This paper was presented at the 21st International Conference on Sustainable Development, held at the Faculty of Social Science and Humanities, University of Ottawa, Ottawa, Canada, on July 15-16, 2025.

An Exploration of Biometrics Payment Technology to Combat Online Banking Fraud and Digital Identity in the South African Banking Industry

Mokopane Charles Marakalala
College of Law, School of Criminal Justice/Law Department of Police Practice,
University of South Africa, Preller Street, Muckleneuk Ridge, Pretoria, South Africa.
Corresponding author: Marakmc@unisa.ac.za

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: The biometrics payment technology to combat online banking fraud and digital identity is offered by the South African Banking Industry to give its clients quick and simple access to banking services. Nowadays, the majority of banking services are done online, which leads to concerning fraud every day. The frequency and severity of online banking fraud and digital identity are rising worldwide, and they harm both banks and consumers. Investigating problems with online fraud detection in South Africa banking industry was the aim of the study. In the South African context, the study found that the banking industry lacks specialists in online banking fraud and digital identity. The results show that banks' detection systems may be inadequate due to a lack of experience with online banking fraud and digital identity. From a South African standpoint, the study found that there is a high risk due to a lack of legal regulation. Banks are encouraged to acquire and develop online banking fraud and digital identity expertise because the banking industry lacks these specialists. Since online banking technology is advancing more quickly than traditional transactions, rules and guidelines must be updated frequently to reflect the swift advancements in technology. Given the importance of international online banking, the study made recommendations for potential research topics that the banking industry could look into in order to create and improve online fraud detection models and stop online fraud. To achieve the study's goals, a literature analysis was used, and secondary data was evaluated and deconstructed. This paper major goal was to look at the causes and motivations behind online banking fraud and digital identity. The study made recommendations for potential research topics that the South Africa communities could look into in order to create and improve online banking fraud and digital identity.

Keywords: Biometric, Payments, Technology, Combat, Online Banking, Fraud, Digital Identity

Introduction

This article looks at case studies from around the globe, investigates new and developing fraud trends in digital banking (both domestically and internationally), and evaluates the technical and strategic measures that banks and regulators can take to prevent fraud. The objective is to draw attention to innovative tactics, such as AI-driven analytics and customer education, that could help South Africa's digital banking industry grow even more quickly than Capitec has in the past while maintaining security and trust. The development of biometrics dates back to the 19th century, when its primary goal was to secure people's identities by learning about their physical characteristics (INTERPOL, 2020:np). In the past, biometrics was mostly used in high-security settings. Currently, though, it is used in a greater range of public-facing applications, such as in prisons, by law enforcement for the purpose of verifying driver's licenses, managing canteens, payment systems, and border control for verification, including electoral systems (Botta, Nadeau, Bruno, Tayar & Chaudhuri, 2020:17) Passwords and security pin codes are examples of older forms of identification that have been replaced by biometrics as the primary security technology since the late 1990s. In the beginning, biometrics was used to assess an individual's behavioral and physical characteristics. ATM use, workplace authentication, network access, travel and tourism, internet connections, and mobile connections are among the upcoming applications for biometric verification.

The impact of biometrics in South African banking and retail has not received as much attention in recent years as studies on digital banking, financial technology, and other topics. Digital information is information that has been separated from physical data storage to its technical potential. Collaboration, sharing, co-creation, connectivity, communication, mobility, and flexibility are some of the traits that define digitization. In order to develop the identified needs for the first online connected catalogues and inventory software systems, digital networks began to connect retailers with traders, clients, and customers. Botta *et al.,* (2020:21) indicated that the transition to online banking and the digitization of all antiquated banking operations, including plans that were previously available to bank customers and required in-person visits, are referred to as digital banking. Digital banking has facilitated customers to overcome controlled time banking and local area operations (INTERPOL, 2020:np). Digital banks use advanced banking systems that can swiftly implement new services allowing for seamless mobility for bank users.

The demand for more creative and safe banking systems that allow clients to access their funds at any time and from any location is the primary issue with this study. Botta *et al.,* (2020:26) mentioned that with the advent of the fourth industrial revolution (4IR) and the need for banking sectors to undergo change, technological advancements have given financial institutions greater access to opportunities. On the other hand, a lot of financial institutions have adapted to operate using the conventional digital banking platforms. Customers can manage their accounts, make deposits, withdrawals, and transfers using this digital banking platform without having to go to the bank in person. Nevertheless, none of these banking industries have been able to fully utilize the 4IR's potential and potential for a more creative and straightforward.

Only a small number of studies have examined biometric banking and payment systems. In order to close the gap, this study aims to assess the creative and safe ways to use biometrics to access money and pay for goods at retail establishments without actually having a bank card or hard cash. INTERPOL (2020:np) stated that as an alternate method of authentication for mobile baking transactions like bank transfers and payments, the study focuses on biometrics in digital banking and financial technology. Conventional password authentication is still used in current authentication methods. Additionally, this article aims to educate banks and retailers about the importance of biometrics as a crucial mechanism in providing a quick, safe, adaptable, and creative authentication process to safeguard customers' funds 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 (Botta *et al.,* 2020:33). Section Challenges of biometrics covers the research problem that this research study attempts to address. Section Research method and design discusses the research methodology.

Literature review

Biometric payment technology in the South African Banking Industry (SABI). A systematic review, also known as a systematic literature review, is a type of literature review that employs structured methods to gather secondary data, critically evaluate research studies, and synthesize the findings either qualitatively or quantitatively. Kumar (2021:55) and Leavy (2022:78) emphasized that systematic reviews develop research questions that can be either broad or narrow in focus and identify and combine studies that are directly relevant to the review question. These reviews aim to provide a thorough, exhaustive summary of existing evidence both published and unpublished that is methodical, comprehensive, transparent, and reproducible.

Having a clear understanding of systematic reviews and how to apply them in practice is highly recommended for professionals working in healthcare delivery, public health, and public policy. Systematic reviews of randomized controlled trials are fundamental to evidence-based medicine, and reviewing existing studies is often faster and more cost-effective than conducting new research (Creswell, 2020:22). In contrast, systematic reviews of observational studies are considered lower in the evidence hierarchy. Nevertheless, the quality of evidence is also significantly influenced by the precision of the methodological design and the execution of the systematic review by the researchers.

