IJAAR PUBLISHING®

International Journal of Advanced Academic Research | ISSN: 2488-9849
Vol. 11, Issue 8 (2025) | www.ijaar.org

Fingerprint Biometrics for Fraud-Resistant ATM Access in Underserved Communities

Olawale Teslim Williams
Stalls Lion Plaza, Marina, Lagos
Wale_77@yahoo.com

Abstract

Identity verification has become an essential aspect of people's everyday lives. Common scenarios requiring identification verification encompass accessing online accounts or computers, making transactions at Automated Teller Machines (ATMs), and gaining entry to buildings or banks. Various methods can be employed to validate a person's identity. While passwords have traditionally served as the most common security mechanism, they are becoming increasingly obsolete as biometrics demonstrate promise in addressing the identity theft epidemic. Nonetheless, traditional ATM access using cards and PINs is vulnerable to skimming, theft, and identity fraud—leaving seniors, immigrants, and low-income users especially at risk. This study explores the deployment of fingerprint-enabled ATMs as a cardless, PIN-less alternative, analyzing its effectiveness in reducing fraud, improving access, and enhancing user trust among the underserved communities. Leveraging on real-world implementation the paper shows how fingerprint biometric authentication significantly reduces fraud and concludes with recommendations for application in U.S. community banking environments, offering a scalable solution that blends technology with dignity.

Keywords: Biometric ATMs, Fraud Resistance, Financial Inclusion, Underserved Populations, Fingerprint Authentication.

Olawale, T. W. (2025). Fingerprint Biometrics for Fraud-Resistant ATM Access in Underserved Communities. *International Journal of Advanced Academic Research. 11*(8), 93-101. DOI: https://doi.org/10.5281/zenodo.17432724

1. Introduction and Background

In the submission of Alsolami (2019), fingerprint data has long been an authentication tool in credit card systems. Gottfried et al. (2001) discovers remote credit card authentication system by using a fingerprint authentication at the point of sale. Then the credit card company verifies the probe fingerprint by the gallery fingerprint stored in the database (Alsolami, 2019). The communication between the point of sale and the central database is in encryption form. Baratelli (2001) invents a smart card with a fingerprint integrated reader. When a user inserts the smart card into a reader/writer, the scan machine asks for a user fingerprint. Then the smart card compares the user finger- print and give the matching result. If the matching is true, the card is enabled, and the user can access to information. Smith [nd] originates a biometric anti-fraud plastic card, which requires a user to use his/her fingerprint for authentication. The plastic credit card compares the probe fingerprint against the gallery fingerprint stored in the plastic credit card. If the matching is true, the card is enabled, and the user can access information. Oshima et al. [nd] formulates a card settlement method using a portable electronic device that has a fingerprint sensor. Chou et al. [2008] invents a cardtype biometric that includes a biometric sensor to read the biometric data of a user and includes an operating/processing system to process the biometric data. Harris [2008] creates an intelligent credit card system to improve biometric reading and other operations in a credit card system. Vogel et al. [2017] produces a flexible card with a fingerprint sensor and circuit chip to manage the communication with the fingerprint sensor. Muley et al. [2018] presents an ATM system that uses fingerprint identification for money transactions that requires the ATM to have a fingerprint scanner.

In recent years, credit and debit cards have become a very convenient method of payment (Alsolami, 2019). The growing use of card payments, hereafter referred to as credit cards, is evident in the daily use with many applications, such as withdrawing money from an Automated Teller Machine (ATM) and making payments in a store.

With the escalation in demand for safe money transfer transactions, there is a shift from conventional PIN-based ATM security mechanisms to biometric systems (Kalpana, 2025). Most ATM systems for secure access have relied on the stolen ATM card and PIN methods, which are prone to a battalion of security threats such as skimming, hacking, and PIN theft. Fingerprint authentication then becomes one of the major emerging biometric solutions to address these problems by providing better security and convenience (Kalpana, 2025).

