International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 3, May-Jun 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Biometrics in Finance

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

For financial institutions and their customers, the traditional reliance on passwords has become a precarious balancing act, a fragile barrier against a tide of increasingly ingenious attacks. Biometric authentication is emerging as a technological novelty and a fundamental shift in how we secure our financial lives. It stands for a security procedure utilizing the individual physical traits or behavioral patterns with the end goal of verifying one's identity. Biometric authentication in banking has arisen as an innovative remedy to common security issues. Financial institutions have been progressively replacing traditional security systems with biometrics technology such as fingerprint sensors, facia recognition, and voice recognition. This shift from passwords and PINs to fingerprints, facial scans, or even voice recognition promises a future of banking that is not only secure but also remarkably convenient and personalized. Biometric payments offer a secure, convenient, and seamless way for consumers to carry out financial transactions. Biometrics is the basis of password less authentication, which is actively spreading worldwide. In this paper, we explore the exciting possibilities of biometric in finance.

KEYWORDS: *biometrics, biometric payments, finance, finance industry*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Biometrics in Finance" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-3, June 2025, pp.66-75, URL: www.ijtsrd.com/papers/ijtsrd79864.pdf

IJTSRD79864

INTRODUCTION

The financial sector is at a crucial crossroads as we navigate an era marked by rapid technological advancements and shifting consumer expectations. Traditional authentication methods—passwords, PINs, and even physical tokens—are becoming increasingly vulnerable to sophisticated cyber-attacks. Our wallets are getting slimmer, our phones are becoming our financial hubs, and the way we bank is undergoing a dramatic transformation. At the forefront of this transformation is the rise of biometrics, a technology that leverages unique physical or behavioral traits for identification and authentication. Biometric technology is emerging as a groundbreaking solution, offering unparalleled security features and ease of use for customers and employees.

Using biometrics to identify ourselves has become a part of daily life. Traditional passwords and PINs are making way for biometric verification methods, like fingerprint scanners, facial recognition systems, and iris detection. These methods offer a more powerful layer of protection compared to traditional passwords. For banking executives, understanding the nuances of biometrics, its opportunities, and its challenges is vital for staying ahead of the curve. Figure 1 shows some business executives [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 2 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 3 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 4 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 5 shows some of these types of biometric authentication [6].

EXAMPLES OF BIOMETRICS

Major credit card companies including Mastercard and Visa have integrated biometric authentication features into their payment systems, enabling cardholders to authorize transactions using their fingerprints or facial scans. Typical examples of biometric implementations include the following [7]:

- *JP Morgan Chase* is one the largest multinational banking and financial services companies serving millions of individual, government and corporate clients. With its foundation dating back over 200 years, it is one of the oldest financial institutions in the United States. JP Morgan Chase has abandoned password based authentication for its mobile app in favor of inbuilt biometric fingerprint sensor on iOS and Android mobile devices. It has even eliminated need of passwords for authenticating money transfers or payments which was earlier a mandate, even if customers had enabled fingerprint security.
- *European Union* plans to examine how biometrics can be used to verify and authenticate users of the EU Digital Identity Wallet, where the digital euro will likely be stored. The expansion of these verification systems can offer additional safeguards beyond the banking sector by confirming a user's identity when sharing medical data, taking online exams, or making age-restricted purchases.
- *Apple and Google* provide APIs to access these scanning features and authentication flow for the app's identity management systems (IDM), core banking systems, and security and data management layers. The biometric data never leaves the user's device; instead, a secure token or verification result is transmitted. The tricky part comes when this token needs to be processed within the bank's infrastructure in a compliant and secure way.
- *Union Bank of Philippines* is one of the major banks of Philippines ranking 7th in terms of assets. Commonly known as UnionBank, it has made multiple channels available for facilitating access to information and performing transactions. The bank has chosen to go with IdentityX platform for mobile biometric authentication. IdentityX platform is developed by Daon, a leading biometric software solution provider.
- *Citi Group Inc*. is an American multinational financial institution providing financial services across the globe. With several subsidiaries around the world, Citi Group is the 4th largest bank in the United States in terms of assets. Citi group became the first company that launched voice authentication in May 2016 across Asia Pacific region. Citi Bank customers from Australia, Hong Kong, India, Malaysia, Philippines, Singapore, Taiwan, Thailand, and Vietnam are leveraging voice biometric authentication to access the financial services provided by the bank.
- *Wells Fargo* is the world second largest American bank in terms of market capitalization and has international presence in banking and financial services. Wells Fargo Company is working on a payment solution that will make use of voice of its customers to authenticate transactions and access services. While other banks and financial institutions still have limited approach towards voice biometrics and use it only to let customers access information like account balance, etc., Wells Fargo Company's bold step to use voice biometrics to authenticate payments is quite a news for financial security experts.
- *Commonwealth Bank of Australia,* headquartered in Sydney, is the largest bank in the Southern Hemisphere. The bank provides a variety of financial and banking services with presence in New Zealand, the United Kingdom, Fiji, Asia and the United States. Biometrics is saving CBA a lot of time and cost while processing new customers.
- *Barclays*, with presence in more than 40 markets, is a multinational banking and financial services company serving individual as well as corporate clients. Barclays chose to ride biometric bandwagon back in 2014 introducing finger vein recognition system to authenticate users accessing banking services. In more recent history, the