While systematic reviews are often applied in the biomedical context, they can be used in other areas where an assessment of a precisely defined subject would be helpful. For example, systematic reviews are becoming increasingly common in management, accounting and finance. Systematic reviews may examine clinical tests, SABI interventions, environmental interventions, social interventions, adverse effects and economic evaluations.

Results and Discussion

Global Fraud Trends in Digital Banking

The rise of digital banking is a double-edged sword globally. While convenience and accessibility have improved, cybercriminals have seized new opportunities. In 2024, attempted digital payment fraud across Europe rose by 43% compared to the previous year, with social engineering attacks (including phishing and deepfake scams) increasing by 156% ((INTERPOL, 2020:np).

In the Asia-Pacific region, APP (Authorised Push Payment) fraud and voice phishing scams surged by 200% between 2022 and 2023 (INTERPOL, 2020:np). These scams exploit human trust rather than technical vulnerabilities, underscoring the importance of customer awareness and system-level protections.

In North America, mobile banking usage reached a record high in 2023 with 73% of customers transacting via mobile apps. This growth was accompanied by a 61% spike in mobile fraud incidents (INTERPOL, 2020:np). Fraudsters increasingly use mobile device emulators and malware to bypass traditional security layers, demonstrating the evolving tactics of cybercrime.

Paradoxically, as banks harden defenses on digital channels, criminals often revert to legacy systems. In the U.S., check fraud and deposit scams have resurfaced as attackers exploit vulnerabilities in traditional banking processes (INTERPOL, 2020:np).

What’s clear is that digital fraud is borderless – criminal networks are organized, agile, and often operate across jurisdictions using shared tools and infrastructure (INTERPOL, 2020:np).

South Africa’s Digital Banking Fraud Landscape

South Africa has experienced a rapid digital shift in banking, but this growth has also drawn the attention of cybercriminals. The country now ranks fifth globally in cybercrime density (Skinner, 2014:58). According to the South African Banking Risk Information Center (SABRIC), digital banking fraud increased by 45% year-on-year in 2023, with financial losses rising by 47%. Mobile banking app fraud alone rose by 89%, making it the most prevalent attack vector (Skinner, 2014:58).

One major concern is the combination of device theft and digital exploitation. With an average of 189 smartphones stolen daily in South Africa, criminals frequently gain access to unlocked devices or socially engineer entry. Once inside, they can retrieve saved passwords, authenticate with biometrics, and initiate unauthorized transactions before victims even notice the breach (Skinner, 2014:66).

SIM-swap fraud is another critical threat. By fraudulently porting a victim’s mobile number, criminals intercept one-time PINs (OTPs) and other security alerts. Balkan (2021.37) indicated that despite ongoing collaboration between banks and telecom providers, SIM-swap attacks continue to undermine SMS-based two-factor authentication (INTERPOL, 2020:np). Phishing and Vishing remain widespread. South Africans lost an estimated R200 million to phishing scams in 2023; an increase of over 50% from the previous year. In a high-profile case, PRASA, the state-owned rail operator, lost R30 million to a compromised email account (Skinner, 2014:48).

In addition to traditional fraud tactics, AI-driven schemes are emerging. Criminals are using deepfake voice and video technologies to impersonate executives and deceive employees or customers into authorizing transfers. Alarmingly, 80% of South Africans surveyed indicated they cannot reliably distinguish between AI-generated and real images (Skinner, 2014:48). These challenges underscore that South Africa’s fraud environment is both technologically advanced and deeply human-centric. With many newly digitized users in the financial ecosystem, banks must balance innovation with robust and accessible fraud prevention mechanisms.

Global Case Studies: Lessons from Digital Banking Fraud

SABI Authorized Push Payment (APP) Scams: SABI consumers suffered losses of around R485 million due to APP scams within one year. These schemes frequently entail con artists masquerading as bank representatives or service providers, deceiving people into carrying out transfers on their own. In reaction, SABI regulators established confirmation-of-payee systems and are currently mandating banks to reimburse victims under certain conditions (Skinner, 2014:40).

Account Takeovers and Mobile Payment Scams: As peer-to-peer applications such as Zelle and CashApp expanded, American banks experienced a notable increase in account takeover scams. In numerous instances, cybercriminals utilized mobile device emulators to seize user sessions and divert money from victims' accounts. This resulted in over a 60% rise in mobile fraud cases, even with heightened security spending (Balkan (2021.39).

Scam Call Centers and Social Engineering in the Asia-Pacific: Nations such as Cambodia and Myanmar have witnessed the rise of scam call centers run by organized crime syndicates. Victims receive phishing calls, frequently utilizing deepfake voices or impersonated support agents, persuading them to provide login information or approve transactions (Balkan (2021.35).

Australia's real-time payment system (NPP) allows quicker transactions while also introducing new risks. Australian banks have implemented real-time fraud detection systems that track transaction speed, behavioral trends, and device fingerprints to quickly stop suspicious payments (Skinner, 2014:41). Every one of these case studies provides insight into finding a balance between speed and security, illustrating how collaborative regulatory and banking actions can greatly diminish the extent and effects of fraud.

South African Banks in Focus: Discovery, TymeBank, and FNB

Discovery Bank Premium Digital Approach: As a digitally focused, upscale entity, Discovery Bank serves a wealthy, tech-oriented clientele. The bank sets itself apart by connecting banking to lifestyle rewards and wellness benefits (INTERPOL, 2020:np). Nonetheless, this segment is also a primary target for fraudsters because of elevated account values. Discovery has introduced multiple groundbreaking fraud prevention measures:

- Concealed account balances: Users have the option to conceal significant accounts within the app for increased privacy.
- Monitoring powered by AI: Behavioral analytics assist in identifying unusual behavior even when valid login credentials are utilized.
- Security alerts within the app: Discovery identifies immediate fraud alerts, like notifying users when they get a call while using the app, which may indicate a vishing attempt (INTERPOL, 2020:np).