According to Srilakshmi et al (2024), ATM security has become a critical concern due to the increasing incidents of fraud, card skimming, and unauthorized access. Traditional ATM authentication methods, such as PIN-based verification and magnetic stripe cards, are vulnerable to theft and hacking. To address these security challenges, this study proposes a Biometric Authentication System for ATM Transactions Using Fingerprint Recognition (Srilakshmi et al, 2024). The system utilizes fingerprint biometrics as a unique and secure authentication mechanism, eliminating the need for PINs and physical cards. The proposed approach integrates high-resolution fingerprint scanners with a secure encryption framework, ensuring accurate user verification and preventing identity theft. The system is designed to operate in real-time, offering faster transaction processing, reduced fraud risks, and enhanced user convenience. Experimental results demonstrate the system's high authentication accuracy, minimal false acceptance rates, and improved security compared to conventional ATM systems.This employs tree-based classification algorithms to determine fingerprint features, such as ridge patterns and minutiae points, thus enabling accurate and reliable

authentication of users (Kalpana, 2025). The ensemble classifiers profited boost in classification accuracy and reduced overfitting, thus increasing the robustness of the developed system. The successful authentication of fingerprints has given access to safer functionalities at ATMs-adverse to the fraud risks prevalent for all other methods. With the implementation of blockchain technology, it assures integrity of transactions data, along with transparency and protection from alteration owing to the immutable ledger of transactions (Kalpana, 2025). The accountability brought about by the decentralized nature of blockchain makes ATM transactions secured and reliable.

The global rise in technological application to financial transaction and management has brought into force many types of equipment that aim at more customer satisfaction. Thus, ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share (Rani, 2025). Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure (Rani, 2025).

2. The Problem

Security of ATMs relies on a variety of authentication methods to verify user identity or ensure the integrity of transactions. The traditional PIN-based authentication faces mostly threats that jeopardize its very foundation, including card skimming, pin thefts, and software breaches, amongst others. Presently, ATM authentication methods are prone to risks such as card theft, skimming, PIN breaches, and fraud, making them vulnerable to unauthorized access.

Despite the great advantages of credit card and new payment technologies, security and privacy are still highlighted concerns for banks and customers (Alsolami, 2019). The most common concern is fraud, where the credit card information is impersonated. Many secure schemes are proposed in literature to improve the security and privacy. Whitworth [2001] invents a credit card resistant fraud system using encryption that encrypts credit card on computing devices. Bezos et al. [1998] invents a secure method of communicating credit cards over a non-secure network where the exchanging message between the merchant and customer contains a portion of each credit card numbers. Then the customer confirms in a return message which credit card can be used. Wong et al. [1999] invents a method to secure a credit card transaction over the internet by inserting a user key into the user account with a permutation variable. In each use, the permutation variable is changed, and the algorithm generates a new number. During the verification process, the permutation variable must be valid at the time of use. Stanfield et al. [2013] invents a dynamic card verification on credit transaction by requiring a Card Verification Value (CVVs) be provided from a secure wallet, which is software on the client side (Alsolami, 2019). This CVVs is used when no physical card is presented while shopping. Even though these schemes have solved many issues in credit card systems and financial transactions, other issues remain research challenges.

3.0 Conceptualization of Terms

3.1 Fingerprint Biometrics

Biometrics have often been identified as the next-generation identity verification method in a variety of applications such as border control, building access, computer login, municipal

services, healthcare services and commerce.Biometrics encompasses measures that quantify human attributes, with biometric identifiers serving as distinct, quantifiable characteristics used to categorize and identify individuals (Janaki et al, 2024). Biometric security is a mechanism that dramatically enhances the integrity, confidentiality, and availability of information (Ahmad et al. 2012, in Ogunjide et al, 2025). The use of biometric may help to protect both logical and physical access constraints. Logical access controls safeguard network facilities, computers, and information systems from unauthorised access (Jain et al. 2006 in Ogunjide et al, 2025), whereas physical access controls guarantee that only approved individuals can access IT infrastructures and document storage (Jain et al. 2006 cited by Ogunjide et al, 2025). This emphasises the importance of biometric and its usefulness for ensuring efficient running of systems and operations (Ogunjide et al, 2025).

