

Blocking Credit Card Theft through Biometric Authentication Systems

Osuagwu O. E., FNCS, Kembe N., Ge T., Oliver O. Osuagwu

^{1,2,3}(Department of Hardware Engineering, South Eastern College of Computer and information Technology, Egbu, Owerri North, Nigeria)

⁴(Department of Software Engineering, South Eastern College of Computer and information Technology, Egbu, Owerri North, Nigeria)

Abstract:

Nigeria's e-commerce ecosystem remains critically impaired by the absence of a secure, dependable, and globally interoperable payment infrastructure. Cross-border procurement is still trapped in rigid Central Bank of Nigeria and Nigerian Customs Service protocols designed to curb capital flight, yet these measures have unintentionally suffocated digital openness, slowed market liberalization, and constrained Nigeria's ability to compete in international commerce. The long-standing epidemic of credit card theft—responsible for millions of dollars in losses annually continues to undermine trust, delay adoption, and destabilize the foundation required for modern electronic transactions.

Although pioneering institutions such as Kuda Microfinance Bank, Zenith Bank and UBA bank have introduced credit card payment systems, the digital environment they operate in has become significantly more hostile. Nigeria now faces escalating cyber-fraud attacks, increasingly sophisticated identity theft networks, fragmented payment platform interoperability, inconsistent KYC enforcement, and slow regulatory adaptation to emerging digital threats. These compounding vulnerabilities threaten not only consumer confidence but the structural viability of Nigeria's digital economy.

This paper advances an uncompromising solution: the deployment of next-generation biometric authentication systems including vein pattern recognition, fingerprint biometrics, and vascular imaging to decisively neutralize credit card theft and establish a high-assurance security layer across Nigeria's financial infrastructure. The authors argue that without biometric integration, Nigeria's e-commerce sector will remain exposed, fragile, and unable to scale. With proper implementation, however, biometric authentication can transform the nation's payment ecosystem, fortify transaction security, restore public trust, and accelerate the emergence of a resilient, fraud-resistant, and globally competitive digital economy.

Key Word: *E-commerce security in Nigeria, Digital payment infrastructure, Cross-border transaction barriers, Central Bank of Nigeria regulations, Nigerian Customs Service protocols, Credit card fraud epidemic, Cyber-fraud escalation, Identity theft networks, Payment platform interoperability, KYC compliance challenges, Regulatory modernization gaps, Biometric authentication systems, Fingerprint biometrics*

1.0 Introduction

Credit card identity theft remains one of the most persistent threats to digital commerce worldwide, and Nigeria has not been spared. Internet fraudsters—popularly known as 419 continue to exploit weaknesses in traditional authentication systems, causing financial losses that run into millions of dollars annually. A well-known case illustrates the sophistication of such criminals: a hacker obtained a copy of Forbes magazine listing America's 400 richest individuals, complete with social security numbers, birth dates, and partial credit card details. He supplemented this information with data illegally acquired from credit bureaus such as Equifax, Experian, and TransUnion, using forged investment-bank letterheads (Jain & Pankanti, 2006).

Armed with these details, the fraudster used public library computers to order merchandise, withdraw funds from brokerage accounts, and apply for credit cards under stolen identities. His spree ended only when he attempted to transfer US\$10 million from the Merrill Lynch account of software entrepreneur Thomas Siebel. Investigators noticed that two Yahoo email addresses—both linked to the same individual—had been used across multiple

unrelated client accounts. In March 2001, New York detectives arrested the perpetrator, bringing an end to one of the most sensational identity-theft operations in modern history.

Today, similar patterns of fraud continue, but with far more advanced tools. Nigeria has witnessed a surge in SIM-swap fraud, compromised POS terminals, large-scale phishing campaigns, and synthetic identity creation. The Nigerian Inter-Bank Settlement System (NIBSS) reported a significant rise in digital fraud attempts between 2021 and 2024, particularly targeting card-not-present transactions and high-volume POS merchants. These trends highlight the urgent need for stronger authentication mechanisms.