company has employed voice biometrics to verify identity of customers calling Barclays call centers.

- *First Bank* is a banking and financial services company serving customers with its 115 locations in Colorado, Arizona, and California. The bank has upgraded its mobile banking app to leverage in-build fingerprint sensor on Touch ID enabled iPhones and iPads. Touch ID integration is set to enhance user experience as customers can now authenticate themselves just with the touch of a finger.
- *MasterCard*, headquartered in New York, provides its payment processing and payment card services around the world. The company is leveraging facial biometrics for payment authentication, colloquially known as "Selfie Pay." User can authenticate a payment by capturing their face on their smartphone camera. The feature has been rolled out in several countries with many others to follow. MasterCard has plans to make the technology available across the globe in the future.
- *Visa* is a world renowned payment processing and financial services company, headquartered in Foster City, California, United States with presence in every country in the world. The company chose to get rid of password based authentication in favor of a biometric solution by partnering with BioConnect, a biometric identity platform provider. Visa's biometric solution is set to work across many devices and operating systems and will accept multiple user biometric identifiers like fingerprint, voice, facial recognition, etc.

APPLICATIONS OF BIOMETRICS

Biometrics are methods of identifying individuals based on their unique physical or behavioral characteristics. Common examples of biometric characteristics include fingerprint, face, iris, voice, DNA, hand geometry, and signature. Biometrics are used for a variety of applications. Common applications of biometrics in banking and finance include the following [8,9]:

- *Biometric Payments:* These payments are transactions that use biological characteristics to verify a person's identity before processing a payment. They use people's distinct biological characteristics, such as their fingerprint, face, eyes, or voice to authenticate their identities during financial transactions. Biometric payment systems are already being piloted, and wider adoption could revolutionize the way we pay for everyday goods and services. Authenticating a person's identity in this way mitigates the risk of fraud and increases consumer confidence during transactions. The payment process typically involves three stages: registration, authentication, and authorization. Unlike traditional methods like cash or credit cards, biometric payments provide enhanced security through inherent biological identifiers, which are near impossible to replicate or steal, greatly reducing the risk of fraud and identity theft.
- *Behavioral Biometrics:* Beyond these established modalities, behavioral biometrics is emerging as a powerful tool for continuous authentication. This emerging field goes beyond physical characteristics, analyzing behavioral patterns like keystroke dynamics or mouse movements. It is like a system that recognizes and flags unusual activity patterns on your banking app, potentially preventing fraud before it happens.
- *Multimodal Authentication:* The future might involve a combination of biometric factors for enhanced security. For instance, a combination of fingerprint scans and facial recognition could be required for high-value transactions.
- *Voice-Activated Banking:* Voice assistants integrated with biometric authentication could become commonplace. It could be used to receive real-time account information or initiate transactions simply by using voice commands.
- *Biometric Insurance:* Biometric data, such as health information collected through wearable devices, could be used to personalize insurance plans and potentially lower premiums for those with healthy habits.
- *Facial Recognition ATMs:* The use of biometrics in banking ATMs is becoming popular in developing countries, and the adoption rate is growing significantly. Self-service ATMs use biometric security means to verify clients. Contactless transactions with facial recognition are revolutionizing the way we interact with ATMs. It gives users a more streamlined and secure experience. For example, Bank of America and National Bank of Qatar have implemented iris scanning programs at ATMs to improve security and simplify customer authentication processes.
- *Wearable Technology:* The integration of wearable technology with biometrics, such as using smartwatches for secure banking access, is gaining momentum. These advancements promise

a future of banking that is not only secure but also seamlessly integrated into our everyday lives.

