International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 5, Sep-Oct 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Biometrics in Banking

Matthew N. O. Sadiku[1], Samuel A. Ajayi[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]Texas Southern University, Houston, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The financial sector is at a crucial crossroads as we navigate an era marked by rapid technological advancements and shifting consumer expectations. Banking has moved rapidly from branches and paper forms to mobile applications, online platforms, digital wallets, and remote customer service. This transformation has made financial services faster and more accessible, but it has also increased the risks of identity theft, phishing, account takeover, and transaction fraud. Banks must consequently verify customers with methods that are both secure and convenient. Biometrics in banking is the use of unique physiological or behavioral characteristics of individuals for authentication and security purposes in digital banking transactions and account access. It addresses this challenge by using measurable human characteristics to recognize or authenticate an individual, reducing exclusive dependence on passwords, PINs, and security questions that may be forgotten, guessed, stolen, or shared. This paper explores major use cases of biometrics in banking.

KEYWORDS: *biometrics, biometric payments, banking, banking industry, banker.*

How to cite this paper: Matthew N. O. Sadiku | Samuel A. Ajayi | Janet O. Sadiku "Biometrics in Banking" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-5, October 2026, pp.513-523, URL: www.ijtsrd.com/papers/ijtsrd142258.pdf

IJTSRD142258

Copyright © 2026 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

INTRODUCTION

Banking has become increasingly digital, enabling customers to open accounts, transfer money, authorize payments, and obtain support without visiting a branch. This convenience has made reliable identity verification essential. Passwords and personal identification numbers remain common, but they may be forgotten, reused, stolen through phishing, or exposed in data breaches. Biometrics offer a different approach by verifying people through physical or behavioral characteristics such as fingerprints, faces, voices, irises, or interaction patterns. They also offer banks a more direct way to determine whether a person requesting access is genuinely connected to an account. Biometric banking refers to the use of unique biological traits—such as fingerprints, facial recognition, iris scans, or voice patterns—to authenticate users instead of traditional PINs or passwords.

In banking, biometric technology can strengthen authentication and simplify the customer experience, but it also creates serious concerns involving privacy, security, fairness, and accessibility. Banks can use biometrics throughout the customer relationship. The strongest argument for banking biometrics is that they can improve both security and usability. When implemented responsibly and combined with trusted devices and cryptographic security, biometrics can make banking safer, simpler, more efficient, and more inclusive [1].

WHAT IS BIOMETRICS?

Any banking customer has used a password or a PIN code at least once. However, these traditional methods of verification are steadily giving way to the next generation of authorization tools. Passwords, codes, PINs, and safety questions have shown to be less dependable when used against modern cybersecurity threats. The financial sector is shifting towards safer, more customer-friendly verification. Biometric authentication has arisen as an answer to the outdated and more easily compromised traditional techniques.

Biometrics is the utilization of unique biological traits for identification. It is a technology powered method of personal identification that leverages unique biological patterns on and in human body. It is based

on one-of-a-kind biological characteristics of a client, which include fingerprints, facial traits, and more. It is a fast-developing field that utilizes users' unique biological characteristics, like fingerprints, facial features, iris patterns, or even voice, to identify and verify the users. This technology is poised to become just as common in the world of financial transactions, where convenience is key and security is paramount. It offers a significant leap forward compared to traditional passwords and PINs. It promises a future of banking that is not only exceptionally secure but also remarkably convenient and personalized. Figure 1 shows a representation of biometrics [2].

Biometric payments date to ancient civilizations, in which physical traits such as handprints and facial features were used for identification. Modern biometrics emerged in the 1800s and biometric payment systems began to gain traction in the early 2000s, when Pay By Touch introduced one of the first fingerprint-based payment systems. By the 2020s, biometric technology has become widespread and is integrated into smartphones for a variety of applications including payment authentication. Today, biometric payments are more popular and widely adopted than ever.

Biometric authentication employs cutting-edge technology to capture and analyze various biological attributes. Two main hardware setups allow biometric payments to work. The first uses the built-in hardware on a customer's smartphone or smart device, such as a fingerprint scanner or facial recognition, to authenticate their identity. The second scenario uses dedicated payment system hardware to verify a person using biometrics. When a user attempts to access a financial service, such as logging into an online banking account or making a transaction, the system prompts them to provide a biometric sample. This sample is compared against the stored biometric template for that individual. Access is granted if there is a match; if not, the system denies access.