1.1 The Problem with Modern Credit Cards

Current credit card authentication systems validate possession or knowledge, not identity. Anyone who can reproduce a cardholder's PIN, password, or physical card can impersonate them. Passwords and PINs are easily guessed using personal information such as birth dates, license plate numbers, or even pet names. Patient thieves gather fragments of data from social media, discarded mail, or poorly secured databases and eventually assemble enough information to inflict severe financial damage. Most common crisis that should be monitored by business or printing centers in colleges etc, Most of this criminals extract data from applicants who might use a public computer to post their resume for job interview or government fund allocation programs.

Social engineering remains a powerful weapon: fraudsters manipulate banking staff, exploit customer service channels, and harvest unshredded documents to build detailed profiles of victims. According to the U.S. Federal Trade Commission, credit cards account for approximately 67% of identity theft cases.

Despite these challenges, deploying biometric authentication systems in Nigeria supported by modern facial recognition and OTP verification for high-volume POS transactions offers a realistic pathway to eliminating identity fraud and strengthening e-commerce adoption.

2.0 Biometric Authentication Systems (BAS)

Biometric Authentication Systems (BAS) represent a modern approach to verifying identity using unique human traits such as fingerprints, iris patterns, facial geometry, and vascular structures. These systems are increasingly used in airports, banks, corporate environments, and digital commerce platforms.

Vascular recognition has gained global acceptance. South Korea's international airports use vein-pattern screening, while several Canadian airports deploy vascular scanners for tarmac access. In Japan, more than a dozen banks have installed ATMs equipped with palm-vein sensors developed by Fujitsu and TechSphere. These systems use near-infrared light to capture vein images, convert them into encrypted templates, and match them against stored records within seconds.

Early adopters preferred smart cards that store biometric templates directly on embedded chips, reducing the need for centralized databases and enhancing privacy. Vascular recognition is often favored over fingerprint scanners in cultures where hygiene concerns discourage physical contact with sensors.

Privacy concerns remain, particularly regarding potential misuse of biometric data. However, modern best practices—such as storing only encrypted templates rather than raw biometric images—significantly reduce risks.

Biometric authentication is no longer experimental; it is a global standard. Nigeria must embrace it to build trust in electronic fund transfers and e-commerce.

2.1 Variants of BAS

i.. **Fingerprints:** Fingerprint authentication has ancient roots, dating back to Babylonian clay tablets. Modern systems analyze both global ridge patterns and minutiae points. Scanners may be embedded in devices or connected via USB.

ii. **Iris Scans:** Iris recognition offers extremely high accuracy due to the complexity of iris vein patterns. Users align their eyes with a scanner, which captures and analyzes the pattern to generate a secure template.

iii. **Biometric Sensors (Hybrid Systems):** Jain and Pankanti (2006) proposed hybrid biometric sensors combining fingerprints with other modalities. These systems enhance privacy, reduce fraud, and support secure transactions across physical stores, telephone orders, and online platforms.

iv. **Advanced Facial Recognition (New Addition):** Recent advancements in AI-driven facial recognition—particularly deep-learning models such as FaceNet, ArcFace, and Vision Transformers—enable real-time identity verification at POS terminals, ATMs, and mobile banking apps. Facial recognition is now used by several African fintech companies to prevent account takeovers and authenticate high-risk transactions.

V. **OTP Verification for High-Volume POS Transactions (New Addition):** Oliver Obilor Osuagwu (2026) proposed integrating OTP verification into high-volume POS transactions to reduce fraud in merchant environments prone to card skimming and terminal compromise. This hybrid approach biometrics + OTP creates a multi-layered security framework that significantly reduces unauthorized card usage. Reference information can be found in Vol, 27(2), P.166 *West African Journal of Industrial and Academic Research*.

2.2 BAS Trials Worldwide

Several institutions have experimented with biometric credit cards. Since 2004, Bank of Tokyo-Mitsubishi has issued Visa cards embedded with palm-vein chips. Their ATMs match live vein scans with encrypted templates stored on the card. The main limitation remains merchant adoption, as most POS terminals lack compatible scanners.