- *Mobile Banking:* Banks around the world are increasingly opting biometrics to authenticate customers accessing their services. Mobile banking is growing rapidly worldwide. Despite the large number, many bank customers still have a lack of trust over the security of mobile banking platforms and concerns over security. Expanding rapidly across the globe, mobile banking is preferred by the majority of digital natives. Biometrics have a pivotal role in boosting user satisfaction regarding authorization and transaction safety. Combined with effective anti-fraud measures, they help provide top security for clients.
- *Accounting:* Biometrics can play a vital part in not only accounting but the audit-related functions of a business. To ensure that only authorized individuals have access to sensitive financial data, biometrics can be used to manage access to accounting systems and software. Employers can correctly report their work hours by using biometrics to track employee time and attendance. This can involve logging into accounting systems using a fingerprint or facial recognition system to clock in and out of work.
- *Marketing:* Biometrics have a much different place in marketing. By assessing client reactions to product displays or making product recommendations based on their facial expressions, a face recognition system can be utilized to customize the customer experience. It can also be used to track customer eye movements to determine which products, advertisements, or displays the customer seem to be most interested in. Customer emotions can be detected and analyzed using biometric technology, giving marketers information into how customers feel about various goods, services, and marketing campaigns.
- *Tax:* Taxpayers' identities can be verified using biometric technology, lowering their risk of fraud and identity theft. This may involve verifying the identity of taxpayers who file their tax returns online using a fingerprint or facial recognition technology. In some cases, biometrics can be used to reduce the exposure of sensitive information. Only authorized staff can access sensitive taxpayer information by using biometrics to manage access to tax systems and software.
- *Digital Wallets:* Biometric authentication is increasingly used in digital wallets, where users can authenticate payments or access digital tickets, boarding passes, and other services using biometric data.
- *Fraud Detection:* 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.

BENEFITS

The main benefit of biometric authorization type lies in its simplicity and safety. Biometric identification is faster, more convenient, and provides vastly more robust security than long-established payment system verification methods like passwords or physical cards. Biometrics are not just about security; they can also significantly improve the customer experience. Facial, eye, or fingerprint recognition easily resolves the problem of lost or lifted smart keys. Biometric authentication methods can be utilized virtually anywhere and anytime, which makes them truly versatile. Other benefits include [3,10]:

- *Enhanced Security:* Biometric data provides an unrivalled level of security compared to traditional passwords and PINs. Passwords can be misused, keycards lost, PINs can be forgotten, and mobile devices stolen, but biometric parameters are always with the client. Biometric identifiers are unique to each person and cannot be easily replicated or stolen, providing a robust authentication mechanism. In most cases, users' data is encrypted and stored on secure servers rather than in third-party databases, which are hard to regulate and monitor.
- *Operational Efficiency:* Traditional banking processes often require consumers to fill out multiple forms of identification. By reducing fraud and the need for manual authentication processes, biometric authentication helps financial services providers save money. Banks use biometric technology to improve operational efficiency by reducing the need for manual reviews and investigations.
- *Convenience:* In terms of user experience, implementing biometric authentication in banking offers customers a convenient alternative to remembering complex passwords. With biometric authentication, users can access their accounts and authorize transactions with a simple scan instead of having to set up and remember passwords and PINs. Voice recognition can

further enhance convenience, thereby allowing for secure transactions while on the go. It eliminates the hassle of remembering passwords. It allows for faster logins and transactions.

