisation of products and services influenced by the input of technology offered in business settings (De Farias et al. 2014). Advanced biometric payment methods enhance the convenience, choice of payments and alternative payment methods for customers. Payment methods allow customers to conduct business and commercial activities with ease and flexibility at any given time (Kristensen & Solvoll 2019). Payment experts concur that electronic payment techniques are efficient, convenient and fast (Crowe, Schuh & Stavins 2006).

Biometrics application in automated teller machines

Biometrics in banking for ATM authentication provides both the banks and the customers with an outstanding benefit through providing customers with the flexibility to do transactions without physically having their bank cards; thus, banks can avoid the costs and liabilities of customer problems because of lost and/or stolen bank cards (Vernkatraman & Delpachitra 2008). Using biometrics in banking, ATMs are popular in developed countries; thus, the adoption rate of biometrics is growing significantly (Venkatraman & Delpachitra 2008). There is no doubt that biometrics is escalating in banking security, but it might be a while before identifying authentication without passwords is completely secure (Furnell & Evangelatos 2007). Biometric authentication is also coming to physical payment cards; thus, biometrics is progressively being used for account access, even replacing debit cards at the ATMs (Choi et al. 2007).

Challenges of biometrics

Biometric challenges can negatively impact people and businesses or customers and organisations. Bank crises and failures can be attributed to the growing extent to which scammers and fraudsters operate (Bhasin 2015). Fraud is considered a global phenomenon that negatively challenges all sectors of the economy (Bhasin 2015). A rapid increase in security cracks and transactional breaches within traditional security systems such as pin codes and passwords is speedily influencing the evolution of a strong biometric authentication method (Hosseini & Mohammadi 2012).

In addition, a factor that can contribute towards the challenges of adopting biometrics is too much time and money spent to educate people who are technologically and biometrically illiterate (Ahmad et al. 2012). New deployments or the premature phase of biometric technology are quite similar to the introduction of any other system, since it might take a while for general users to accept it, depending on the system's impact on them (Wayman et al. 2005).

Any form of change in the customers finger (a user cuts him-/herself by mistake) may lead to the users being denied access to their respective systems that has been created by the users with their normal fingerprint (Ahmad et al. 2012).

Another significant challenge of biometrics includes a scenario whereby, should the user be involved in an accident and lose an eye, finger or facial changes occur because of scratches or cuts, the biometric system will not recognise the user and will reject the user as a result of the physical changes or damages (Aly et al. 2008; Buddharaju, Pavlidis & Manohar 2008).

Biometrics has difficult challenges that may impact the human rights of a person negatively, for example, when a thief decides to cut off a victim's finger to gain access to their information and the system (Choi et al. 2007; Chetty & Wagner 2009; Jin, Kim & Elliott 2007; Pacut & Czaika 2006; Tan et al. 2010; Toth 2005). Dust and grime on the fingerprint scanner may impact the quality of the system negatively, which may result in a situation where the system does not recognise the user (Ahmad et al. 2012).

There are various issues that characterise the challenges of biometrics in problems such as signature authentication forgery, the high cost of implementing liveness detection, dust dropped on scanners, poor quality of the scanner to recognise the user, a time-consuming system, poor human machine interaction, lack of guidance for interacting with the system and a lack of proper information security policies and procedures (Brooks 2010; Jain & Kumar 2010; Koppenhaver 2007; Park 2008).

The main contributing factors to the challenges of biometric information usage is the misuses, negative interpretation,

and failure to complying to the *Protection of Personal Information Act* (POPIA). The purpose of the Act is to protect people from harm by protecting their personal information, to stop their money being stolen, to stop their identity being stolen, and generally to protect their privacy, which is a fundamental human right (POPIA Act 2021). In South Africa, a person's fingerprints and blood type are considered personal information under the *Electronic Communications and Transactions Act* (ECTA 2002).

Since early 2020, the COVID-19 pandemic has impacted on and disrupted many aspects of peoples daily life. Touch-based technologies such as fingerprint and facial recognition scanners can be considered as indirect contributing factors for COVID-19, because they are used by many people for authentication and verification purposes at ATMs, stores and banks (Gomez-Barrero et al. 2021). Hygiene related fears have increased the societal resistance towards the use of touch-based biometrics sensors (Priesnitz et al. 2021). In addition, it is important to note that such fears have in turn fuelled research efforts in 2D or 3D touchless fingerprint recognition systems (Gomez-Barrero et al. 2021).

Benefits of biometrics

Biometric benefits can impact both people and businesses or customers and organisations. Moreover, biometrics can be considered a quicker information tracer and recovery method than manual or traditional verification methods carried out at the counter (Ahmad et al. 2012; Jain & Kumar 2010; Jain, Ross & Pankanti 2006).

Biometric security can be considered a method that contributes significantly towards ensuring the integrity, confidentiality and availability of information (Ahmad et al. 2012). Biometrics protects both logical and physical access controls. Logical access controls include the protection of network facilities, computers and information systems against unauthorised admission (Jain et al. 2006), whilst physical access controls ensure that only authorised people have access to IT infrastructures and document filing (Jain et al. 2006).

Forensic accounting is a requirement for banks to decrease the speedy growth of financial frauds (Bhasin 2015). In addition, biometric authentication methods offer a natural, unforgettable and rarely breached verification (Hosseini & Mohammadi 2012). Password, pin and code word authentication can be forgotten, cracked and guessed by hackers or scammers (Jain et al. 2006). In addition, fingerprint authentication is more secure, as it provides users with quicker verification and is impossible to forget compared to a password (Johnson 2019). Smartcards are also at risk of being lost, stolen and duplicated (Jain et al. 2006). Therefore, biometrics can be considered a solution for enhanced security, as the authentication relies on a person's physical traits (Jain et al. 2006). Physiological biometric features include retina, fingerprint, hand vein, iris, hand geometry facial recognition, and ear shape. These features are unique, and no one in the world shares them (Ahmad et al. 2012). Behavioural biometric features include voice recognition and signature verification (Ahmad et al. 2012; Jain & Kumar 2010).

Biometric security systems can assist banks with various benefits such as forensic application, criminal identification, border control and surveillance (Rhodes 2003). Various impacts may characterise the benefits of biometrics, for example, human signature authentication, being user-friendly, convenient and flexible, maintaining accuracy, faster information retrieval, strong matching algorithm and speaker recognition (Koppenhaver 2007; Park 2008; Wang et al. 2011).