TYPES OF BIOMETRICS

Biometrics in financial digital services concerns the protection of users' financial and personal data and the conduct of financial transactions. The different types of biometric payments include [3]:

- *Fingerprint Recognition:* A fingerprint biometric is a representation of multiple points on the fingerprint, and the relative positions of those points. Fingerprint recognition is the most common form of biometric payment. It involves scanning and matching the unique patterns on a person's fingertip or fingertips to authenticate their identity and authorize a transaction. Fingerprint biometrics in finance offer several benefits to financial institutions and their customers. Figure 2 shows fingerprint biometrics [4].
- *Facial Recognition:* This technology works similarly to how our eyes and brains identify people. First popularized by Apple's Face ID, this method is quickly catching up to fingerprint recognition in popularity. It works by using infrared light to scan a person's face and pinpoint thousands of dots that make up their unique facial structure. The traits are transformed into a template for subsequent authorization. If the features are nearly identical, the admission is authorized. With face recognition technology, computer vision is used to create a biometric template of a user's face, measuring unvarying characteristics such as the distance between the eyes and the length of the nose. Figure 3 shows facial recognition [5].
- *Retina Recognition:* This is also known as eye scanning. Its essence is to check people based on the unique patterns found on their irises. By capturing the intricate patterns within the iris or retina, this method offers a high level of accuracy in authenticating users, and has long been trusted in high-security environments. A special camera captures the iris in high definition, and the resulting image is matched up with the pre-existing framework. If they are mostly identical, the client is allowed onto the application. Airports originally used iris scanning for security screening. However, it has now become part of banking security.
- *Voice Recognition:* This method is based on the vocal traits of users. The pitch of voice modulation, as well as speaking habits, help create a voiceprint for further verification. The method analyzes the nuances in speech patterns and voice characteristics, then compares this voiceprint to registered samples to certify a match.
- *Behavioral Recognition:* A client's behavior patterns have unique dynamics online, including typing rhythm, mouse/touchscreen use, speech, or walking. Unlike the other biometric authentication examples, this one takes into consideration the interaction with versatile systems and devices. A behavioral profile is established and then utilized for authorization. Behavioral recognition is non-disruptive and highly secure because of its resistance to forgery.
- *Vein Patterns:* Using near-infrared light and often centering on the palm or finger, this technology

analyzes the pattern of visible blood vessels unique to each person.

- *Signature Recognition:* This somewhat less common process scans and digitizes a person's signature, then puts it through a shape-identifying algorithm to verify their identity.
- *Palm Recognition*: Similar to fingerprint scanning, this verification type relies on capturing the individual traits of the client's palm. It embraces patterns, ridges, loops, and other modalities. They are very precise and difficult to reproduce. Rich in detail and complex, these contribute to the successful identification.

Figure 4 shows some of these types of biometric authentication [6].

BIOMETRICS IN BANKING

Banking has always depended on a difficult question: how can an institution know that the person requesting access to money is truly the account holder? Banking increasingly takes place through mobile applications, websites, automated teller machines, and remote customer-service channels. This shift has made financial services faster and more accessible, but it has also exposed the weaknesses of passwords, personal identification numbers, and one-time codes. Such credentials can be forgotten, reused, stolen, shared, or obtained through phishing. Biometrics—technologies that recognize people through physical or behavioral characteristics—promise a more natural form of trust. Biometrics in financial services, in most cases, concerns the protection of users' financial and personal data and the conduct of financial transactions. Biometric technologies have become an increasingly prominent feature of modern banking. They utilize unique physiological or behavioral traits, such as fingerprints, facial recognition, or voice patterns, for authentication and transaction verification [1]. Figure 5 shows biometrics in banking [7], while Figure 6 illustrates the biometric banking journey [8].