- *Accessibility:* Using fingerprints, facial recognition, or voice, customers can seamlessly access their accounts at any time. Voice recognition is part of the approach to accessibility and inclusiveness of banking services. Biometrics enables secure digital transactions for individuals who do not have official identification documents. 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.
- *Speed:* Biometric payments accelerate the checkout process, reducing transaction times and increasing the throughput of customers. This can lead to higher sales volumes and improved customer satisfaction. Biometric verification methods are often faster and more convenient than traditional methods. Biometric payments make for a quick and almost intuitive checkout process, enabling faster transactions, greater customer satisfaction, and improving operational efficiency for businesses.
- *Flexibility:* Biometric authentication in financial services can be applied to multiple platforms, including mobile apps, online services, and ATMs. Its superiority lies in providing consistency for different touchpoints. Speaking of applications, biometrics enable unified access to services from portable devices. Instead of typing in a password or verification code each time, users can effortlessly access their account.
- *Financial Inclusion:* Financial inclusion is a global priority that seeks to ensure that all people, regardless of their location or economic status, have access to basic financial services. Some view biometric payments as a tool for financial inclusion. By letting people use their biometric data for authentication, those without access to traditional banking or those who cannot remember PINs or passwords can participate in the financial system. Biometrics can enable financial inclusion by providing secure identity verification for individuals who may lack traditional identification documents
- *Competitive Edge:* Adopting biometric payment technology can position a business as a leader in innovation, differentiating it from competitors. Offering new payment options can attract tech-savvy customers and improve the overall brand perception.
- *Scalability:* Another important factor to consider is scalability and integration with existing systems. Biometric authentication can be scaled and integrated efficiently into established setups. This is incredibly important for banks implementing such biometrics for the first time.
- *Regulatory Compliance:* Financial institutions must comply with regulatory standards and legal norms. Biometrics can facilitate adherence to such norms as GDPR or KYC. Regulatory frameworks around data privacy and biometric usage need to be clear and comprehensive. This will help build trust among users and ensure the responsible implementation of biometric technologies.
- *Reduced Risk of Fraud:* Biometric verification significantly reduces the risk of unauthorized access to accounts. Since biometric data is unique and inherent to a user, it is much harder for fraudsters to bypass security measures compared to traditional methods.
- *Multi-Factor Authentication:* Multi-factor authentication systems can be created by integrating biometric verification with other security measures. This adds an extra layer of security, making it even more difficult for unauthorized individuals to gain access to accounts.
- *Scam Prevention:* Biometric authentication is one way to prevent identity theft or account hijacking. Verification systems that rely on biometrics are equipped with cutting-edge anti-spoofing precautions to avoid dishonest practices. Fake facial captures or fingerprints can become a pathway to compromising client data. Biometrics in banking security can trace aberrations in behavior or presented data which may indicate fraud.

Some of these benefits are displayed in Figure 6 [11].

CHALLENGES

In spite of the many clear benefits of biometric payments, there are some challenges to consider. Banks that can effectively address these challenges and build trust with their customers will be well-positioned to reap the benefits of biometric banking. The challenges include the following [3,8]:

- *Security and Privacy:* Safeguarding sensitive biometric data is paramount. Banks need to implement robust security measures, including data encryption and secure storage practices, to

prevent unauthorized access and misuse of biometric information. Personal biometric data is sensitive, and some consumers may approach this newer technology with trepidation. There is always some risk that personal data could be stolen or that it could lead to identity theft or bank fraud. Stringent data protection measures are essential to safeguard people's personal information and address privacy issues. Physical and behavioral biometrics are becoming a more critical component of the zero-trust security model, which assumes all network traffic is malicious.

- *Complexity:* There is implicit technological complexity to biometric payments. Any well-built biometric payment system requires a software solution that is both secure and user-friendly. And while hardware options are fairly well-established in smartphones, non-phone-based biometrics are more difficult to execute. Because the technology is new, standards are still being established, making manufacturing complex and implementation expensive. This can act as a deterrent for merchants.
- *Social Acceptance:* There is the element of social acceptance. Some cultures and communities may not accept or be appropriate for biometric technology, and some people may feel uncomfortable supplying their biometric information. Privacy concerns vary greatly between individuals as well as more broadly across demographics and cultures. There is a noticeable difference in acceptance rates between age groups. General acceptance and comfort with biometric technology are crucial for its widespread adoption and depend on ease of use and established trust.
- *Customer Education:* While concerns regarding data privacy and security are valid, advancements in technology and a commitment to user education can pave the way for a future where these anxieties are effectively addressed. Educating customers about the benefits and security measures surrounding biometric banking is crucial. Transparency and clear communication will help alleviate any anxieties and encourage wider acceptance.
- *Transparency:* Communicate how biometric data is collected, stored, and used. Customers have the right to understand how their information is being handled.
- *Accuracy:* No biometric technique is 100% accurate, and false positives or false negatives are always a possibility. Accuracy can be impacted by external elements like lighting, background noise, and the biometric sensor's quality.
- *Cost:* While biometric devices are becoming more affordable, the initial setup for biometric payment systems can be costly. Businesses need to invest in the necessary hardware and software, and it can be expensive to integrate these systems into payments and information technology (IT) infrastructures. Implementing and maintaining biometric technology can be expensive, particularly for large enterprises or governmental institutions.
- *Emerging Technologies:* Biometric payment systems are likely to become more integrated with other emerging technologies such as blockchain, Internet of Things (IoT), and artificial intelligence (AI). The convergence of artificial intelligence with biometric authentication represents perhaps the most transformative trend in banking security. Modern biometric systems increasingly incorporate sophisticated machine learning algorithms that continuously improve accuracy and security.