Multi-factor authentication methods

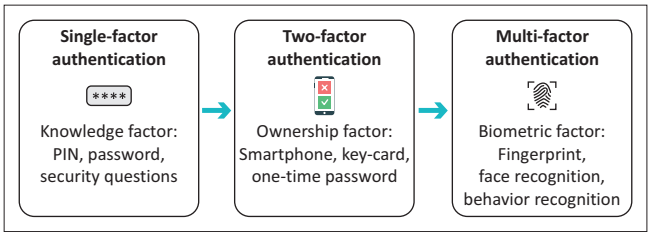
The use of a password (or a PIN) to confirm the ownership of the user ID could be considered as a single-factor authentication (SFA) method (Ometov et al. 2018). Evidently, this is the weakest level of authentication (Dasgupta, Roy & Nag 2016; Bonneau et al. 2015).

Authentication with just a single-factor method is not reliable to provide enough protection because of several security threats such as rainbow table and dictionary attacks (Gunson et al. 2011). Two-factor authentication (2FA) methods consist of something the user has, such as cards, smartphones, or other tokens (Sun et al. 2014; Bruun, Jensen & Kristensen 2014). Multi-factor authentication (MFA) methods consist of something the user/customer is, specifically, biometric data or behaviour patterns such as fingerprint, face recognition, behaviour recognition and others (Ometov et al. 2018).

The need for reliable user authentication method has increased in the wake of intensified concerns about security and rapid advancements in communication, mobility, and networking (Yadav & Gothwal 2011). Frequently, MFA is based on biometrics, which is automated recognition of individuals based on their behavioural and biological characteristics (Frank, Biedert, Ma, Martinovic & Song 2012). Biometrics challenges and benefits will be further discussed in detail, because the term can be considered as a key technique of MFA. Figure 1 shows the evolution from SFA factor to MFA.

Research method and design

The research design that was used in this study was quantitative. Quantitative research refers to a numerical



Source: Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y., 2018, *'Multi-factor authentication: A survey'*, *Cryptography* 2(1), 1.

FIGURE 1: Evolution of authentication methods from single-factor authentication to multi-factor authentication.

illustration of explanations of the phenomena (Sukamolson 2000). Throughout the study, data have been collected by means of:

- A literature review and comparing a list of similar work done over the years.
- Conducting an online survey to evaluate the use of biometrics to authenticate payment and day-to-day personal banking transactions.
- Consulting with shoppers, bank users, financial institutions such as banks and general societies (students, employed and unemployed community members) with bank accounts.

A questionnaire survey was conducted on a sample population of respondents who have knowledge on biometrics, digital banking, financial technology, retail and customers. The overall number of the questionnaires shared received 336 responses. Out of the 336 responses, only 173 respondents submitted fully completed questionnaire, the remaining 162 respondents did not complete the survey. This process gave the questionnaire a successful completion response rate of 52%. The questionnaire was designed into four sections which are: A, B, C and D. Section A gathered the background information of the respondents, Section B collected the challenges of biometric, Section C collected benefits of biometric, and the final Section D gathered biometric solutions to enhance secured and innovative means of accessing, transferring and sharing money. The survey was distributed electronically via different social media platforms. The selected sample technique for this study is the probability sampling technique which facilitates study of a large population, and therefore was relevant for this study as its targeted sample size was 300 responses. Furthermore, quantitative research is commonly aligned with the probability sampling technique to enhance generalisability (Saunders et al. 2019). The reason for the study to employ students is because financial decision-making is very important for the success of students in their lives and careers; therefore, it is critical for students to understand funds management (Sachitra, Wijesinghe & Gunasena 2019). Another contributing reason for the study to use bank members such as managers is because they value financial information and have key financial knowledge (Akhtar & Liu 2018).

The study employed the random sampling technique in preference of the systematic, stratified and cluster random sampling techniques. The inclusion criterion for the study was shoppers with one or more bank accounts. The study mainly focused on the city of Johannesburg in Gauteng province. Johannesburg has an estimated population of 5 782 747. Out of this population, about 30% are below the standard age of owning a bank account (Department of Statistics South Africa 2019), totalling 1 734 824. From the remaining 4 047 923 shoppers with bank accounts, the sample size of the research was limited to 300 respondents because of issues such as time and resource constraints. The study only targeted the age group of 18–60. The study also targeted the population using payment mechanisms such as:

- eWallet
- Electronic Fund Transfers (EFTs)
- Credit and cheque cards
- Internet banking transfers
- Card-based payments
- Debit cards
- PayPal
- Visa Checkout
- Google Pay
- Samsung Pay/ Mobile Pay

Validity of the data collection tool used

The validity of the collected data was demonstrated through questionnaires and surveys. Content validity will be determined based on the reliably collected data provided by respondents (bank managers, retail managers and customers). Thus, constructive validity will be determined through evaluating the views of customers, bank managers and retail managers using biometrics authentication for payments and other activities. Both Cronbach's alpha and Statistical Package for the Social Sciences (SPSS Version 26) were used to ensure that the collected data is accurate, logical and factual (Scherbaum & Shockley 2015).

Using the Cronbach's alpha analytical tool on SPSS, it was found that the validity of the response regarding 'usage of biometrics in terms of financial sector' is 0.857. Table 1 shows the Cronbach's alpha values.

Ethical considerations

Approval to conduct the study was obtained from the College of Business and Economics, the University of Johannesburg. During data collection, personal information was not requested and participation in this research work was voluntary, and participants were allowed to withdraw upon completing the questionnaires.

Results and analysis

This section of the study presents findings of the study obtained during questionnaire distribution.

Descriptive statistics

Figure 2 describes the sector or occupation in which respondents are involved. In a practical example, the people belonging to academic and education sectors visit retail stores to purchase books, laptops and other academic or education-related merchandise. In construction sector, there must be a purchase of building or construction materials;

TABLE 1: Cronbach's alpha values.

Section	Cronbach's alpha value
E-Banking	0.852
Financial Technology	0.857
Biometrics	0.858

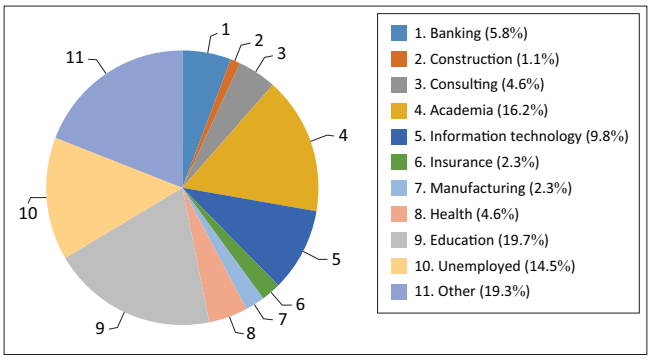


FIGURE 2: Sector or occupation analysis.

the same applies to other occupations. This shows that data supplied by these categories of respondents are reliable.