Discovery's CEO emphasized that fraud is shifting to the client's device, meaning client empowerment and proactive tooling are now central to fraud strategy ((INTERPOL, 2020:np)**.**

TymeBank's Affordable Digital-Only Strategy: TymeBank's approach emphasizes scale, straightforwardness, and accessibility. Lacking physical branches and serving more than 10 million clients, its value offering is grounded in cost-effective banking through kiosks, smartphones, and retail affiliates. This model requires fraud controls that are highly automated and scalable:

- Biometric sign-ins (fingerprint, facial recognition) are encouraged to lessen reliance on passwords and OTPs.
- Instant onboarding verifications utilize South Africa's national ID database to authenticate new users and thwart synthetic identity fraud.
- Educating customers is crucial: TymeBank utilizes Emails, SMS notifications, and app alerts to inform users about emerging scam strategies (TymeBank).
- Simplicity as a safeguard: Providing straightforward, comprehensible banking services minimizes attack surfaces and aids customers in identifying irregularities.

SABI Customer perspectives

A customer can be defined as a stakeholder of an organization who offers payment in return for goods or services. Moreover, a customer can be identified not just as an individual but also as an entity (e.g., university, bank, construction firm, school, law office, and hospital) that purchases products and services from various vendors. Businesses (banks and retailers) must recognize that clients have diverse job backgrounds. Customers are increasingly conducting more banking and financial transactions online, which has led fraudsters to adopt more advanced methods of attack (INTERPOL, 2020:np). As the threat of digital fraud and theft rises, numerous organizations have sought solutions to prevent fraudsters from executing increasingly sophisticated attacks. Traditional security measures like passwords, PINs, and ID cards are ineffective at preventing the surge of transaction scams and security breaches, making digital banking solutions an ideal way to counter these risks. Relying solely on pin code verification cannot be considered a robust defense against security breaches. By utilizing digital banking solutions, the operator's data or information is safely stored within an encrypted container or sandbox.

Digital Identity 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. 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. INTERPOL (2020:np) highlighted that 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. 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.

The use of biometrics in banks is prevalent in developed nations, leading to a significant increase in the adoption of biometrics. Balkan (2021.41). There is no doubt that biometrics are increasing in importance for banking security; identifying authentication through biometric applications is significantly more secure than password authentication. Biometric authentication is now being integrated into physical payment cards; biometrics are increasingly utilized for account access, even substituting debit cards at ATMs. Biometrics offers a significantly more dependable and effective means of verification compared to solely depending on human agents. The principles of security and efficiency associated with biometrics render its adoption appealing to banks globally. As the typical banking customer handles a wider array of financial transactions online via desktops and mobile devices, the demand for straightforward yet secure access to their banking information is increasingly a primary focus for banking service providers aiming to stand out from direct competitors. With the growth of the digital era, banks must find a balance between security and accessibility (Balkan, 2021.41).

Prominent banks in South Africa are ABSA, FNB, Nedbank, Standard Bank, and Capitec. This relies on their income production, extensive customer base, services and products they provide, and marketing tactics they implement. If the South African banking industry fails to effectively implement and adapt e-banking, many banks will find it difficult to operate at an optimal level while adapting to the 4IR and FinTech. Companies have recognized the growing significance of digitization in fostering business growth.

Challenges of biometrics

Biometric issues can adversely affect individuals and companies or clients and institutions. Bank crises and failures are increasingly linked to the rising prevalence of scammers and fraudsters (Bhasin 2015). Fraud is viewed as a worldwide issue that adversely affects all areas of the economy (Wewege, Lee, & Thomsett, 2020:17). A swift rise in security vulnerabilities and transaction breaches in conventional security systems like PINs and passwords is quickly driving the development of robust biometric authentication techniques. Biometric advantages can affect individuals as well as companies or clients and institutions. Furthermore, biometrics can be seen as a faster way to trace and recover information compared to manual or traditional verification procedures performed at the counter.

The Challenges Facing Biometric Authentication

While biometric authentication has grown in popularity in recent years, the field faces many challenges that will need to be addressed as the technology continues to develop.

Implicit Biases

Numerous human rights defenders have noted that certain biometric authentication techniques exhibit concerning and fundamentally flawed implicit biases. Facial recognition technology utilizes existing data sets that can harbor inherent racism or gender bias, thereby mirroring these problems. The datasets typically show images that are 77% male and 83% white, which represents a significant distortion of the overall demographics of any nation (South African Banking Risk Information Centre [SABRIC], 2020:np). Transgender and gender non-binary people can be inaccurately classified by biological identification methods. There have been troubling incidents where facial recognition systems have failed to recognize Asian or African American individuals or have misidentified them. Balkan (2021.38). In the UK, for instance, Uber has adopted a policy that employs facial recognition technology to recognize its drivers. Every Uber driver must undergo security and verification procedures; however, due to this policy, Transport for London (TFL) has canceled drivers' licenses based on negative recognition outcomes linked to the fact that these drivers have brown skin.

Privacy Concerns

Numerous security watchdogs have expressed significant worries regarding the extensive data gathered without consent by governmental bodies and public organizations during biometric authentication procedures. Many contend that people should retain the right to privacy regarding their image and should not be obligated to supply their facial characteristics or other biometric information for inclusion in government databases. Safety represents an additional area of worry (Balkan, 2021.35) These massive repositories of biometric data present appealing targets for malicious individuals aiming to cause widespread disruption. Should hackers infiltrate biometric data repositories, they could effortlessly undermine secure systems and launch extensive fraud and identity theft operations. Encryption techniques are employed to thwart such attacks, yet significant concerns persist regarding the safety of substantial sensitive biometric information.

Physical Alterations

When only a single form of biometric authentication is employed to grant access to certain apps, devices, documents, or locations, individuals risk losing entry to these secured areas if an event occurs that changes their physical traits. People involved in an accident that alters their facial characteristics may not be identifiable by the biometric database analysts, potentially leading to them being unable to access their accounts (Balkan, 2021:36). Likewise, if an individual sustains serious burns on their hands, their fingerprints might become unreadable to the scanners, preventing them from accessing their accounts. Consequently, using a mix of authentication factors is essential for any safe account.

Final Thoughts

Despite offering a straightforward and highly secure method for identity verification, biometric authentication encounters numerous challenges. As technology advances and organizations of all types adopt this approach to user validation, there are undoubtedly challenges that must be tackled (Balkan, 2021:37). Developers must implement adjustments to eliminate implicit biases from the system, fostering a more inclusive dataset that prevents the misclassification of dark-skinned or transgender individuals. Governments or agencies that safeguard human rights must develop regulations regarding the types of information gathered by whom and guarantee that individuals possess the right to grant or withdraw consent concerning the collection of their biometric data. However, due to these regulations and technological advancements, we can anticipate biometric authentication methods proliferating into additional facets of our daily existence.