Biometrics can bring substantial benefits to banking by strengthening authentication, reducing exposure to stolen passwords, accelerating digital service, lowering administrative friction, widening access, and increasing customer trust. The value of biometrics depends on responsible implementation. Biometric data is sensitive and, unlike a password, cannot simply be replaced if compromised. Biometrics should also be part of layered authentication rather than treated as infallible proof. When banks combine biometrics with cryptographic credentials, privacy-by-design, rigorous testing, fraud monitoring, and accessible fallback methods, they can create financial services that are both more secure and easier to use. Figure 7 shows how biometrics works in banking [9], while Figure 8 shows a bank client using biometrics [10].

APPLICATIONS OF BIOMETRICS IN BANKING

The applications of biometrics in banking include mobile login, digital onboarding, payment authorization, biometric cards, call-center authentication, ATM access, employee security, and continuous fraud detection. When combined with trusted devices, cryptographic credentials, liveness detection, behavioral analysis, and multi-factor authentication, biometric technology can make financial services both easier to use and more resistant to fraud. There are many examples of how biometrics can be used in banking. Figure 9 shows some use cases of biometrics in banking [5]. Common applications of biometric in banking include the following [1,5,11]:

- *Online Services*: The most widespread banking application of biometrics is customer authentication in mobile and online services. A customer can use a fingerprint or facial scan to access a banking application instead of entering a password during every session. This creates a faster user experience and reduces exposure to weak, reused, or observed credentials. It is especially valuable on smartphones, where fingerprint sensors and facial-recognition cameras are already integrated into the device.
- *Multi-factor Authentication*: Biometrics is strongest when it operates within multi-factor authentication. A bank may combine something the customer possesses, such as a registered phone, with something the customer is, such as a face or fingerprint. Combining an associated device with a biometric factor can reduce unauthorized access by placing multiple barriers between an attacker and an account. A stolen password is therefore less useful if the criminal cannot also obtain the trusted device and biometric approval.
- *Transaction Authorization*: An important application is payment and transaction authorization. Banking and digital-wallet applications may request a fingerprint or facial scan before approving a transfer, changing account details, adding a beneficiary, or completing a purchase. Risk-based systems can apply such checks selectively. A routine payment from a familiar device may proceed quickly, whereas a large transfer from a new location may trigger stronger biometric and non-biometric

verification. This method allows the bank to increase security where risk is highest without burdening every customer interaction.

- *Payment Cards*: Biometric technology is being incorporated into payment cards. A biometric card contains a fingerprint sensor that captures the cardholder's print when the card is inserted or tapped and compares it with an enrolled reference value. A successful comparison authenticates the cardholder. Such cards may combine the familiarity of card payments with biometric verification, including in contactless transactions. Biometric payment cards require rigorous testing and clear fallback procedures when verification fails.
- *Voice Verification*: In telephone banking, voice biometrics can help determine whether a caller matches an enrolled voice profile. This may reduce dependence on lengthy knowledge-based questions and improve the speed of customer service. Voice verification can also operate in the background while a caller speaks naturally. Nevertheless, a bank should combine voice with other evidence because background noise, illness, microphone quality, replayed recordings, and synthetic speech may affect reliability. Device information, telephone number, location, transaction history, and risk signals can strengthen the overall decision.
- *Fraud Detection*: Fraud evolves with technology. Data theft is becoming a growing problem for both financial organizations and banking customers. Advanced biometric systems go beyond static physical characteristics and incorporate behavioral biometrics like typing rhythm, device interaction patterns, and even mouse movements to build a comprehensive user profile. These profiles can flag irregularities in user behavior, thus acting as a proactive fraud detection mechanism. Such systems can detect anomalies in user behavior, signaling potential fraudulent activity. In such cases, banks are instantly notified in real-time, allowing them to take immediate action.