The education sector has the highest percentage of 19.7%, followed by Other with 19.1%. Academia is the third-ranked sector with 16.2%, followed by the unemployed respondents with 14.5%. The information technology sector is ranked fifth with 9.8%, followed by the banking sector with 5.8%. Both the health and consulting sectors have a percentage of 4.6%. The manufacturing and insurance sectors both have a percentage of 2.3%. The construction sector has the lowest percentage of 1.1%. Table 2 shows the sector or occupation values to clarify values in Figure 2.

The results show that the study has covered various organisational sectors. Academia, construction, consulting, education, health, information technology, insurance, manufacturing and other sectors, including the unemployed individuals, are all represented. This concludes that most organisational sectors have been represented in the study.

Highest qualification

Figure 3 describes the highest qualification of respondents to evaluate their potential level of understanding new topics that impact their daily lives and activities in this modern era of the 4IR. The results are arranged from the highest to the lowest percentage. Results reveal that 31.8% of the respondents have obtained a bachelor's degree, 16.8% matric or Grade 12, 15.0% an honours degree, another 13.3% a university diploma, 11.0% a Master's degree, 6.4% college diplomas, 4.0% other qualifications, 1.2% with a Ph.D. degree and 0.5% without matric.

The results indicate that a large percentage of the respondents have obtained a bachelor's degree. This indicates that most respondents have a good education and are more knowledgeable (Bosupeng 2017). A question on rating the educational level of the respondents has been included to evaluate their level of understanding new topics impacting their daily lives and activities in this modern era of the fourth industrial revolution.

It is important to be educated, well-informed and technologically exposed because education contributes significantly to developing a person's opinions, character, trading with others and preparing one for life experiences (Al-Shuaibi 2014).

TABLE 2: Sector or occupation analysis.

Sector	Values (%)
Education	19.7
Other	19.1
Academia	16.2
Unemployed	14.5
Information Technology	9.8
Banking	5.8
Health	4.6
Consulting	4.6
Insurance	2.3
Manufacturing	2.3
Construction	1.1

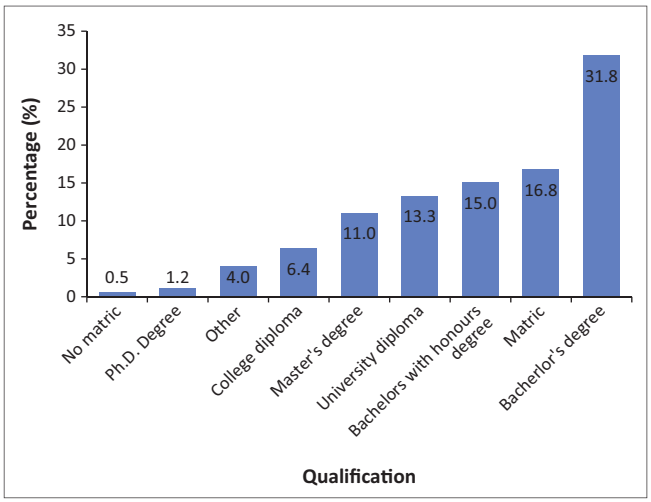


FIGURE 3: Highest qualification of respondents.

Additional literature aligned with the study provides that promising stages to prevent fraud activities are educating customers with various processes of avoiding being a victim of fraudsters (Bhasin 2015).

Correlation statistics

The purpose of this section is to describe the relationship between variables. Thus, extensive literature was used to analyse other sections of the article; the Pearson's correlation was conducted to explore statistical relationships amongst variables. Moreover, data analysis was conducted through matching and comparing the benefits variables together with the challenge variables. The Pearson's correlation was used because it works with the raw data values of the variables, whereas Spearman works with rank-ordered variables. Moreover, the Pearson's correlation evaluates the linear relationship between two continuous variables, whilst the Spearman correlation coefficient is based on the ranked values for each variable rather than the raw data (De Winter, Gosling & Potter 2016).

The data analysis technique used to analyse the data was correlation to predict the strength and direction between two variables. The strength of correlation between the variables is shown under the Pearson's correlation, whilst Sig. (2-tailed) represents the significance of the influence amongst the variables. Sig. (2-tailed) below 0.05 indicates that the

relationship between the variables is significant, whilst Sig. (2-tailed) above 0.05 indicates that there is no significant relationship between the variables (Pallant 2020). Table 3 illustrates the Sig. (2-tailed) declaration, whilst Table 4 demonstrates the Pearson's correlation declaration.

Biometric challenges and benefits analysis

The Pearson's correlation was conducted to examine the relationship between biometric challenges and biometric benefits.

Appendix 1 shows the Pearson's correlation for enhanced surveillance with involvement in an accident, sensitivity of sensor performance and biometric characteristics. There is a weak positive significant relationship between enhanced surveillance and involvement in an accident (r = 0.004; p = 0.216), enhanced surveillance and sensitivity of sensor performance (r = 0.008; p = 0.202), and enhanced surveillance and biometric characteristics (r = 0.004; p = 0.220).

These findings indicate that should the user be involved in an accident and have cuts on their biometric features such as fingers, face or iris, it will be difficult for a biometric reader to fully recognise the authorised user to gain access to a system. The biometric security system can assist banks and retailers with a wide range of benefits such as surveillance, as reported by Rhodes (2003).

Appendix 1 also shows the Pearson's correlation for enhanced border control with involvement in an accident, sensitivity of sensor performance and biometric characteristics. Statistical results indicate that there is a weak positive significant relationship between enhanced border control and involvement in accident (r = 0.001; p = 0.253), enhanced border control and sensitivity of sensor performance (r = 0.007; p = 0.205), and enhanced border control and biometric characteristics (r = 0.048; p = 0.150).

These findings indicate that enhanced border control can be challenged by the fact that biometric characteristics such as face, fingerprint and voice recognition can be copied. The biometric security system can assist banks and retailers with a wide range of benefits such as forensic application, criminal identification, border control and surveillance (Rhodes 2003).

TABLE 3: Sig. (2-tailed) declaration.

Correlation	Value	Level of Significance
Sig. (2-tailed)	Below 0.05	Significant relationship
Sig. (2-tailed)	Above 0.05	No significant relationship

Source: Pallant, J., 2020, *SPSS survival manual: A step by step guide to data analysis using IBM SPSS,* Routledge, London

TABLE 4: Pearson's correlation declaration.