Multi-factor authentication methods

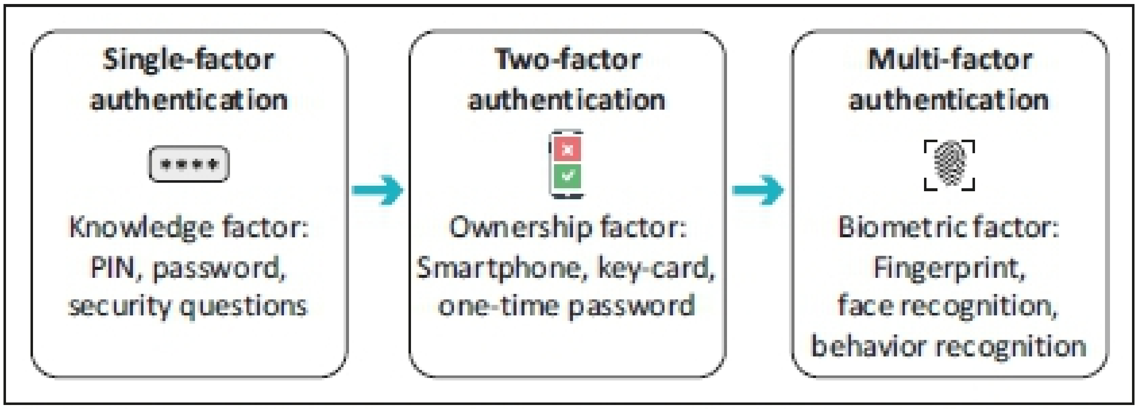
Utilizing a password (or PIN) to verify the possession of the user ID may be viewed as a single-factor authentication (SFA) technique (Open Data Charter, 2018:np). Clearly, this represents the most inadequate form of authentication (Ombudsman for Banking Services). I'm sorry, but you didn't provide any text to paraphrase. Please provide the text you would like me to paraphrase.

Single-factor authentication is insufficient for adequate protection due to various security threats, including rainbow table and dictionary attacks (Pieter, 2022:np). Methods of two-factor authentication (2FA) involve an item the user possesses, like cards, smartphones, or various tokens (PricewaterhouseCoopers, 2019:np). Multi-factor authentication (MFA) techniques include something that the user/customer embodies, particularly biometric information or behavioral patterns like fingerprints, facial recognition, behavior recognition, and more (Kruse, 2015:78).

The demand for a dependable user authentication method has risen due to heightened security concerns and the swift progress in communication, mobility, and networking (Patel, 2023:np). Often, MFA relies on biometrics, which involves the automated identification of individuals through their behavioral and biological traits (SABRIC, 2020:np). The challenges and benefits of biometrics will be explored in detail, as this method is regarded as a crucial aspect of MFA.

Next page

Figure 1: Shows the evolution from SFA factor MFA


Single-factor authentication
****
Knowledge factor: PIN, password, security questions
Two-factor authentication
Ownership factor: Smartphone, key-card, one-time password
Multi-factor authentication
Biometric factor: Fingerprint, face recognition, behavior recognition

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.

Types of biometric technology use cases

Currently, there is a vast array of applications and services that leverage biometric technology (James & Nordby, 2018 :120). Here are several typical ways individuals engage with physiological and behavioral biometrics in their everyday routines:

- Personal devices - Smartphones, laptops, desktops, and tablets frequently support fingerprint or facial recognition for device access.
- Financial transactions - Payments such as wire transfers often necessitate identity confirmation via biometrics and/or cloud-based biometrics for secure access.
- Healthcare - Biometric authentication enables healthcare professionals to securely handle patient records and avert unauthorized entry to confidential information.
- Airports - Numerous contemporary airports utilize facial recognition to accelerate passenger handling. Travelers can sign up by getting a picture of their eyes and face taken, enabling quicker passage through lines.
- Entertainment locations – Stadiums and various sites are starting to provide ticketless entry through facial recognition technology.
- Ensured physical entry – Biometrics are taking the place of key cards and PIN codes as a safer and more traceable method to grant access to secured locations or sections within buildings.

As stated by Kruse (2015:56), biometric authentication and verification are now essential components of contemporary technology. Nonetheless, as its utilization grows in different sectors, worries regarding safety and privacy remain. Users frequently inquire, "What occurs if my biometric information is breached?". Although passwords can be changed, biometric characteristics are immutable, highlighting the importance of strong data security protocols like liveness detection (Pieter, 2022:np). If breached, these templates can't be reverse engineered and are not accessible to fraudsters

Advantages of biometric authentication

High security and assurance

Biometrics enhances security and guarantees an individual's authenticity by confirming their distinct physiological or behavioral traits. According to PricewaterhouseCooper (2019:np), it has become more frequent for users' passwords, PINs, and personal identification information to be exposed due to data breaches, allowing fraudsters easier access to the information required to bypass conventional authentication methods. Incorporating biometric authentication into the procedure creates a barrier for fraudsters that can only be bypassed by an actual, authorized user although a fraudster might be aware that someone uses their pet's name and a few lucky numbers across many of their online accounts (Patel, 2023:np). They are unable to use their face to access an account particularly with liveness safeguards in place to verify the actual presence of the legitimate account holder

User experience is convenient and fast with biometrics

Although the technology underlying biometric authentication is complex, it is remarkably simple and fast from the user's perspective (Balkan (2021:38). Unlocking an account instantly with biometrics is quicker than entering a lengthy password filled with various special characters or waiting for a PIN through email or SMS. Moreover, forgetting a password is a common issue and a source of frustration for users

Non-transferable

Biometric authentication necessitates that its input is available during the authentication process. It cannot digitally transfer or share a physical biometric – the sole method to use most biometric authentication systems is through a physical application. In contrast to passwords, PINs, and responses to security queries, biometrics stand out because they cannot be shared – whether deliberately or unintentionally (like sharing streaming credentials with a family member or a login with a colleague). Biometric authentication guarantees the correct individual

Near spoof-proof

Biometrics, such face and voice, are very hard to fake (Lynch, 2020:78). Modern face recognition algorithms are created to identify traits that are very specific and may attain accuracy. In optimal circumstances, the rate exceeds 99.97%, and in such systems, the probability of two unrelated people sharing identical facial templates is extremely improbable. In reality, lightning is statistically more likely to hit you than for someone else to unlock your account.