BENEFITS

The main benefits of biometrics in banking are greater convenience, stronger identity assurance, and improved operational efficiency. The most important benefit of biometrics is stronger account security. Other benefits of biometric in banking include the following [1,12]:

- *Accessibility*: Voice recognition is part of the approach to accessibility and inclusiveness of banking services. People who cannot visit a bank branch for some reason or have difficulties using mobile apps can confirm their identity. This way, they access information about their products or make one-time transactions.
- *Easier to Use:* Any banking customer has used a password or a PIN code at least once. However, these methods of verification are steadily giving way to the next generation of authorization tools. As data safety demands grow stricter with time, bank clients are asked to create progressively complex and sophisticated passwords. Unlike traditional methods, biometrics are much simpler and do not require memorizing complex passwords. They are inherent and readily available in most scenarios where a person needs to access their account.
- *Efficiency*: Improvements can produce operational and financial efficiencies. Password resets, locked accounts, manual identity checks, and fraud investigations all consume employee time. A well-designed biometric system can automate part of this work, enable faster self-service, and allow staff to concentrate on complex or high-risk cases. Such layered controls help the institution apply stronger protection where the potential loss is greatest without making every customer interaction unnecessarily burdensome.
- *Customer Experience*: Consumers expect banking to be as seamless as unlocking their phones. Biometric banking offers that level of convenience while maintaining trust. Biometrics improve the customer experience. Customers frequently manage numerous passwords and may struggle to recall a complex banking credential used only occasionally. A fingerprint or facial check is generally faster and requires less effort than entering a password, receiving a code, and switching between applications. The result is a smoother login process and quicker approval of transfers, purchases, or other sensitive actions. Convenience is not merely cosmetic; biometrics can reduce the traditional tension between security and usability.
- *Customer Confidence*: Another benefit is greater customer confidence. Financial relationships depend on trust, and customers are more likely to adopt digital banking when they believe that unauthorized users cannot easily enter their accounts. A clear biometric approval step can reassure customers that access and high-risk transactions are being checked carefully. Standards and independent testing strengthen that confidence.

- *Identity Verification*: Another advantage is more efficient customer onboarding and identity verification. When a person opens an account remotely, a bank must establish that the applicant is a real individual and that the presented identity documents belong to that person. Facial comparison, document checks, and liveness detection can help connect the applicant to a legitimate identity while discouraging impersonation and duplicate enrollment. Biometric recognition can assist with detecting duplicate registrations and enabling authentication, although these systems must be designed for accessibility, security, privacy, and inclusion. For banks, effective digital verification can shorten approval times, reduce paperwork, and make it possible to serve customers who live far from a branch.
- *Financial Inclusion*: Biometrics can also promote financial inclusion. Traditional authentication may disadvantage people who have limited literacy, difficulty remembering passwords, no reliable postal address, or limited access to physical branches. A biometric identity system can provide another way to establish continuity between a person and an account, potentially enabling remote or agent-assisted banking. The benefit is especially meaningful where customers lack conventional identity documents or where duplicate and inconsistent records make verification difficult.

Figure 10 shows some benefits of biometrics [13].

CHALLENGES

These benefits are accompanied by significant risks. Unlike a password, a fingerprint, face, or iris cannot easily be replaced following a breach. Other challenges of biometric in banking include the following [1,11]:

- *High Implementation Costs*: While biometric devices are becoming more affordable, the initial capital required for wide-scale implementation can be substantial. Not only is there the cost of the hardware and software, but there are also the operational costs tied to employee training and systems integration.
- *Security:* A major challenge concerns the security of biometric data. Traditional methods of transaction security are proving to be increasingly inadequate. They seem to be no match for sophisticated identity fraudsters. A compromised password can be reset, but a person cannot readily replace a fingerprint, face, iris, or voice. A breach may consequently expose the customer to persistent risks extending beyond a single bank or account. Centralized biometric databases can become particularly attractive targets because they concentrate identity-linked information. Biometric authentication is also vulnerable to presentation attacks, commonly called spoofing. An attacker may attempt to deceive a sensor with an artificial fingerprint, a photograph, a mask, a replayed voice recording, or synthetic audio and video. Figure 11 compares biometric security with user experience [8].
- *Privacy:* Privacy is important because biometric information links a person's body or behavior to an identity. Biometric data relating to an identifiable person is personal data and it becomes special-category data when processed to uniquely identify that person. Biometric information that can uniquely identify an individual is sensitive information because the information is stable over time, difficult to change, and innately linked with an individual's identity. Customers should also know whether biometric use is optional, what happens after a failed match, and how to challenge an automated decision.
- *Accuracy*: Accuracy presents another challenge because biometric matching is probabilistic, meaning that systems can produce false acceptances, in which an unauthorized person is incorrectly matched, and false rejections, in which a genuine customer is denied access. The central challenge is that biometric systems do not establish identity with absolute certainty; they make probabilistic comparisons using highly sensitive personal data. The acceptable balance depends on the task. Performance may also vary across devices, lighting conditions, injuries, disabilities, age groups, and demographic groups.
- *Retention*: Retention must also be limited. Official Canadian privacy guidance states that biometric information should be kept only for the period necessary to fulfil its stated purpose and legal obligations, after which it should be permanently destroyed from devices, cloud storage, and backups. In addition, banks should test systems across diverse user groups, monitor false acceptance and false rejection rates, deploy liveness detection, audit technology providers, prepare breach-response plans, and maintain safe non-biometric alternatives.
- *Transparency*: Transparency is equally important. Customers should understand what biometric information is collected, how it is transformed and stored, who can access it, how long it will be retained, and how they can withdraw or challenge