Correlation declaration 1	Correlation declaration 2	Level of Significance
0.00	0.29	Weak impact
0.30	0.49	Medium impact
0.50	1.00	Strong impact

Source: Pallant, J., 2020, *SPSS survival manual: A step by step guide to data analysis using IBM SPSS,* Routledge, London

Appendix 1 next shows the Pearson's correlation for criminal identification with sensitivity of sensor performance and biometric characteristics. Statistical results indicate that there is a weak positive significant relationship between criminal identification and sensitivity of sensor performance (r = 0.017; p = 0.181) and criminal identification and biometric characteristics (r = 0.032; p = 0.163).

These findings imply that the process of effortlessly providing information about the criminal record of the individual can be challenged by a sensitivity of sensor performance. The biometric security system can assist banks and retailers with a wide range of benefits such as forensic applications, criminal identification, border control and surveillance (Rhodes 2003).

From Appendix 1, the Pearson's correlation for ease of information retrieval with involvement in an accident and biometric characteristics can be observed. Statistical results show that there is a weak positive significant relationship between ease of information retrieval and being involved in an accident (r = 0.014; p = 0.166) and ease of information retrieval and biometric characteristics (r = 0.003; p = 0.224).

These findings indicate that the process of providing users with quicker verification can be hindered by damages or changes to the users' physical biometric features such as face, eyes and fingers caused by accidents. The biometric security system can assist banks with features maintaining accuracy, convenience, faster information retrieval, strong matching algorithm and speaker recognition (Koppenhaver 2007; Park 2008; Wang et al. 2011).

Appendix 1 shows the Pearson's correlation for strong matching algorithm with involvement in an accident, sensitivity of sensor performance and non-technologically inclined individuals. Moreover, statistical results indicate that there is a weak positive significant relationship between strong matching algorithm and being involved in an accident (r = 0.017; p = 0.161), strong matching algorithm and sensitivity of sensor performance (r = 0.007; p = 0.204), and strong matching algorithm and non-technologically inclined individuals (r = 0.008; p = 0.200).

These findings indicate that biometric systems, which can easily differentiate between two or more biometric traits such as hands, eyes and face, can also be hindered by damages or changes to the user's physical biometric features such as the face, eyes and fingers caused by accidents. Pin code verification alone cannot be regarded as a strong defence mechanism against security breaches. However, by using biometric verification, the operator is secured to their data or information which is securely kept in an encrypted container or sandbox (Johnson 2019).

Appendix 1 shows the Pearson's correlation for lost or stolen smartcards and mobile devices with scammers, fraudsters and non-technologically inclined individuals. There is a weak positive significant relationship between lost or stolen smartcards and mobile devices and scammers (r = 0.013; p = 0.188), lost or stolen smartcards and mobile devices and fraudsters (r = 0.003; p = 0.224), and lost or stolen smartcards and mobile devices and non-technologically inclined individuals (r = 0.005; p = 0.214).

These findings indicate that individuals, such as scammers, who participate in dishonest schemes by committing fraudulent activities may intend to exploit lost or stolen smartcards and mobile devices and steal funds of individuals. Biometrics in banking for ATM authentication provides both banks and customers with an outstanding benefit through providing customers with the flexibility to do transactions without physically having their bank cards; thus, banks can avoid the costs and liabilities of customer problems because of lost and/or stolen bank cards (Vernkatraman & Delpachitra 2008).

Appendix 1 also shows the Pearson's correlation for impossible to forget fingerprint authentication, non-technologically inclined individuals and biometric characteristics. There is a weak positive significant relationship between impossible to forget fingerprint authentication and non-technologically inclined individuals (r = 0.014; p = 0.187) and impossible to forget fingerprint authentication and biometric characteristics (r = 0.041; p = 0.155).

These findings indicate that fingerprint authentication is impossible to forget compared to a password. Moreover, non-technologically inclined individuals still trust that the pin code or password authentication method is the best technique for security authorisation (Bhasin 2015).

Appendix 1 further shows the Pearson's correlation for uniqueness, involvement in accident, sensitivity of sensor performance, non-technologically inclined individuals and biometric characteristics. Statistical results reveal that there is a weak positive significant relationship between uniqueness and being involved in an accident (r = 0.011; p = 0.194), uniqueness and sensitivity of sensor performance (r = 0.042; p = 0.155), uniqueness and non-technologically inclined individuals (r = 0.001; p = 0.247), and uniqueness and biometric characteristics (r = 0.002; p = 0.253).

These findings indicate that the uniqueness and benefits of the biometric authentication systems are supported by variables such as being involved in an accident, sensitivity of sensor performance, non-technologically inclined individuals and biometric characteristics such as the face, fingerprint and voice recognition (Hosseini & Mohammadi 2012). Physiological biometric features include retina, fingerprint, hand vein, iris, hand geometry, facial recognition and ear shape. These features are unique and no one in the world shares them (Ahmad et al. 2012).

Appendix 1 shows the Pearson's correlation for forensic application and dust dropped on the fingerprint scanner, involvement in an accident, sensitivity of sensor performance, non-technologically inclined individuals, and fake fingerprint forgery. There is a weak positive significant relationship between forensic application and dust dropped on the fingerprint scanner (r = 0.015; p = 0.185), forensic application and involvement in an accident (r = 0.002; p = 0.236), forensic application and sensitivity of sensor performance (r = 0.000; p = 0.278), forensic application and non-technologically inclined individuals (r = 0.000; p = 0.273), and lastly forensic application and fake fingerprint forgery (r = 0.045; p = 0.153).

These findings indicate that because of physical biometric changes acquired by the users through an accident, it will be difficult for a biometric scanner system to easily recognise the user in a system. Forensic accounting is a requirement for banks to decrease the speedy growth of financial fraud (Bhasin 2015). In addition, the biometric authentication method offers natural, unforgettable, and hardly breached verification (Hosseini & Mohammadi 2012).

Biometric connections as solutions to deliver secured and innovative means of accessing, transferring and sharing money

Table 5 represents biometrics connections, including the level of agreeing and disagreeing by the respondents that the above-mentioned biometrics connections can be labelled as solutions that can assist banks and retailers in delivering secured and more innovative means of accessing, transferring and sharing money. From the 173 surveyed respondents, 93.1% of the respondents agreed that advanced authentications systems/single authentication that a user shares with no one

TABLE 5: Biometric connections as solutions.

