Jagua Publication

*Computational Methods, 3(1):8–17, 2026. DOI: 10.58614/cm312*

**Computational Methods**

*Journal homepage: https://www.jpub.org/journal-details.php?journal-id=43*

***Research Article***

# A comprehensive analysis on the implementation of Multifactor Authentication for online banking systems in Nigeria

**Samuel Okure[1], Israel Umana[1], Ofonime Okon Dominic[1], Emmanuel Udoiwod[1], Florence Atakpo[1] and Bliss Utibe-Abasi Stephen[1,2*]**

[1] *Computer Engineering, University of Uyo, Uyo, Akwa Ibom State, Nigeria.*
[2] *TETFund Centre of Excellence in Computational and Innovation Research, University of Uyo, Nigeria.*
[*] *Corresponding author: blissstephen@uniuyo.edu.ng*

**Article Info**

***Keywords:*** *Nigeria Banking Sector, Multi-Factor Authentication (MFA), Cybersecurity, Online Banking Security, Digital Transformation.*

***Received:*** *23.01.2026;*
***Accepted:*** *15.03.2026;*
***Published:*** *21.03.2026*

© *2026 by the author's. The terms and conditions of the Creative Commons Attribution (CC BY) license apply to this open access article.*

**Abstract**

Nigeria's banking sector has grown rapidly through digital transformation, but this growth has also brought more cybersecurity threats. Because of this, multifactor authentication (MFA) has become an essential layer of protection. This study looked at how major Nigerian banks use MFA by evaluating them with four measures — SMSS, ISI, FDS, and OWS — based on regulatory information and a structured scoring system. The findings show a clear divide: bigger banks like Access, Zenith, and GTBank use stronger authentication methods such as biometrics and hardware tokens, while many smaller banks still depend mainly on simple SMS or email codes. Overall, the banks were grouped into top, mid, and low adopters, highlighting that MFA usage across the sector is still uneven. This research adds to existing knowledge by offering a focused look at MFA in Nigerian online banking, an area that has not been studied as much compared to developed countries. It also introduces the Security Mechanism Strength Score (SMSS) as a new way to evaluate MFA readiness, ranking banks into Low, Mid, and Top Tiers. These insights are useful for regulators, policymakers, and researchers, and they emphasize the broader importance of secure digital banking for society.

## 1. Introduction

Nigeria's large population [1] and the increasing volume of daily transactions have made its financial system very crucial to economic growth [2]. Mobile and internet banking has been widely adopted due to their efficiency and accessibility, supported by innovations such as ATM cards and PINs [3]. However, they also introduce risks, particularly in payment and settlement systems, where users often fall victim to phishing, cloned applications, and malware. In response, the Central Bank of Nigeria (CBN) mandated Two-Factor Authentication (2FA) under the Payments System Vision 2020 [4] to address these issues.

Nigeria's banking industry is trying to offer smooth digital services while also keeping customers safe from rising cyber threats. Multifactor Authentication (MFA) offers a stronger level of protection by using more than one verification method—like passwords, biometrics, or device confirmations. But its adoption in Nigeria is still slow. Many banks struggle with poor infrastructure, low public awareness, and the high cost of setting up advanced security systems. This raises an important question: *how effective could MFA be if it were widely adopted across the sector?*

This research examines the mechanisms of MFA and analyzes local data on its effectiveness in protecting customer data in Nigeria. The study also identifies banks that currently use MFA to assess their adoption levels. Through this, it seeks to improve customer protection, rebuild trust, and enhance the resilience of digital banking services in the country.

**How To Cite:** S. Okure, I. Umana, O.O. Dominic, E. Udoiwod, F. Atakpo, B.U. Stephen. A comprehensive analysis on the implementation of Multifactor Authentication for online banking systems in Nigeria. *Computational Methods*, 3(1):8–17, 2026. https://doi.org/10.58614/cm312

## 2. Literature Review

Nigeria's banking sector is a key sector in driving economic growth as it serves a population of over 250 million with different financial needs [5]. Its rapid digitalization has improved financial inclusion, investment, and economic empowerment, but it has also increased exposure to cyber threats [6, 7]. Fraud remains a pressing issue in Nigeria, with global losses reaching 485 billion dollars in 2023 [8]. In Nigeria, fraudsters are adept at exploiting mobile channels most frequently, followed by internet banking and POS systems, with a clear example such as the 2023 compromise of a Payment Service Solution Provider (PSSP), which showed how vulnerable the payment systems are [9].