its use. Clear communication can build trust and help customers distinguish legitimate biometric prompts from fraudulent requests.

- *Regulation*: Regulatory fragmentation adds another layer of complexity. Regulatory requirements regarding collecting and using biometric data vary across countries and legal systems. Banking rules, payment regulations, cybersecurity obligations, privacy law, consumer protection, anti-discrimination requirements, and emerging artificial-intelligence legislation may all apply to the same system. The applicable standards also vary by jurisdiction. An international bank may need to reconcile different definitions of biometric data, consent requirements, cross-border transfer rules, breach-notification duties, and rights to deletion or human review.
- *Legacy Systems*: Implementation across existing banking infrastructure is costly and complex. Many banks operate legacy core systems alongside mobile applications, call centers, branches, payment networks, and outsourced identity platforms. Introducing biometrics across this environment requires institutions to manage secure enrolment, device replacement, software updates, model compatibility, customer complaints, service outages, and disputed transactions. Vendor dependence can produce lock-in because templates created by one recognition engine may not work with another.
- *Account Recovery*: Account recovery is a particularly weak point. A sophisticated biometric login offers little protection if a criminal can bypass it by persuading a call-center employee to reset the account. Conversely, a recovery process that demands the same biometric that has failed may permanently exclude the legitimate customer. Banks need secure alternatives, such as hardware-bound credentials, supervised identity checks, or carefully governed in-person procedures.

FUTURE OF BIOMETRICS IN BANKING

The future of biometrics in banking will not be defined simply by replacing passwords with faces or fingerprints. It will be shaped by whether banks can combine convenience, cryptographic security, privacy, fairness, resilience, and human choice. The future of banking authentication will likely combine biometrics with device intelligence, cryptography, and risk-based monitoring. The most important development will be a shift from biometrics as a remotely stored credential to biometrics as a local authorization mechanism [1].

No biometric system will remain permanently secure. Banks will need continuous testing, independent evaluation, incident response, and periodic reconsideration of whether each use remains necessary and proportionate. The resulting model will be biometric-enabled rather than biometric-dependent. Biometrics will become one layer in a broader, risk-sensitive authentication system rather than the sole gatekeeper. The future of biometrics in banking is therefore not the future of the body as a password. It is the future of the body as one carefully governed signal within a wider architecture of digital trust. Figure 12 shows that biometrics is the future of banking [14].

CONCLUSION

Biometric banking is redefining trust in financial services. Biometrics has become an important part of modern banking because it can connect stronger security with a smoother customer experience. It can make banking faster, more convenient, and more resistant to familiar password attacks. Yet the same technology can expose customers to lasting data compromise, unequal error rates, hidden surveillance, and exclusion. Consequently, biometrics should supplement—not replace—other security controls. The most effective approach is therefore not biometrics instead of all other controls, but biometrics as one layer in a broader system of cybersecurity, privacy governance, and human oversight. Applied in this balanced manner, biometrics can strengthen confidence in digital banking while protecting the rights and dignity of customers. More information on biometrics in banking can be found in the books in [15,16].