Variables	Frequency	%
Advanced authentications systems/single authentication a user shares with no one (such as fingerprint compared to the old traditional authentication such as pins and passwords that can be guessed or traced)		
No	12	6.9
Yes	161	93.1
Total	**173**	**100.0**
Simple and secured access (ability to manage a broader range of financial transactions online)		
No	10	5.8
Yes	163	94.2
Total	**173**	**100.0**
Enhanced convenience		
No	5	2.9
Yes	168	97.1
Total	**173**	**100.0**
Increased security		
No	14	8.1
Yes	159	91.9
Total	**173**	**100.0**
Reliable and efficient verification relying only on human agents		
No	13	7.5
Yes	160	92.5
Total	**173**	**100.0**

(such as fingerprint compared to the old traditional authentication such as pins and passwords that can be guessed or traced) could be labelled as one of the solutions that can assist banks and retailers in delivering secured and innovative means of accessing, transferring and sharing money, whilst 6.9% disagreed on the statement. A majority (94.2%) of the respondents agreed that simple and secured access (ability to manage a broader range of financial transactions online) can be labelled as one of the solutions that can assist banks and retailers to deliver secured and innovative means of accessing, transferring and sharing money. In comparison, 5.8% disagreed with the statement. Whilst, 97.1% of the respondents agreed that enhanced convenience could be labelled as one solution that can assist banks and retailers in delivering secured and innovative means of accessing, transferring and sharing money, 2.9% disagreed with the statement. A higher percentage (91.9%) of the respondents agreed that increased security could be labelled as one of the solutions that can assist banks and retailers in delivering secured and innovative means of accessing, transferring and sharing money, whilst 8.1% disagreed with the statement. Regarding the final connection, 92.5% of the respondents agreed that reliable and efficient verification relying only on human agents could be labelled as one of the solutions that can assist banks and retailers in delivering secured and innovative means of accessing, transferring and sharing money, whilst 7.5% disagreed on the statement.

Literature postulates that banks must provide customers with more innovative and secured banking services (Hosseini & Mohammadi 2012). Biometric authentication or verification method that includes face and fingerprint recognition is considered a precise security solution for accessing, transferring and sharing money (Hosseini & Mohammadi 2012).

Discussion

Pearson's correlation for enhanced surveillance indicates that should the user be involved in an accident and have cuts on biometric features such as fingerprint, face, and iris, it will be difficult for a biometric reader to fully recognise the authorised user to gain access into a system. Biometric security systems can assist banks and retailers with a wide range of benefits such as surveillance, as reported by Rhodes (2003).

Pearson's correlation for enhanced border control indicates that enhanced border control can be challenged by the fact that biometric characteristics such as face recognition, fingerprint and voice can be copied none are 100%. Biometric security systems can assist banks and retailers with a wide range of benefits such as forensic application, criminal identification, border control and surveillance (Rhodes 2003).

Pearson's correlation for criminal identification shows that the process of effortlessly providing information about the criminal record of the individual can also be challenged by the sensitivity of sensor performance. A biometric security system can assist banks and retailers with a wide range of benefits such as forensic application, criminal identification, border control and surveillance (Rhodes 2003).

Pearson's correlation for ease of information retrieval indicates that the process of providing users with quicker verification can be hindered by damages or changes to the user's physical biometric features such as face, eyes and fingers caused by accidents. Biometric security systems can assist banks with the following features maintaining accuracy, convenience, faster information retrieval, strong matching algorithm and speaker recognition (Koppenhaver 2007; Park 2008; Wang et al. 2011).

Pearson's correlation for strong matching algorithm findings indicate that biometric systems that can easily differentiate between two or more biometric traits such as hands, eyes and iris, can also be hindered by damages or changes to the user's physical biometric features such as face, eyes and fingers caused by accidents. Pin code verification alone cannot be regarded as a strong defence mechanism against security breaches, using biometric verification, the operator is secured to their data or information which is securely kept in an encrypted container or sandbox (Johnson 2019).

Pearson's correlation for lost or stolen smartcards and mobile devices findings indicate that individuals who participate in dishonest schemes through committing fraudulent activities such as scammers may intend to exploit lost or stolen smartcards and mobile devices of other users and steal funds of other individuals. Biometrics in banking for ATMs authentication provides both banks and customers with an outstanding benefit through providing customers with the flexibility to make transactions without physically having their bank cards. Thus, banks can avoid the costs and liabilities of customer's problems because of lost and stolen bank cards (Vernkatraman & Delpachitra 2008).

Pearson's correlation for impossible to forget fingerprint authentication indicates that fingerprint authentication is impossible to forget as compared to a password. Moreover, non-technologically inclined individuals still trust that pin code or password authentication methods are the best security authorisation techniques (Bhasin 2015).

Findings for the Pearson's correlation for uniqueness indicate that the uniqueness and benefits of the biometric authentication systems can be astounded by matters such as, involved in an accident, sensitivity of sensor performance, non-technologically inclined individuals and biometric characteristics such as face recognition, fingerprint and voice can be copied none are 100% (Hosseini & Mohammadi 2012). Physiological biometric features include retina, fingerprint, hand vein, iris, hand geometry, facial recognition and ear shape, these features are unique and no one in the world shares them or have the same (Ahmad et al. 2012).

Finally, Pearson's correlation for forensic application findings indicate that, because of physical biometric changes acquired by the users through an accident, it will be difficult for a

biometric scanner system to recognise the user in a system easily. Forensic accounting is a requirement for banks to decrease financial fraud's speedy growth (Bhasin 2015). In addition, the biometric authentication method offers a natural, unforgettable and hardly breached verification (Hosseini & Mohammadi 2012).

Conclusion

This study was carried out to investigate the need for security and simplicity in the authentication of retail payments, digital banking and financial technology through the application of the biometric system. Furthermore, the study assessed the possible challenges, benefits and solutions to the biometrics authentication payment system. From the findings, the study further elaborated and discussed the biometric solutions that can assist banks and retailers in enhancing secured and innovative means of accessing, transferring, and sharing money. It is concluded that biometric technology is the innovative technology that different banking institutions can use to enhance security and innovation, protect the funds of their customers against scammers, fraudsters, hackers, and other constraints. Therefore, further studies can focus on the combined relationship amongst biometrics, digital banking and financial technology.

Acknowledgements

My genuine gratitude to Alpha and Omega, Creator of heaven and earth. Thank you to my supervisor, Mr Lucas Khoza and co-supervisor Mrs Tebogo Bokaba, for their patience, guidance, and continuous support towards completing this Journal.