Flexible and scalable

A cloud-based biometric system has the capacity to expand and contract in response to changes in user demand. In contrast to on-device biometric systems, which are restricted to a single user due to the capabilities and connectivity of the physical device. Moreover, solutions may be implemented across apps, channels, and locations with ease and speed (Lynch, 2020:78).

Disadvantages of biometric authentication

Costs

As would be expected, implementing a more sophisticated security system would involve considerable expenditures and expenses. According to a Spiceworks study conducted in 2018, 67% of IT experts named cost as "the biggest reason" for not implementing biometric authentication (Lynch, 2020:79). Changing With 47% of respondents expressing a demand for biometrics authentication, a firm would have to pay for more than just that. Improve existing systems to facilitate the move to biometric identification on their devices.

Data breaches

The personal information of users that is collected and stored by governments and businesses is always at risk from hackers (Balkan (2021:35). Because biometric data cannot be replaced, organizations must handle sensitive biometric data with greater security and care, which is a costly and technically challenging effort to keep up with fraud developments. In the event that a password or pin is compromised, you may always alter it. The same is not true for a person's behavioral or physiological biometrics.

Data privacy

The privacy of users must be taken into account as the world increases its use of biometric authentication methods such facial recognition technology and other biometric security measures. Balkan (2021:41). stated that work with a provider who is knowledgeable about industry standards and best practices, such as using industry-standard methods to safeguard consumer data while it is being transmitted and at rest. establishing templates to prevent reverse engineering, using enterprise-grade encryption and security methods, maintaining templates apart from the consumer's personally identifying information, and adhering to global standards legislation on data protection at the national and state levels (GDPR).

Minimizing bias

The design of biometric technology, especially its lack of algorithmic inclusivity and bias in, can lead to discrimination. Biometric technology is not inherently biased. bias in performance indicators and feature selection. Find technology that a biometrics lab accredited by NIST NVLAP has confirmed to be fair.

False positives and false negatives

In biometrics, a false positive occurs when the system mistakenly allows an unauthorized person access. In ideal circumstances, NIST experiments have revealed false match rates for faces as low as 0.0001%. However, issues such as bad lighting, facial obstructions, or large shifts in appearance may cause the inability to identify legitimate users (false negatives) to rise. Secondary authentication techniques, such an extra biometric modality or another verification factor, can be used by firms to mitigate these issues, improving both reliability and security.

The way we protect systems and data is changing thanks to biometric identification. It is necessary to discuss its drawbacks, especially in terms of cost and privacy, even if its benefits in security and ease are obvious. By keeping up with current developments and embracing new innovations, businesses may utilize the complete capabilities of biometric technology. Biometric authentication has become a key component of contemporary security systems since it offers the potential to replace traditional passwords with something that is more secure and practical—our individual biological traits. Biometric technology is quickly changing how we confirm identity, from fingerprint readers on smartphones to facial recognition at airports. But before deploying biometric security systems, one must carefully assess their substantial benefits and inherent dangers.

The Compelling Benefits of Biometric Authentication

Increased Security Via Uniqueness Biometric identifiers are far more unique than conventional authentication techniques. Biometric features like fingerprints, iris patterns, and facial geometry are inherently unique and extremely hard to duplicate, in contrast to passwords, which may be guessed, shared, or stolen. The possibility of illegal access via credential sharing or theft is greatly decreased by this uniqueness. Better User Experience Biometric verification removes the mental load of remembering complicated passwords or carrying around physical tokens. By merely introducing themselves to the system, users may authenticate, resulting in a smooth and straightforward experience. This convenience aspect frequently results in greater user acceptance rates and fewer help desk calls concerning forgotten credentials.

Authentication That Is Not Transferable The fact that biometric credentials cannot be readily shared, taken, or transferred between people may be the most crucial aspect. Biometric authentication, on the other hand, necessitates the physical presence of the permitted user, giving robust non-repudiation capabilities for audit and compliance, while passwords may be written down or shared with coworkers.

Significant Risks and Vulnerabilities

Problems with Data Protection and Privacy Some of the most private personal information that a company can acquire is biometric data. Biometric traits are permanent, unlike passwords that can be modified if compromised. Because people cannot just "reset" their fingerprints or facial features, a breach of biometric databases can have lifelong consequences for those who are impacted. Misidentifications of Both Types Biometric systems are never entirely accurate. According to Harvey (2016:137) false positives can give unauthorized users access, whereas false negatives can prevent legitimate users from entering. Biometric readings might be impacted by environmental factors, aging, injuries, or medical disorders, which might cause operational disruptions and accessibility problems. Sophisticated attackers can use spoofing and presentation attacks (Balkan, 2021.43). Employing a variety of spoofing strategies may potentially circumvent biometric systems. Less advanced biometric systems can be tricked by high-resolution images, silicone fingerprint replicas, and even deepfake technology. Although live detection techniques help reduce these dangers, they increase the complexity and expense of implementations.

Implementation Challenges in Real-World Environments

Technical infrastructure needs include specialized hardware, secure storage systems, and reliable network connection for the deployment of biometric systems. Additionally, companies must think about integration with current identity management systems and make sure that various platforms and devices are compatible. The complexity of regulatory compliance Biometric data acquisition and processing are becoming more and more regulated by privacy laws around the world. Businesses must contend with complicated legislative structures such as GDPR, CCPA, and industry-specific regulations (Harvey, 2016:138). This involves using suitable data reduction strategies, consent procedures, and safe deletion methods. Factors to Consider Regarding Cost and Scalability The price of biometric technology has dropped, but setting up company-wide systems still requires a significant investment. Businesses should take into account the continuous maintenance, support, and potential technology upgrade cycles, in addition to the initial expenditures for hardware and software.