REFERENCES

[1] https://manus.im

[2] D. Orme, "The death of the PIN," https://internationaldirector.com/technology/the-death-of-the-pin/

[3] "Biometric payments: What are they and how are they shaping the future of commerce?" March 2024, https://www.payset.io/post/biometric-payments-how-are-they-shaping-the-future-of-commerce

[4] "Fingerprint biometrics in finance: Balancing security and convenience in a digital world," https://theenterpriseworld.com/how-fingerprint-biometrics-in-finance-work/

[5] A. Shalimov, "Biometric authentication: The future of secure FinTech transactions," June 2024, https://easternpeak.com/blog/biometric-authentication-in-financial-services/

[6] "How biometrics in banking is redefining security and user experience?" April 2025 https://www.appventurez.com/biometrics-in-banking

[7] A. Gallegos, "The silent sentinel: AI-powered behavioral biometrics transforming banking security," May 2024, https://medium.com/@carlosgallegos16/the-silent-sentinel-ai-powered-behavioral-biometrics-transforming-banking-security-d44738fcb798

[8] N. Kozłowska, "Biometrics in banking: Use cases, benefits & standards," October 2025, https://www.miquido.com/blog/biometrics-in-banking/

[9] P. Singh, "Unlocking the potential of biometrics technology in digital banking," May 2026, https://appinventiv.com/blog/biometrics-technology-in-digital-banking/

[10] G. Uttamchandani, "Biometric banking: Are fingerprints and face scans the end of PINs?" https://itmunch.com/biometric-banking-future-pinless/

[11] "Biometrics in banking: The future of secure transactions," May 2024, https://councils.forbes.com/blog/biometrics-in-banking

[12] D. Grinberg, "Biometrics in banking: Unlocking security and efficiency," January 2025, https://www.techmagic.co/blog/biometrics-in-banking

[13] "How secure are biometrics in banking?" https://resources.additionfi.com/biometrics-in-banking

[14] M. Clark, "Adoption of biometrics in banking and financial service industry," https://www.bayometric.com/biometrics-in-banking-and-finance/

[15] E. Higueras-Castillo et al., *Biometrics: Challenges, Trends and Opportunities*. Boca Raton, FL: CRC Press, 2025.

[16] J. D. Woodward, N. M. Orlans, and P. T. Higgins, *Biometrics: Identity Assurance in the Information Age.* McGraw-Hill Osborne Media, 2002.



Figure 1 A representation of biometrics [2].



Figure 2 Fingerprint biometrics [4].



Figure 3 Facial recognition biometrics [5].

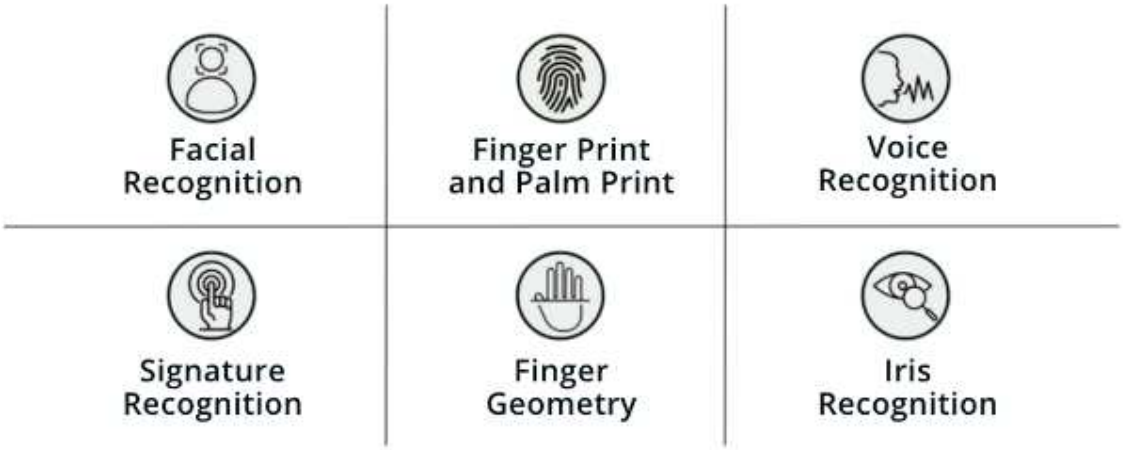


Figure 4 Types of biometric authentication [6].