Competing interests

The authors have declared that no competing interest exist.

Authors' contributions

All authors contributed equally to this work.

Funding information

This study received no specific funding from any agency in public, commercial or non-profit sectors. Because of the budget and time constraints, the study sampled only 173 respondents. The authors acknowledge that this could have impacted the ability to generalise the results of the study. It is therefore recommended that future studies should look at larger sample size. In addition, because of the limited number of individuals who are technologically inclined in the South African society, it was difficult to find respondents who fitted the criteria used to select respondents for the study. The study has not been extended to other provinces, as it is limited to the Gauteng province of South Africa.

Data availability

Data that support the findings of the study can be obtained from the corresponding author L.T.K.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Adewole, K.S., Abdulsalam, S.O., Babatunde, R.S., Shittu, T.M. & Oloyede, M.O., 2014, 'Development of fingerprint biometric attendance system for non-academic staff in a tertiary institution', *Development* 5(2), 62–70.

Agidi, R.C., 2018, 'Using biometric in solving terrorism and crime activities in Nigeria', *Techsplend Journal of Technology* 1(12), 91–105.

Ahmad, S.M.S., Ali, B.M. & Adnan, W.A.W., 2012, 'Technical issues and challenges of biometric applications as access control tools of information security', *International Journal of Innovative Computing, Information and Control* 8(11), 7983–7999.

Akhtar, S. & Liu, Y., 2018, 'SMEs' use of financial statements for decision making: Evidence from Pakistan', *Journal of Applied Business Research (JABR)* 34(2), 381–392.

Aly, S., Sagheer, A., Tsuruta, N., & R.I. Taniguchi, 2008, 'Face recognition across illumination', *Artificial Life and Robotics* 12(1–2), 33–37.

Ashbourn, J., 1999, *The biometric white paper*, viewed 30 July 2021, from http://homepage.ntlworld.com/avanti/whitepaper.htm.

Ateba, B.B., Maredza, A., Ohei, K., Deka, P. & Schutte, D., 2015, 'Marketing mix: it's role in customer satisfaction in the South African banking retailing', *Banks and Bank Systems (open-access)* 10(1), 82–91.

Bhasin, M.L., 2015, 'An empirical study of frauds in the banks', *European Journal of Business and Social Sciences* 4(7), 1–12.

Brooks, D.J., 2010, 'Assessing vulnerabilities of biometric readers using an applied defeat evaluation methodology', *Paper presented at the Proceedings of the 3rd Australian Security and Intelligence Conference*, Perth, November 30, 2010.

Board of Governors of the Federal Reserve System, Consumers and Mobile Financial Services, 2016, Board of Governors of the Federal Reserve System Washington, DC, pp. 1–86.

Bonneau, J., Herley, C., Van Oorschot, P.C. & Stajano, F., 2015, 'Passwords and the evolution of imperfect authentication', *Communications of the ACM* 58(7), 78–87.

Bosupeng, M., 2017, 'How Relevant Are Academic Degrees In The Workplace?', Munich Personal RePEc Archive, MPRA Paper No. 77914. pp. 2–7.

Bruun, A., Jensen, K. and Kristensen, D., 2014, 'Usability of single-and multi-factor authentication methods on tabletops: a comparative study', in *International Conference on Human-Centred Software Engineering*, Springer, Berlin, Heidelberg, pp. 299–306.

Buddharaju, P., Pavlidis, I. & Manohar, C., 2008, 'Face recognition beyond the visible spectrum', in *Advances in Biometrics*, pp. 157–180, Springer, London.

Chandran, R., 2014, 'Pros and cons of mobile banking', *International Journal of Scientific and Research Publications* 4(10), 1–5.

Chetty, G. & Wagner, M., 2009, 'Biometric person authentication with liveness detection based on audio-visual fusion', *International Journal of Biometrics* 1(4), 463–478.

Choi, H., Kang, R., Choi, K. & Kim, J., 2007, 'Aliveness detection of fingerprints using multiple static features', in *Proc. of World Academy of Science, International Journal of Biological and Medical Sciences,* vol. 2, pp. 200–205, Engineering and Technology.

Clodfelter, R., 2010, 'Biometric technologies in retailing: Will consumers accept fingerprint authentication?', *Journal of Retailing and Consumer Services* 17(2010), 181–188. https://doi.org/10.1016/j.jretconser.2010.03.007

Coetzee, J., 2018, 'Strategic implications of Fintech on South African retail banks', *South African Journal of Economic and Management Science* 21(1), 2455. https://doi.org/10.4102/sajems.v21i1.2455

Crowe, M.D., Schuh, S.D. & Stavins, J., 2006, 'Consumer behavior and payment choice: A conference summary', FRB of Boston Public Policy Discussion Paper, (06-1).

Das, S.S., 2018, 'A study of digital banking facilities: With reference to Guwahati in kamrup (metro) district of assam', *Journal of Management* 5(1), 6–13.

Dasgupta, D., Roy, A. & Nag, A., 2016, 'Toward the design of adaptive selection strategies for multi-factor authentication', *Computers & Security* 63, 85–116.

De Farias, S.A., Aguiar, E.C. & Melo, F.V.S., 2014, 'Store atmospherics and experiential marketing: A conceptual framework and research propositions for an extraordinary customer experience', *International Business Research* 7(2), 87–99.

De Souza Faria, G. & Kim, H.Y., 2013, 'Identification of pressed keys from mechanical vibrations', *IEEE Transactions on Information Forensics and Security* 8(7), 1221–1229. https://doi.org/10.1109/TIFS.2013.2266775

De Winter, J.C., Gosling, S.D. & Potter, J., 2016, 'Comparing the Pearson and Spearman correlation coefficients across distributions and sample sizes: A tutorial using simulations and empirical data', *Psychological Methods* 21(3), 273–290.

Electronic Communications and Transactions Act (ECTA), 2002, *South Africa Government Gazette* 446(23708), 1–41.

Eze, S.G. & Chijioke, E.O., 2016, 'Public enlightenment education on the acceptance of fingerprint biometric technologies for administration in academic institutions and other organisations', *Journal of Education and Practice* 7(28), 158–163.

Frank, M., Biedert, R., Ma, E., Martinovic, I. & Song, D., 2012, 'Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication', *IEEE transactions on information forensics and security* 8(1), 136–148.