CONCLUSION

Biometrics refers to the use of unique physical or behavioral traits to identify and authenticate individuals. Biometrics in finance uses unique physiological and behavioral characteristics like fingerprints, facial recognition, and voice recognition to authenticate users and secure financial transactions. Biometric technology is an automatic or computerized technique that plays a vital role in security and recognition. It has become very popular. It reduces the chances of theft and misuse of financial data due to each user's unique information and its impossibility to copy. Today, all reliable banking service providers use biometrics. The integration of biometric verification into banking systems offers a compelling proposition for both financial institutions and their customers. By leveraging this powerful technology, banks can create a more secure and efficient banking environment.

The outlook for biometric payments is marked by continuous innovation, with advancements poised to address current challenges and expand the technology's applications. The future of banking is undeniably biometric. This powerful technology offers a shift from traditional authentication methods. In our ever-digitizing world, biometric payments are on the fast track to become a future standard. As shown in Figure 7, biometrics is the future of banking [7]. More information on biometrics in finance can be found in the books in [12,13].

REFERENCES

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

[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] "The evolution of biometrics: A comprehensive guide to modern authentication methods in combating financial crimes," March 2025, https://financialcrimeacademy.org/the-evolution-of-biometrics/

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

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

[8] H. Akiode, "The future of biometrics in banking," May 2024, https://youverify.co/blog/the-future-of-biometrics-in-banking

[9] "Biometrics," May 2023, https://www.investopedia.com/terms/b/biometrics.asp

[10] "What are biometric payments? A quick guide for businesses," April 2024, https://stripe.com/en-br/resources/more/what-are-biometric-payments-a-quick-guide-for-businesses

[11] "Biometric authentication: The future of secure fintech transactions," https://easternpeak.com/blog/biometric-authentication-in-financial-services/

[12] W. Rodgers, *Biometric and Auditing Issues Addressed in a Throughput Model*. Information Age Publishing, 2011.

[13] K. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press, 2011.

Figure 1 Some business executives [1].

Figure 2 A presentation of biometrics [2].

Figure 3 Fingerprint biometrics [4].

Figure 4 Facial recognition biometrics [5].

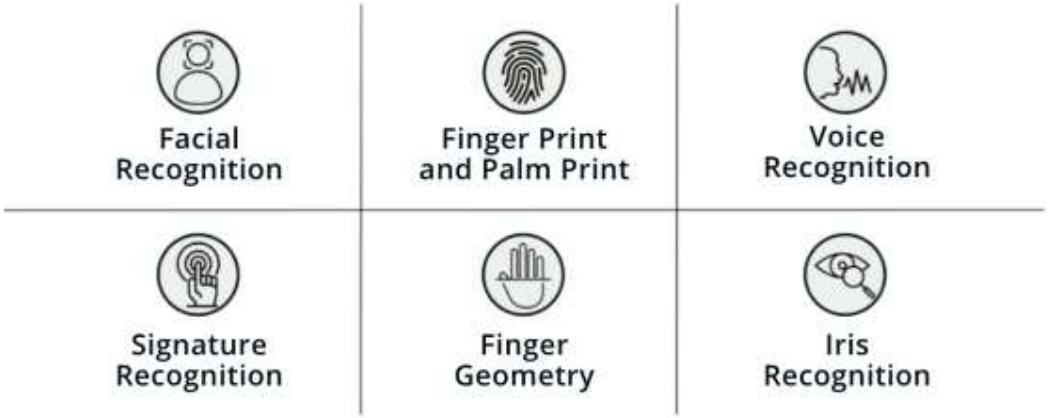

Figure 5 Types of biometric authentication [6].

Figure 6 Some benefits of biometrics [11].

Figure 7 Biometrics is the future of banking [7].