Behavioural biometrics on the other hand include rhythm, gait, and voice, while physiological biometrics encompass fingerprints, facial features, the iris, and finger veins (Janaki et al, 2024). Each modality has its own set of advantages and drawbacks, and some are currently in high demand. Chaure and Sahu (2015) therefore argued that biometric systems provide access control to both physical assets like ATMs and logical information using biometric metrics such as fingerprints. These systems are considered more advantageous and futuristic technology because they are more resistant to fraud.

Since the emergence of science and technologically dominated era, it is imperative for robust personal authentication in electronic information systems becomes increasingly evident. Hence, a secure and dependable solution to address this need is biometric authentication (Janaki et al, 2024). Due to their intrinsic features of being universal, unique, and fraud-resistant, finger vein-based recognition systems have gained importance. Veins provide an efficient barrier against misleading methods since they are buried under the skin and undetectable to human sight. While many researchers focus on advanced technology for finger-vein-based authentication systems, existing research has often overlooked significant challenges, such as short datasets, high computational complexity, and a lack of efficient and lightweight feature descriptors (Janaki et al, 2024).

Ultimately, Wayman et al (2005) noted that the performance of a biometric authentication system, and its suitability for any particular task, will depend upon the interaction of individuals with the automated mechanism. It is this interaction of technology with human physiology and psychology that makes “biometrics” such a fascinating subject.

3.2 A Literature Review of Fraud-Resistant

Fraud is the most pressing issue in credit card systems and bank transactions. Many schemes have been introduced in literature to detect fraud in a credit card system (Alsolami, 2019). Chan et al. [1999] provides a survey, evaluates the fraud detection techniques, and proposes a method that combines a fraud detector with a “cost model” to get significant results. They divide the large data set into small subsets and apply data mining technique to generate classifiers in parallel. Brause et al. [1999] presents a credit card fraud detection system by using a data mining technique with a neural network to achieve antifraud against credit cards. They apply data mining and a neural network algorithm on a given credit card transaction database to discover fraud attempts. Flitcroft et al. [2009] invents a secure method that provides remote access a limited use number to reduce chances of credit card fraud. The access requires user authentication and another entry to validate the user. Wang et al. [2018] uses secondary verification to improve the accuracy of fraud detection. Then they perform an optimization experiment by applying the secondary verification using different threshold values. Carcillo et al. [2018] and Alsolami (2019) proposes a scalable real-time fraud finder

(SCARFF) which implements machine learning with big data tools like Spark. The result of their experiment shows accurate fraud detection with a scalable system. Finally, Wang et al. [2018] uses distributed deep learning for credit card fraud detection which provides end-to-end privacy.

3.3 Underserved Communities

According to Mori (2019), millions and millions of consumers can be labelled as "underbanked", not only in fragile areas but also in industrialized countries, and surveys are likely to underestimate such a disappointing situation: it is due to both supply and demand factors resulting in a limited provision of financial services to the market segments that can be devised accordingly and that include both households and firms, mostly micro- and small-sized enterprises; to make things worse, a significant share of the world population is said "unbanked", thus leading to shed light on people who do not even have their own bank accounts and often resort to expensive check-cashing services. For sure, this scenario is not consistent with the Sustainable Development Goals (SDGs) that have been adopted by the United Nations (UN) in 2015 while setting the "2030 Agenda" and that seek to complete what the Millennium Development Goals did not achieve, particularly in reaching the most vulnerable (UN, 2015).

4. Benefits of Biometrics-Centred model to Financial Inclusivity of the underserved Communities

Since many financial institutions strongly depend on customer trust and convenience (see McIntosch 2009 in Breebaart et al, 2011).Biometricscan play an important role to prevent the inconvenience that results from card fraud, and have the potential to increase trust for electronic payments. A second convenience-related motivator to use biometrics that has often been mentioned is not having to remember a PIN, or even not having to present a debit/credit card. For many people and particularly elderly, PINs can be difficult to remember, especially if different PINs have to be remembered for different cards. This in turn results in a security risk of customers writing down their PINs on a card or on a small piece of paper kept in their wallet. It has also been shown that if people are permitted to choose their own passwords or PINs, they tend to select ones that are easily guessed or are the same across bank cards (Gong et al. 1993 cited by Breebaart et al, 2011).