Furnell, S. & Evangelatos, K., 2007, 'Public awareness and perceptions of biometrics', *Computer Fraud & Security* 2007(1), 8–13. https://doi.org/10.1016/S1361-3723(07)70006-4

Galton, F., 1901, 'Biometry', *Biometrika* 1, 7–10. https://doi.org/10.1093/biomet/1.1.7

Gomez-Barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A. et al., 2021, 'Biometrics in the era of COVID-19: Challenges and opportunities', *arXiv preprint arXiv:2102.09258*, 1–14.

Gunson, N., Marshall, D., Morton, H. & Jack, M., 2011, 'User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking', *Computers & Security* 30(4), 208–220.

Hosseini, S.S. & Mohammadi, S., 2012, 'Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system', *Journal of Basic and Applied Scientific Research* 2(9), 9152–9160.

Jain, A., Hong, L. & Pankanti, S., 2000, 'Biometric identification', *Communications of the ACM* 43(2), 90–98. https://doi.org/10.1145/328236.328110

Jain, A.K., Flynn, P. & Ross, A., 2007, *Handbook of biometrics*, pp. 1–556, Springer Science & Business Media, New York.

Jain, A.K. & Kumar, A., 2010, 'Biometrics of next generation: An overview', *Second Generation Biometrics* 12(1), 2–3.

Jain, A.K., Ross, A. & Pankanti, S., 2006, 'Biometrics: A tool for information security', *IEEE Transactions on Information Forensics and Security* 1(2), 125–143.

Jaiswal, A.M. & Bartere, M., 2014, 'Enhancing ATM security using fingerprint and GSM technology', *International Journal of Computer Science and Mobile Computing (IJCSMC)* 3(4), 28–32.

Jin, C., Kim, H. & Elliott, S., 2007, 'Liveness detection of fingerprint based on band-selective Fourier spectrum', in *International Conference on Information Security and Cryptology*, Springer, Berlin, Heidelberg, pp. 168–179.

Johnson, A., 2019, 'How biometrics (and blockchain) could save bricks-and-mortar retail', *Biometric Technologies Today* 3, 8–10. https://doi.org/10.1016/S0969-4765(19)30040-2

Kelman, J., 2016, *The history of banking: A comprehensive reference source & guide*, pp. 1–384, CreateSpace Independent Publishing Platform, California,

Kim, S., 2007, 'Governance of information security: New paradigm of security management', in *Computational intelligence in information assurance and security*, pp. 235–254, Springer, Berlin.

Koppenhaver, K.M., 2007, *Forensic document examination: Principles and practice*, pp. 1–389, Springer Science & Business Media, New Jersey.

Kristensen, L.B.K. & Solvoll, M., 2019, 'Digital payments for a digital generation', *Nordic Journal of Media Studies* 1(1), 125–136.

Lee, T., 2016, *Biometrics and disability rights: legal compliance in biometric identification programs*, U. Ill. JL Tech. & Pol'y, p. 209.

Legner, C.T., Eymann, T., Hess, C., Matt, T., Böhmann, P., Drews, A. et al., 2017, 'Digitalization: Opportunity and challenge for the business and information systems engineering community', *Business & Information Systems Engineering* 59(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

Liang, Y., Samtani, S., Guo, B. & Yu, Z., 2020, 'Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective', *IEEE Internet of Things Journal* 7(9), 9128–9143. https://doi.org/10.1109/JIOT.2020.3004077

Lowrence, D., 2014, 'Biometrics and retail: Moving towards the future', *Biometric Technologies Today* 2014(2), 7–9. https://doi.org/10.1016/S0969-4765(14)70032-3

Maguire, M., 2009, 'The birth of biometric security', *Anthropology Today* 25(2), 9–14. https://doi.org/10.1111/j.1467-8322.2009.00654.x

Mahfouz, A., Mahmoud, T.M. & Eldin, A.S., 2017, 'A survey on behavioral biometric authentication on smartphones', *Journal of Information Security and Applications* 37, 28–37. https://doi.org/10.1016/j.jisa.2017.10.002

Mallat, N., Rossi, M. & Tuunainen, V.K., 2004, 'Mobile banking services', *Communications of the ACM* 47(5), 42–46. https://doi.org/10.1145/986213.986236

Mansfield-Devine, S., 2013, 'Biometrics in retail', *Biometric Technologies Today* 2013(9), 5–8. https://doi.org/10.1016/S0969-4765(13)70161-9

Mir, G.M., Balkhi, A.A., Lala, N.A., Sofi, N.A., Kirmani, M.M. & Mir, I.A., 2018, 'The benefits of implementation of biometric attendance system', *Oriental Journal of Computer Science and Technology* 11(1), 50–54. https://doi.org/10.13005/ojcst11.01.09

Neumeier, A., Wolf, T., & Oesterle, S. 2017, 'The Manifold Fruits of Digitalization - Determining the Literal Value Behind', in St. Gallen, J.M. Leimeister & W. Brenner (eds.), *Proceedings der 13*, Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, pp. 484–498.

Pacut, A. & Czajka, A., 2006, 'Aliveness detection for iris biometrics', in *Proceedings 40th annual 2006 international carnahan conference on security technology,* IEEE, pp. 122–129.

Pallant, J., 2020, *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*, Routledge, London.

Park, R.C., 2008, 'Signature identification in the light of science and experience', *Hastings LJ* 59, 1101.

Petrlic, R. & Sorge, C., 2013, 'Establishing user trust in automated teller machine integrity', *IET Information Security* 8(2), 132–139. https://doi.org/10.1049/iet-ifs.2012.0220

Prabhakar, S., Pankanti, S. & Jain, A.K., 2003, 'Biometric recognition: Security and privacy concerns', *IEEE Security & Privacy* 2, 33–42. https://doi.org/10.1109/MSECP.2003.1193209

Priesnitz, J., Rathgeb, C., Buchmann, N., Busch, C. & Margraf, M., 2021, 'An overview of touchless 2D fingerprint recognition', *EURASIP Journal on Image and Video Processing* 2021(1), 1–28. https://doi.org/10.1186/s13640-021-00548-4

Rahman, M.R. and Safeena, P.K., 2016, 'Customer Needs and Customer Satisfaction', In Ramees Rahman (eds.), *book: Theeranaipunya - A Capacity Building Training Programme Equipping the Fisher women Youth for the Future*, Central Marine Fisheries Research Institute, pp. 259–262, Kochi, India.

Rattani, A. & Derakhshani, R., 2018, 'A survey of mobile face biometrics', *Computers & Electrical Engineering* 72, 39–52.

Rhodes, K.A., 2003, *Information security: Challenges in using biometrics*, General Accounting OfficeTechnical Report # GAO-03-1137T.