Companies such as BioPay LLC and Pay By Touch allow shoppers to pay using fingerprint sensors at cash registers. Millions of Asian smartphones now include fingerprint sensors for secure device access and mobile payments. The global biometrics market continues to grow, driven by demand for secure authentication in finance, healthcare, and transportation.

3.0 Technology Components for Sensor-Based BAS

To activate a biometric smart card, users load fingerprint images onto the card using embedded micro-capacitor sensors. These sensors measure capacitance differences between fingerprint ridges and valleys, generating a digital image. A microprocessor extracts minutiae points, encrypts them, and stores the template in flash memory.

During transactions, POS terminals establish secure communication with the card and the credit card company's database. The system verifies card status, matches biometric templates, and authorizes payments.

For online transactions, users enroll their biometric data through secure PC sensors and install certified protocol plug-ins. The plug-in matches live scans with encrypted templates stored locally and sends a certified digital signature to the credit card company.

4.0 Deployment Strategy for Nigeria

Nigeria requires a public-private partnership to build a unified smart-card infrastructure with strong security standards. The Federal Government should establish an e-commerce and credit-card development commission to coordinate indigenous production of smart cards, biometric sensors, and transaction-management systems. This commission should collaborate with banks, fintech companies, NIBSS, and international security experts to ensure interoperability, fraud resistance, and regulatory compliance.

5.0 Conclusions and Recommendations

Biometric authentication systems are essential for combating identity theft and strengthening Nigeria's digital economy. Integrating advanced facial recognition, vascular imaging, fingerprint sensors, and OTP verification into credit card systems will significantly reduce fraud, restore consumer confidence, and accelerate e-commerce adoption.

Nigeria must urgently deploy BAS technologies to protect citizens, support financial institutions, and position itself competitively within the global information society.

References

- [1]. Osuagwu, O.O., 2026. Advanced Facial Recognition And OTP Verification In High-Volume POS Transactions. *West African Journal of Industrial and Academic Research* vol, 27(2), p.166.
- [2]. National Identity Management Commission (NIMC), 2026. President Tinubu signs NIMC Act 2026 into law, ushering in a new era of secure digital identity for Nigeria. NIMC Press Release, 26 June.
- [3]. Burt, C., 2026. Nigeria's ID authority takes on new duties to secure growing digital ecosystem. *Biometric Update*, 21 July.
- [4]. Admin, 2026. Nigeria Modernises Its Digital Identity Ecosystem: Analysis of the National Identity Management Commission (Establishment) Act, 2026. *Regulatory Updates*, 23 July.
- [5]. Oparada, P., 2026. Nigeria's New Identity Law: 11 Key Things to Know as Enforcement Begins. *Legit.ng*, 3 July.
- [6]. Eleanya, F., 2026. Nigeria's new identity law turns NIMC into the country's digital trust authority. *TechCabal*, 2 July.
- [7]. Jain, A.K. & Pankanti, S., 2006. A Touch of Money. *IEEE Spectrum*, July.
- [8]. Weaver, A. C. (2006). Biometric authentication. *Computer*, February 2006.
- [9]. Jain, A. K., & Pankanti, S. (2006). A Touch of Money. *IEEE Spectrum*, July 2006.
- [10]. NIBSS (2024). Annual Fraud Report: Digital Payment Fraud Trends in Nigeria.
- [11]. Kaspersky Labs (2023). Africa Digital Fraud Landscape Report.
- [12]. Fujitsu (2022). PalmSecure Technology Overview.
- [13]. Central Bank of Nigeria (2023). Guidelines for Contactless Payments and Biometric Verification.
- [14]. National Cholesterol Education Program (NCEP) Expert Panel on Detection, Evaluation, and Treatment of High Blood Cholesterol
- [15]. Jones, W. D. (2006). Blood Test: Vascular Patterns Provide New Means of Identification and Authentication. *IEEE Spectrum*, November 2006.