A third benefit of biometrics that is often being reported is the one of cost reduction. Point-of-sale terminals may decrease their transaction time, resulting in a faster throughput of customers. Suggested reduction of transaction times between 10% up to 70% have been reported in the past (Banking Automation Bulletin, 2009, Boyle, 2006 all in Breebaart et al, 2011). Furthermore, costs associated with forgotten PINs and associated cards that have to be renewed may be reduced.

A quick look at the "2030 Agenda" is enough to grasp statements of special interest in sight of furthering financial inclusion. It is not a case that the 17 SDGs deal with economic growth, sustainable communities, reduced inequalities, industry, innovation and infrastructure, as well as multi-stakeholder partnerships aimed at mobilizing and sharing knowledge, expertise, technology and financial resources; all of these goals have been associated with specific targets to be achieved in the 15 years covered by this document and are supported by a set of actions that can be taken in everyday life as a contribution to a better worldMori (2019).Thus, through biometric authentication in conjunction with blockchain security, this system

provides a completely seamless and secure ATM experience, as well as efficiency in the operations while safeguarding users' identities and financial assets.

The conceptual thoughts that have been outlined so far lead to focus on financial infrastructure inclusion: it “means that individuals and enterprises can access and use a range of appropriate and responsibly provided financial services offered in a well-regulated environment”, according to the UN Capital Development Fund (UNCDF, 2016); a closely linked viewpoint emphasizes financial resilience as the declared, feasible capacity to survive financial shocks and to obtain money for unexpected expenses. To sum up, “inclusive finance strives to enhance access to financial services for both individuals and micro-, small and medium-sized enterprises” Mori (2019), as a way to reduce poverty, tackle inequality and foster growth.

5. Concluding Remarks and Recommendations

Conclusions imply that a more inclusive financial system would provide benefits to the underbanked (not to mention the unbanked), as well as to society at large, with financial competence, literacy and education set to gain momentum.

This paper fills a gap in U.S./global literature on biometric ATM deployment by focusing on the human-level impact—particularly for marginalized user groups—and offering a tested model for American institutions to adopt. It also directly addresses systemic vulnerabilities in ATM fraud, aligning with consumer protection and inclusion objectives. Considering the above, the following are recommended.

While facial recognition-based ATM authentication presents a promising advancement, further improvements can enhance its accuracy, security, and adaptability. There should be future developments that can focus on improving recognition under challenging conditions, such as poor lighting, extreme facial angles, aging effects, and the use of accessories like masks or glasses. Integrating multi-factor authentication (MFA), such as combining facial recognition with fingerprint scanning, voice recognition, or behavioral biometrics, could further strengthen security.

Also, there should be another key area of enhancement in the use of AI-driven anti-spoofing techniques, which can detect and prevent fraudulent attempts using photos, videos, or 3D masks.

Additionally, there should be exploring of cloud-based biometric databases that can improve scalability, efficiency, and real-time processing, enabling faster authentication across multiple ATM locations. Blockchain technology could also be considered for secure and tamper-proof storage of biometric data. Moreover, ensuring compliance with data privacy regulations such as GDPR and biometric security laws is crucial to gaining public trust and preventing biometric data breaches.

For widespread adoption, user education and awareness programs should be implemented to address privacy concerns and help users understand the security benefits of facial recognition. Future research can also explore cost-effective hardware solutions to make this technology affordable and accessible across different banking sectors worldwide. With continuous advancements, facial recognition-based ATMs can set a new benchmark for secure, convenient, and fraudproof banking systems in the future.

References

Alsolami, F. (2019). BioPay: Your fingerprint is your credit card. International Journal of Advanced Computer Science and Applications, 10(1).

Alsolami, F., Bayan, A., & Terranee, B. (2018). Cloud-IDScreen: Secure fingerprint data in the cloud. Identity, Security, and Behavior Analysis (ISBA), 2018 IEEE 4th International Conference on. IEEE.

Baratelli, P. J. (2001). Smart card with integrated fingerprint reader. U.S. Patent No. 6,325,285. 4 Dec.