Figure 5 Biometrics in banking [7].

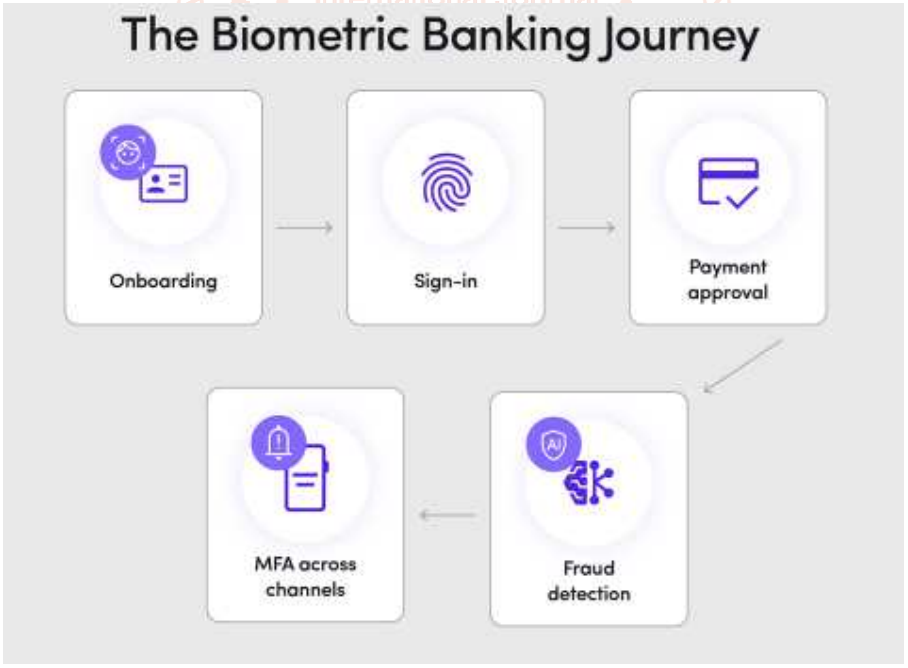


Figure 6 The biometric banking journey [8].

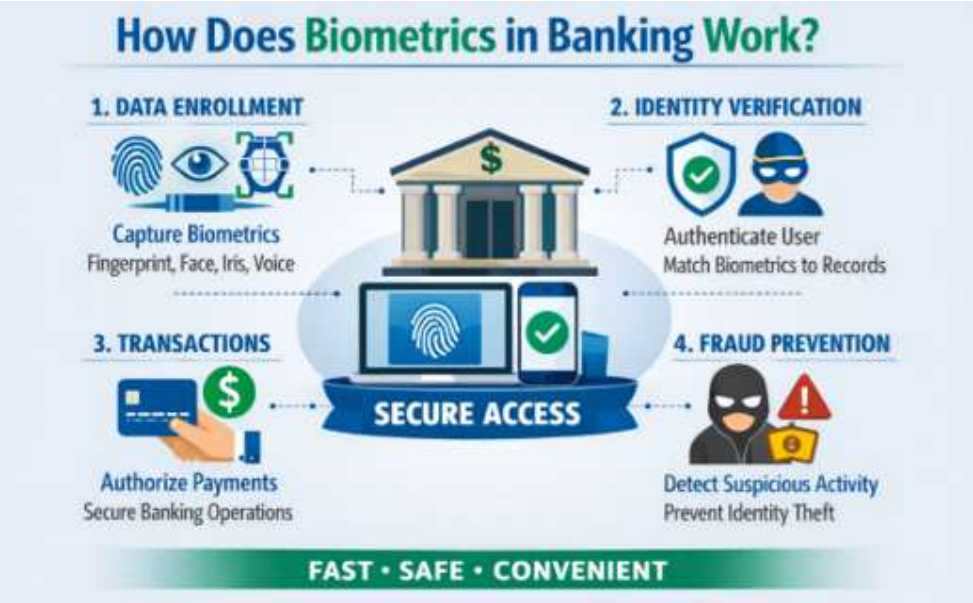


Figure 7 How biometrics works in banking [9].