Fraud cases that were reported doubled between 2019 and 2023, with losses increasing nearly five times, indicating more costly and sophisticated attacks. Despite banks' ongoing security investments, watchdogs like FITC report persistent fraud activity, with ₦52.26 billion in losses in 2024 alone [10]. Additionally, systemic data leaks affecting millions of accounts [11] increase risks of identity theft and account takeover. Overcoming these challenges calls for using new technologies, improving digital banking experiences, unifying banking systems, and boosting customer financial literacy. [12]

Due to these, the role of multi-factor authentication (MFA) becomes critical. Some regulatory frameworks support its adoption, for example, PCI-DSS requires MFA for remote administrative access, while the EU's Second Payment Services Directive (PSD2) mandates strong customer authentication for electronic payments [13]. Similar measures appear in US directives such as HSPD-12 [14]and NIST's authentication guidelines [15, 16]. These legal and regulatory frameworks highlight MFA's growing importance in securing sensitive financial systems.

Traditional username-password methods are insufficient against modern cyber threats as they only combine two factors, such as possession (ATM card) and knowledge (PIN) [17]. For online banking, proper and strong authentication is a major concern to determine if a user is eligible to access a specific system [18]. While effective at first, criminals have exploited its weaknesses, necessitating the evolution to MFA.

Unlike 2FA, MFA requires two or more distinct authentication factors — (a) knowledge, which is based on "what you know", for example, passwords and PINs, (b) possession, which is based on "what you have", for example, tokens, OTPs, security keys, and (c) inherence. which is based on "what you are," for example, biometrics such as fingerprints or iris scans [19]. This layered defense makes it significantly harder for attackers to gain unauthorized access, since missing any factor denies entry. Thus, while all 2FA systems are forms of MFA, MFA extends beyond two factors, offering broader resilience [17].

MFA also aligns directly with the CIA Triad —confidentiality, integrity, and availability — which underpins information security policies [20]. Confidentiality is enhanced by requiring multiple verifications, Integrity is safeguarded as only verified users can alter data, and Availability is maintained by preventing unauthorized disruptions.

Finally, related studies show variations in MFA implementation. Choubey et al.'s study shows there was a lack of standardization in MFA protocol design across seven countries [21], while Kiljan et al. analyzed 80 banks, and concluded that mobile platforms were less secure than internet platforms [22]. Dmitrienko et al. checked and identified vulnerabilities in six common MFA protocols [23], while Krol et al. and Althobaiti's research was based on usability and user perceptions [18, 24]. Federico et al. broadened the scope by analyzing compliance, robustness, and complexity of MFA adoption in European banks, excluding African banks [19]. This gap underscores the relevance of studying Nigerian banks' MFA practices by adapting evaluation methods from prior works to assess security readiness and compliance in the country.

- **Geographical Gap:** Limited African/Nigerian Studies: Existing works [20–22] show that MFA studies focus on European, American, or Asian banks. Very few works have examined MFA adoption in Nigeria or Sub-Saharan Africa, despite the high fraud rates and rapidly growing digital banking usage in the region.
- **Implementation and Compliance Gap:** While regulations like PCI-DSS, PSD2 provide global frameworks, there is no equivalent evaluation of how Nigerian banks implement MFA within CBN's security mandates. Existing Nigerian works (NIBSS reports, FITC fraud analyses) highlight rising fraud, but they do not consider measuring MFA adoption levels [25] across Nigerian banks.
- **Security Mechanism Strength Gap:** Studies abroad compare MFA protocols for robustness, usability, and cryptographic soundness, but there has been no analysis that focuses on the strength of MFA mechanisms (e.g., encryption of OTPs, liveness detection for biometrics, audit practices) in Nigeria, thereby causing uncertainty about whether Nigerian banks meet best practices.
- **Empirical Data Gap:** While NIBSS and FITC publish fraud statistics [9, 10], no study directly correlates fraud incidents with the absence/presence of MFA in Nigerian banks. This lack of empirical linkage weakens policymaking and slows down effective adoption.