Best Practices for Successful Implementation

Rather than depending on just one biometric method, many leading applications employ a multimodal approach that combines several elements, such fingerprint and face recognition, or incorporates biometric data. traditional authentication methods in a multi-factor authentication approach (SABRIC, 2020:np). Template Protection Unnecessary hazards are created by storing raw biometric data. Template-based systems are used in sophisticated implementations. The shop employs mathematical representations of biometric characteristics rather than real biometric photos, which greatly minimizes privacy exposure while preserving security efficacy. Fallback Procedures Strong biometric systems Always provide backup authentication methods for scenarios where biometric authentication fails or is not accessible. This preserves business continuity while adhering to security norms.

Strategic Implications

Prior to implementing biometric authentication, businesses should conduct thorough risk assessments that weigh the expenses of implementation and privacy issues against the security benefits. One must meticulously plan, include stakeholders, and continually monitor to ensure that systems remain efficient and compliant in order to be successful. Biometrics, despite being a powerful tool in the modern cybersecurity arsenal, are not a panacea. When implemented properly with sufficient protections and realistic expectations, biometric systems may significantly increase security while also improving the user experience (SABRIC, 2020:np).

Research method and design

Quantitative research, as defined in this study's methodology, is a numerical depiction of explanations for the occurrences (Bryman, 2021:89; data collection methods used throughout the research (Kumar, 2021:67):

- Comparing a list of similar work done throughout the years with a literature review (a systematic review, or systematic literature review, is a type of) a review of the literature that employs methodical approaches to gathering secondary data.
- Surveying internet users to see how biometrics are used to verify payments and regular everyday personal banking transactions.
- Speaking with customers, bank users, financial organizations like banks, and the public at large (students, members of the working and unemployed community) who have bank accounts.

In order to avoid the systematic, stratified, and cluster random sampling methods, the study used the random sampling approach (Mason, 2018:44; Maxfield & Babbie, 2018:90). Customers with one or more bank accounts were included in the study's inclusion criteria. The city of Johannesburg in Gauteng province, with a population of about 5,782,747, was the primary subject of the research. Ombudsman for Banking Services According to the Department of Statistics South Africa (2019), around 30% of this group is under the age at which one is typically allowed to have a bank account (2022:np). The study sample size was restricted to 300 respondents from the remaining 4,047,923 customers who had bank accounts, for a total of 1,734,824. due to difficulties like limited time and resources (Open Data Charter, 2018:np). 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

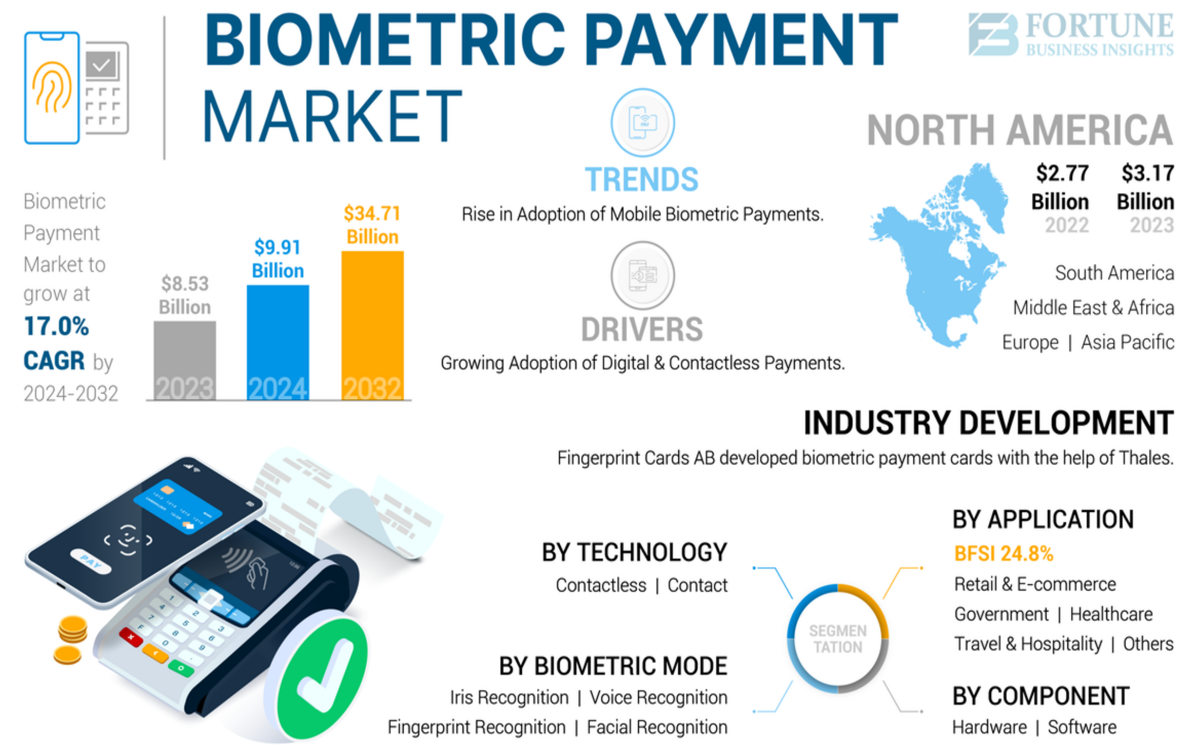
Validity of the data collection tool used

The validity of data within a dataset or database is measured by its accuracy and reliability. According to Yin (2018:111) and Snyder (2019:54) it entails confirming that the data adheres to specified norms, regulations, or restrictions, ensuring that the information is reliable and appropriate for its intended use. The data gathered in the systematic literature review (a comprehensive, thorough overview of current evidence, both published and unpublished) will be used to assess content validity. As a result, the opinions of consumers, bank managers, and retail managers who use biometrics authentication for payments and other transactions will be assessed in order to ascertain constructive validity.

Results and analysis

This section of the study presents findings of the study obtained during the systematic literature review (a complete, exhaustive summary of current evidence, published and unpublished).

Figure 2: Descriptive statistics of biometric payment market



Correlation statistics

The goal of this section is to illustrate the link between variables. As a result, other parts of the article were examined using a large body of literature, and the Pearson's correlation was carried out to investigate statistical links between variables (Skinner, 2014:23). Additionally, the advantages and problems variables were compared and matched to conduct the data analysis. Because Spearman uses rank-ordered variables, while Pearson's correlation uses the raw data values of the variables, it was employed. The Pearson correlation, however, analyzes the linear relationship between two continuous variables, whereas the Spearman correlation coefficient is based on the ranked values for each. the variable instead of the raw data (Lobley, Winter, & Wheeler, 2018:54). The data was analyzed using correlation, which predicts the magnitude and direction of the relationship between two variables.