Figure 8 A bank client using biometrics [5].



Figure 9 Some use cases of biometrics in banking [11].

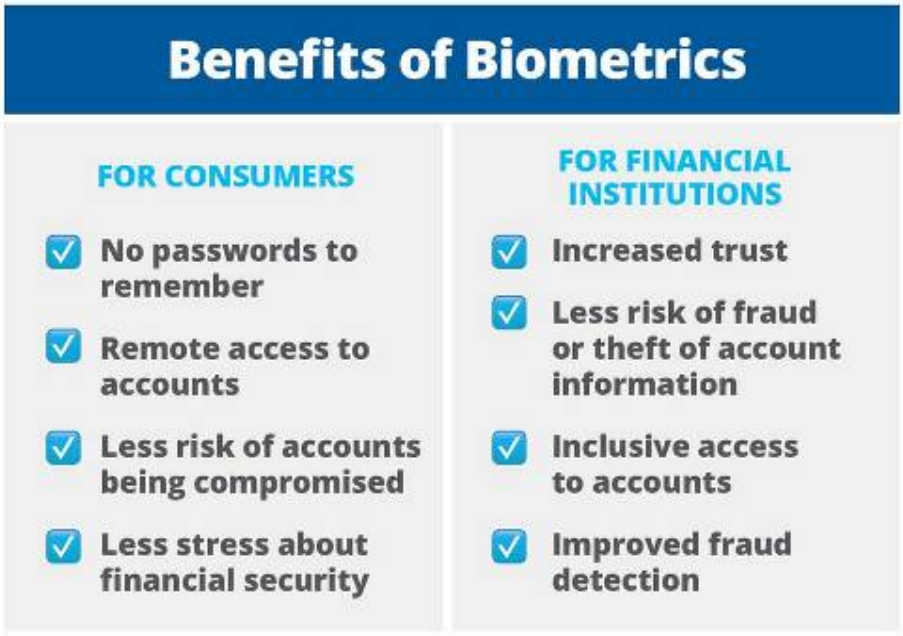


Figure 10 Some benefits of biometrics [13].

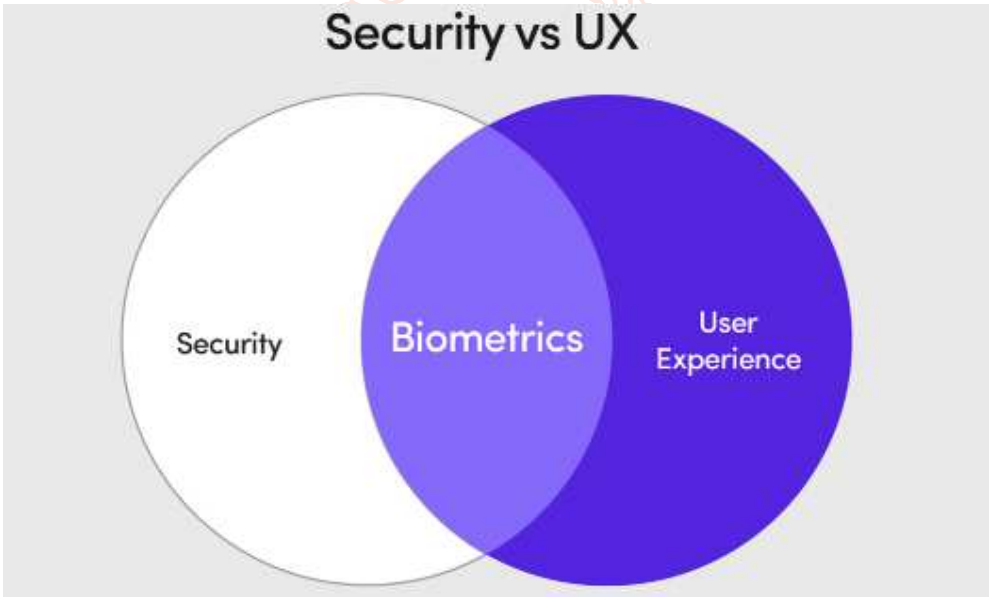


Figure 11 Comparing biometric security with user experience [8].



Figure 12 Biometrics is the future of banking [14].