Bezos, J. P. (1998). Secure method and system for communicating a list of credit card numbers over a non-secure network. U.S. Patent No. 5,715,399. 3 Feb.

Breebaart, J., Buhan, I., de Groot, K., & Kelkboom, E. (2011). Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure. Electronic Commerce Research and Applications, 10(6), 605-614.

Brause, R., Langsdorf, T., & Michael, H. (1999). Neural data mining for credit card fraud detection. Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on. IEEE.

C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet, & K. Ko. (2004). User's guide to non-export controlled distribution of nist biometric image software.

Carcillo, F., et al. (2018). SCARFF: A scalable framework for streaming credit card fraud detection with spark. Information fusion, 41, 182-194.

Chan, P. K., et al. (1999). Distributed data mining in credit card fraud detection. IEEE Intelligent Systems and Their Applications, 14(6), 67-74.

Chaure, M., & Sahu, A. (2015). Biometrics as a Security System - An Overview. International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), 9.

Chou, B. C. S. (2008). Card-type biometric identification device and method therefor. U.S. Patent No. 7,424,134. 9 Sep.

D. Maltoni, D. Maio, A. K. Jain, & S. Prabhakar, (2009). Handbook of fingerprint recognition.

Flitcroft, D. I., & Graham, O. (2009). Credit card system and method. U.S. Patent No. 7,567,934. 28 July.

Gottfried, O. (2001). Remote credit card authentication system. U.S. Patent No. 6,270,011. 7 Aug.

Harris, S. C. (2008). Intelligent credit card system. U.S. Patent No. 7,360,688. 22 Apr.

Janaki, K., Srinivasan, C., & Hema, M. A. (2024). FPGA-enhanced system-on-chip for finger vein-based biometric system using novel DL model. Integration, 98, 102231.

Kalpana, K. (2025). Secure Fingerprint Authentication in ATM Transaction using Blockchain Technology. In 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 674-678). IEEE.

Mori, M. (2019). Banking underserved market segments. Open Journal of Social Sciences, 7(03), 506.

Muley, A., & Vivek, K. (2018). Prospective solution to bank card system using fingerprint. 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE.

Ogunjide, J. O., Olalekan, A. A., Agboola, O. K., & Adamaagashi, I. P. (2025). Relationship Between Biometric Technology and Customer Satisfaction in the Fintech Sector. International Journal of Economics and Business Management, 11(4), 190-204.

Oshima, S., et al. Card settlement method using portable electronic device having fingerprint sensor. U.S. Patent Application No. 10/542,888.

Rani, K. M. K. V. J. (2025). Enhancing ATM Security Through Biometric Face Recognition. International Journal of Advanced Research in Education and Technology (IJARETY), 12(2), 687-694. DOI:10.15680/IJARETY.2025.1202047

Smith, R. Biometric anti-fraud plastic card. U.S. Patent Application No. 11/233,412.

Srilakshmi, C., Sravani, S., Sekhar, M. R., & Anjaneya Prasad, K. (2024). Biometric Authentication for ATM Transactions Using Fingerprint Recognition. Journal of Computational Analysis & Applications, 33(4).

Stanfield, M., George, T., & Joseph, V. (2013). Dynamic card verification values and credit transactions. U.S. Patent No. 8,567,670. 29 Oct.

Vogel, K., & Lyn, J. (2017). Flexible card with fingerprint sensor. U.S. Patent No. 9,792,516. 17 Oct.

Wang, D., Bintong, C., & Jing, C. (2018). Credit card fraud detection strategies with consumer incentives. Omega.

Wang, Y., et al. (2018). Privacy Preserving Distributed Deep Learning and Its Application in Credit Card Fraud Detection. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An Introduction to Biometric Authentication Systems. In J. Wayman, A. Jain, D. Maltoni, & D. Maio (Eds.), Biometric Systems. Springer, London. https://doi.org/10.1007/1-84628-064-81

Whitworth, B. (2001). Fraud resistant credit card using encryption, encrypted cards on computing devices. U.S. Patent Application No. 09/764,369.

Wong, J. Y., & Roy, L. A. (1999). System for secured credit card transactions on the internet. U.S. Patent No. 5,956,699. 21 Sep.