Future Perspectives and Recommendations

As biometric technologies continue to advance, law enforcement agencies face both tremendous possibilities and significant obstacles (Turvey & Crowder, 2017:26). A sensible and strategic strategy is necessary to maximize the capabilities of these technologies, taking into consideration existing trends and professional advice.

- *Developing Reliable Artificial Intelligence*

The reliability of the artificial intelligence (AI) systems that underpin biometric technologies is a crucial factor in their application. These systems must adhere to transparency, accountability, and accuracy standards in order to be utilized efficiently while respecting fundamental rights. The European Union High-Level Expert Group on Artificial Intelligence states that "reliable AI must be lawful, complying with all applicable laws and regulations; ethical, ensuring" adhering to ethical norms and values, and being strong from both a social and technological standpoint" (Wewege, Lee & Thomsett, 2020:36).

- *Adopting an Adequate Ethical and Legal Framework*

To successfully integrate biometric technologies into law enforcement activities, it is necessary to adopt a robust ethical and legal framework.

This framework should include clear rules on the collection, storage, and use of biometric data, as well as oversight and accountability mechanisms to prevent abuses and protect citizens' fundamental rights. The European Parliament passed the Artificial Intelligence Act (AI Act) in 2024, which states that "the use of biometric technologies in public" is prohibited. Spaces must adhere to the tenets of necessity and proportionality, only being permitted in rare circumstances and under close supervision (Investing in Professional Training and) Education. It is essential to adequately train law enforcement officers in biometric technologies, including technology training, in order to guarantee their effective and ethical deployment. understanding the ethical and legal ramifications of use and acquiring the skills necessary to handle sensitive information responsibly. A study by the European Agency for Fundamental Rights the FRA emphasizes that "the lack of training among personnel in the use of biometric systems can lead to the erroneous application of technology and violations of fundamental rights" (Hardyanthi, 2024:68).

- *Promoting Transparency and Public Engagement*

Maintaining public confidence requires transparency in the usage of biometric technologies. Engaging communities in the implementation process through open communication and public consultations can help identify concerns and create solutions that address social needs. The European Data Protection Board (EDPB) states that "any facial recognition system implemented by authorities must be accompanied by clear transparency measures, including informing citizens." and enabling them to question the way biometric data is processed" (Hofmann & Mustert, 2023:468).

- *Continuous Monitoring and Impact Assessment*

For the use of biometric technologies, it's crucial to implement impact assessments and monitoring methods. These should include frequent assessments of the systems' effectiveness and fairness, as well as analyses of how they affect individual rights and liberties. The Council of Europe states in a report that regular assessments of the impact of biometric technologies on human rights are essential to ensure there. Hardyanthi (2024:73) states that the usage "aligns with democratic principles." The integration of biometric technologies into law enforcement operations presents a great chance to improve public safety. It is imperative, nevertheless, that this integration be done in a responsible manner, protecting citizens' basic rights and fostering a just and secure society (Shulzhenko & Romashkin, 2020:21).

Essential steps for promoting ethical behavior include the establishment of a clear legislative framework, investments in professional training, and the creation of efficient oversight systems. and the efficient application of these technologies. To fully realize the promise of biometrics while safeguarding individual rights and liberties, we must adopt a transparent and fair strategy. The use of biometric technology in law enforcement operations has led to considerable improvements in operational effectiveness, public safety, and suspect identification skills (Lynch, 2020:65). However, the use of these technologies also raises significant issues regarding ethical considerations, cybersecurity, and the protection of personal data. It's crucial to strike a balance between national security and citizens' basic rights in order for biometrics to be used ethically and effectively.

Biometric technologies have undeniable advantages, including the capacity to quickly and precisely identify people, lower crime rates, and make the most of law enforcement resources. According to Lynch (2020:78), "increased efficiency in criminal investigations and improved public safety" have been made possible by face recognition, fingerprint identification, and behavioral analysis.

However, the use of these technologies raises concerns regarding data privacy, potential misuse, and technological errors.

The EU Agency for Fundamental Rights's study states that "biometric systems used by authorities must be subject to strong safeguards to prevent disproportionate." use and excessive surveillance" (Nguyen, 2018:64). Algorithmic bias, which may result in misidentifications and discrimination, is another significant danger. According to current studies, "biometric technologies have a higher error rate in identifying people of color and women, which can affect fairness in law enforcement" (Nguyen, 2018:76). To ensure that biometric technology is morally and legally acceptable, authorities must strike a balance between the need for national security and the preservation of fundamental rights. The General Data Protection Regulation (GDPR) mandates that the use of biometric data be justified by a clear public interest that is proportionate to basic rights and freedoms. The implementation of oversight and transparency measures is necessary in order to ensure that biometric technology does not result in widespread breaches of privacy. The Artificial Intelligence Act (AI Act), which sets explicit limitations on the live application of facial recognition and is an example of a balanced regulation, is one such example. establishes stringent data protection standards (Nguyen, 2018:63).

To ensure the ethical and efficient use of biometric technology, several regulatory measures and best practices are necessary:

- *Establishing clear data protection standards*

All uses of biometric technology must adhere to the AI Act and the GDPR, and data processing must be proportionate and rational. "Law enforcement agencies must" employ particular safeguards to safeguard biometric information, such as encryption and access limitations" (Nguyen, 2018:71).

- *Monitoring and auditing biometric systems*

The misuse of technology can be avoided by establishing independent oversight mechanisms. The Council of Europe states that a framework for periodic audits and reporting is necessary to assess the impact of biometric technology on citizens' rights (Rodríguez, 2025:89).

- *Increasing transparency and public engagement*

To guarantee public understanding of the usage of biometric technology, law enforcement organizations must implement transparent policies. "Informing citizens about the use" Maintaining public confidence requires the use of facial recognition and the establishment of methods to contest automated choices" (Smith *et al.,* 2021:33).