Saunders, M., Lewis, P. & Thornhill, A. 2019, *Research methods for business students*, 8th edn., Pearson Education Limited, Harlow.

Sukamolson, S., 2000, *Conducting and developing a multimedia computer-assisted instruction program for teaching Foundation English IIII*, Chulalongkorn University, Language Institute.

Sun, Y., Zhang, M., Sun, Z. & Tan, T., 2017, 'Demographic analysis from biometric data: Achievements, challenges, and new frontiers', *IEEE transactions on pattern analysis and machine intelligence* 40(2), 332–351.

Syler, R. & Baker, E., 2016, *Building a framework for the influence of digital content on student course engagement*.

Tan, X., Li, Y., Liu, J. & Jiang, L., 2010, 'Face liveness detection from a single image with sparse low rank bilinear discriminative model', in *European Conference on Computer Vision*, Springer, Berlin, Heidelberg, pp. 504–517.

Ten Have, H. & Gordijn, B. (eds.), 2014, *Handbook of global bioethics*, vol. 4, Springer, New York, NY.

Toth, B., 2005, 'Biometrics. Biometric Liveness Detection', *Information Security Bulletin* 10, 291–297.

Varga, D., 2017, 'Fintech, the new era of financial services', *Vezetéstudomány/Budapest Management Review* 48, 22–32. https://doi.org/10.14267/VEZTUD.2017.11.03

Venkatraman, S. & Delpachitra, I., 2008, 'Biometrics in banking security: A case study', *Information Management & Computer Security* 16(4), 415–430. https://doi.org/10.1108/09685220810908813

Wang, N., Ching, P.C., Zheng, N. & Lee, T., 2011, 'Robust speaker recognition using denoised vocal source and vocal tract features', *IEEE Transactions on Audio, Speech, and Language Processing* 19(1), 196–205. https://doi.org/10.1109/TASL.2010.2045800

World Health Organization, n.d., *Coronavirus disease (COVID-19) pandemic*, viewed 16 September 2021, from https://www.who.int/emergencies/diseases/novel-coronavirus-2019.

Wayman, J.L., Jain, A.K., Maltoni, D. & Maio, D. (eds.), 2005, *Biometric systems: Technology, design and performance evaluation*, Springer Science & Business Media, London, United Kingdom.

Zhu, Y., Tan, T. & Wang, Y., 2000, 'Biometric personal identification based on iris patterns', in *Proceedings 15th International conference on pattern recognition*, ICPR-2000, vol. 2, pp. 801–804, IEEE.

Appendix 1 starts on the next page→

Appendix 1

TABLE 1-A1: Pearson correlations results of biometric challenges and benefits.

Variables	Hackers	Scammers	Fraudsters	Signature authentication forgery	Lack of guidance for interacting with the system	Dust dropped on the fingerprint scanner	Poor human machine interactions	Any form of change in the user's finger	Involvement in accident	Sensitivity of sensor performance	Non-technologically inclined individuals	Fake fingerprint forgery	Biometric characteristics	Biometric information leakage
Enhanced surveillance														
Pearson's correlation	-0.004	-0.019	0.007	0.038	0.094	-0.003	0.013	0.141	0.216**	0.202**	0.094	0.109	0.220**	0.024
Sig. (2-tailed)	-0.963	0.803	0.929	0.620	0.220	0.973	0.867	0.064	0.004	0.008	0.220	0.153	0.004	0.752
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Enhanced Border control														
Pearson's correlation	-0.033	-0.053	-0.020	-0.094	-0.014	0.026	0.032	0.129	0.253**	0.205**	0.142	0.147	0.150*	0.094
Sig. (2-tailed)	0.669	0.491	0.792	0.220	0.850	0.732	0.680	0.091	0.001	0.007	0.063	0.053	0.048	0.217
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Criminal identification														
Pearson's correlation	0.009	-0.008	-0.008	0.048	0.008	0.012	-0.063	0.019	0.140	0.181*	0.061	0.063	0.163*	0.054
Sig. (2-tailed)	0.903	0.921	0.917	0.533	0.915	0.876	0.414	0.806	0.067	0.017	0.427	0.407	0.032	0.482
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Ease of information retrieval														
Pearson's correlation	0.040	0.054	0.090	0.050	0.046	0.115	0.019	0.076	0.186*	0.106	0.127	0.121	0.224**	0.110
Sig. (2-tailed)	0.604	0.484	0.237	0.514	0.545	0.132	0.806	0.321	0.014	0.165	0.096	0.114	0.003	0.151
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Strong matching algorithm														
Pearson's correlation	-0.036	-0.076	0.015	0.027	0.056	0.104	0.042	0.080	0.181*	0.204**	0.200**	0.055	0.146	0.089
Sig. (2-tailed)	0.636	0.322	0.841	0.720	0.465	0.175	0.582	0.295	0.017	0.007	0.008	0.472	0.055	0.242
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Lost or stolen Smartcards and mobile devices														
Pearson's correlation	0.134	0.188*	0.224**	0.076	0.145	0.094	0.076	0.046	0.102	0.076	0.214**	0.026	0.094	0.055
Sig. (2-tailed)	0.080	0.013	0.003	0.323	0.057	0.217	0.322	0.544	0.180	0.318	0.005	0.733	0.219	0.473
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Impossible to forget Fingerprint authentication														
Pearson's correlation	-0.032	0.093	0.118	0.101	0.144	0.042	0.087	0.011	0.085	0.062	0.187*	0.022	0.155*	−0.020
Sig. (2-tailed)	0.679	0.225	0.123	0.186	0.058	0.587	0.255	0.890	0.268	0.420	0.014	0.776	0.041	0.790
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Uniqueness														
Pearson's correlation	0.030	0.090	0.097	0.117	0.133	0.138	0.007	0.028	0.194*	0.155*	0.247**	0.099	0.235**	0.039
Sig. (2-tailed)	0.698	0.240	0.205	0.124	0.082	0.071	0.928	0.716	0.011	0.042	0.001	0.194	0.002	0.614
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173
Forensic application														
Pearson's correlation	-0.020	0.052	0.073	0.096	0.146	0.185*	-0.010	0.081	0.236**	0.278**	0.273**	0.153*	0.142	0.037
Sig. (2-tailed)	0.793	0.497	0.341	0.209	0.055	0.015	0.892	0.288	0.002	0.000	0.000	0.045	0.063	0.626
N	173	173	173	173	173	173	173	173	173	173	173	173	173	173

*, Correlation is significant at the 0.05 level (2-tailed).

**, Correlation is significant at the 0.01 level (2-tailed).