- *Developing more equitable and reliable algorithms*

Biometric systems must undergo rigorous testing to ensure accuracy and eliminate technological biases (Haley &) in order to lessen algorithmic bias, which is essential for preventing misidentifications and discrimination. Biometric technologies have revolutionized law enforcement practices and identification methods, providing potent tools for crime prevention and public safety (Burrell, 2025:11). Nevertheless, their application needs to be balanced to avoid discrimination, excessive monitoring, and misuse.

Law enforcement agencies will be able to use the advantages of biometrics without sacrificing basic rights if the implementation is responsible, transparent, data-protected, and founded on solid legislation. citizen rights (Haley *et al.,* 2025:17). In order for innovation to be used for the benefit of everyone, it is essential for society to stay vigilant and involved as technology progresses.

Conclusion

Through the verification of retail payments, online banking, and financial technology, this research sought to determine whether security and simplicity are necessary. the utilization of the biometric system. In addition, the research looked at potential problems, advantages, and solutions for the biometric authentication payment system. The research went on to examine the biometric solutions that may help banks and retailers improve the security and creativity of their methods for accessing, sending, and sharing funds. It is determined that biometric technology is the cutting-edge technology that various banking institutions can utilize to strengthen security and innovation as well as safeguard their assets. their clients from scammers, fraudsters, hackers, and other limitations. Thus, additional research might concentrate on the interaction between biometrics, digital banking, and financial technology.

Reference List

1. Babbie, E. 2021. *The practice of social research*(15th edition). Australia: Cengage Learning.
2. Balkan, B., 2021. Impacts of digitalization on banks and banking. In *The Impact of Artificial Intelligence on Governance, Economics and Finance, Volume I* (pp. 33-50). Singapore: Springer Nature Singapore.
3. Botta, A., Nadeau, M.C., Bruno, P., Tayar, G. and Chaudhuri, R., 2020. Global Banking Practice.
4. Bryman, A. 2021. *Social research methods*(6th edition). Cape Town: Oxford University Press.
5. Creswell, J.W. 2020. *Research design* (6th edition). Thousand Oaks (CA): SAGE.
6. Haley, P. and Burrell, D.N., 2025. Integrating Artificial Intelligence into Law Enforcement: Socioeconomic and Ethical Challenges. *SocioEconomic Challenges (SEC)*, *9*(2).
7. Hardyanthi, T., 2024. Biometric Data Protection in Human Rights Perspective: Analysis Based on the UN Charter and International Conventions. *E-Justice: Journal of Law and Technology*, *1*(1), pp.68-80.
8. Harvey, D., 2016. Digital transformation in banks: The trials, opportunities and a guide to what is important. *Journal of digital Banking*, *1*(2), pp.136-145.
9. Hofmann, H.C. and Mustert, L., 2023. Data protection. In *Research Handbook on the Enforcement of EU Law* (pp. 461-475). Edward Elgar Publishing.
10. INTERPOL. 2020. Interpol Warns of Financial Fraud Linked to COVID-19. Available at: http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraudlinked-to-COVID-19 (Accessed on 10 July 2025).
11. James, S.H. & Nordby, J. 2018. *Forensic science. An introduction to Scientific and Investigative Techniques* (3rd edition). Boca Raton: CRC Press.
12. Kruse, C., 2015. *The social life of forensic evidence*. Univ of California Press.
13. Kumar, R. 2021. *Research Methodology- a step-by-step guide for beginners* (7th ed.). London: SAGE Publications.
14. Leavy, P. 2022. *Research design: Quantitative, qualitative, mixed methods, arts based, and community-based participatory research approaches*. New York: The Guilford Press.
15. Lobley, M., Winter, M. and Wheeler, R., 2018. *The changing world of farming in Brexit UK*. Routledge.
16. Lynch, J., 2020. Face-off: Law enforcement use of face recognition technology. *Available at SSRN 3909038*.
17. Mason, J. 2018. *Qualitative researching* (3rd edition). London: Sage.
18. Maxfield, M. & Babbie, E. R. 2018. *Research methods for criminal justice and criminology*(8th edition). Boston, MA: Cengage Learning.
19. Nguyen, F.Q., 2018. The standard for biometric data protection. *Journal of law & cyber warfare*, *7*(1), pp.61-84.
20. Ombudsman for Banking Services. 2022. New wave of fraud targeting banking customers. Available at: https://www.obssa.co.za/press_releases/new-wave-of-fraud-targeting-bank-customers/ (Accessed on 29 May 2025).
21. Open Data Charter. 2018. *Using data to combat corruption*. https://open-datacharter.gitbook.io/open-up-guide-using-open-data-to-combatcorruption/background-charter-open-up-guides (Accessed on 14 April 2025).
22. Patel, F. 2023. The Citizen. SA grappling with a surge in banking app fraud, SABRIC reveals. Available at: https://www.citizen.co.za/news/sa-grappling-surge-banking-app-fraud-SABRIC/ (Accessed on 06 March 2025).
23. Pieter, B. 2022. *Digital Transformation in South Africa's banking industry*. Available at: https://www.sovtech.co.za/blog/digital-transformation-in-south-africas-banking-industry (Accessed on 14 January 2025).
24. PricewaterhouseCoopers. 2019. *PwC 2019 Global Economic Survey. Confronting the changing face of economic crime 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2025).
25. Rodríguez, B.F., 2025. Biometric Breakthroughs. *Management*, *104*, p.89.

26. SABRIC. 2020. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2025).
27. Shulzhenko, N. and Romashkin, S., 2020. Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), pp.162-172.
28. Skinner, C., 2014. *Digital bank: Strategies to launch or become a digital bank*. Marshall Cavendish International Asia Pte Ltd.
29. Smith, M. and Miller, S., 2021. *Biometric identification, law and ethics* (p. 99). Springer Nature.
30. Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104, pp.333-339.
31. Sukhera, J. 2022. Narrative reviews: flexible, rigorous, and practical. *Journal of graduate medical education*, 14(4), pp. 414-417.
32. Turvey, B.E. and Crowder, S., 2017. *Forensic investigations: An introduction*. Academic Press.
33. Wewege, L., Lee, J. & Thomsett, M.C. 2020. Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, 10(6), pp.15-56.
34. Wewege, L., Lee, J. and Thomsett, M.C., 2020. Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, *10*(6), pp.15-56.
35. Yin, R.K. 2018. *Case study research and applications: Designs and methods (*6th edition). Los Angeles, CA: Sage.