## 3. Methodology

### 3.1. Materials

#### Research and Data Collection

- **Google Docs:** This served as the main platform for the writing of the research paper. It was also used to organize all the findings, notes, and reviews of the literature in one accessible place.
- **Google Sheets:** This tool was used to manage and analyze the quantitative data that I collected in the course of the investigation. It was also used to create tables to show different authentication methods and to generate charts to visualize key findings and trends obtained in the course of the research.

### 3.2. Methods

This research aims to effectively investigate the extent to which MFA is used in Nigerian banks. To achieve this, the following steps were taken:

- **Creating Measurable Data Metrics:** Some of the measurable metrics include Types of MFA Factors Offered, Implementation Scope, Compliance with Security Standards, etc.
- **Data Collection:** Data Collection was carried out via the following ways:
  Analyzing user guides, FAQs, and security policy documents from primary sources.
  Direct Observation using real accounts for testing and documenting the results obtained.
  Identifying Nigerian Bank lists and ensuring that enough banks have been recorded.
- Data Analysis will be based on model components that carry the various authentication factors. This will also involve the following:
  Weighting different MFA factors based on their security implementations,
  Creating a scoring system for each security feature, scope of implementation, and
  Categorizing banks into different tiers based on the research analysis.

### 3.3. Model Components

The Components that would be employed in the course of this research are:

**Security Mechanism Strength Score (SMSS)**

The SMSS checks how robust and compliant MFA systems are with best practices, including encryption, liveness detection, and regular audits. A higher score reflects stronger resilience against evolving cyber threats. Points will be assigned to specific security features:

- Compliance with existing laws and best practices: 1point
- Robustness against known attacker models: 1 point
- Complexity, defined by the user effort required: 1 point
- End-to-end encryption for OTP Transmissions: 1 point
- Feedback Mechanisms during suspicions: 1.5 point
- Liveness detection for biometrics: 1.5 point
- Regular security audits of MFA systems: 1 point

SMSS would be calculated as the sum of points for all applicable areas with a benchmark of 6 points.

**Implementation Scope Index (ISI)**

The ISI evaluates where MFA is applied, such as during logins, transactions, and even profile updates. The broader the implementation, the more effectively a bank minimizes risks across different access points. Points would be based on where MFA is applied:

- Login (web): 1 point
- Login (mobile app): 1 point
- Sensitive transactions (e.g. transfers to unknown accounts): 1.5 points
- Beneficiary management: 1 point
- Profile Updates: 0.5 point

ISI would be calculated as the sum of points for all applicable areas with a benchmark of 4 points.

**Factor Diversity Score (FDS)**

The FDS measures the different factors of authentication a bank uses, covering knowledge-based, possession-based, and biometric-based factors. A higher score indicates stronger protection by reducing reliance on any single factor. Points will be assigned to each unique MFA factor offered as shown below:

- Something you know: PIN/Password (0.5 point)
- Something you have: SMS OTP (1 point)
- Something you have: Email OTP (1 point)
- Something you have: Authenticator App OTP (1.5 points)
- Something you have: Hardware Token (2 points)
- Something you are: Fingerprint Biometrics (2 points)
- Something you are: Facial Recognition (2 points)
- Something you are: Voice Recognition (1.5 points)
- Location-Based Authentication: 1 point

FDS would be calculated as the total sum of all selected featured factors with a benchmark of 10 points.

**Overall Weighted Score (OWS)**

This will be the sum of all the weighted sums of FDS, ISI and SMSS for each bank specified. This score would be used to determine the security category under which the bank is based. This will consist of three tiers:

- **Tier 1 (Basic):** In this tier, banks would be seen as having low OWS, limited MFA options, and are potentially weak, security-wise, with a score 0-10.
- **Tier 2 (Intermediate):** Banks in this tier would be considered to have moderate OWS, offer a few standard MFA methods, and the security level would be considered satisfactory, with a score ranging from 10.1 to 20.
- **Tier 3 (Advanced):** Banks in this category would be considered to have high OWS, diverse MFA options, and the security system would be considered highly satisfactory with a score $>20$.

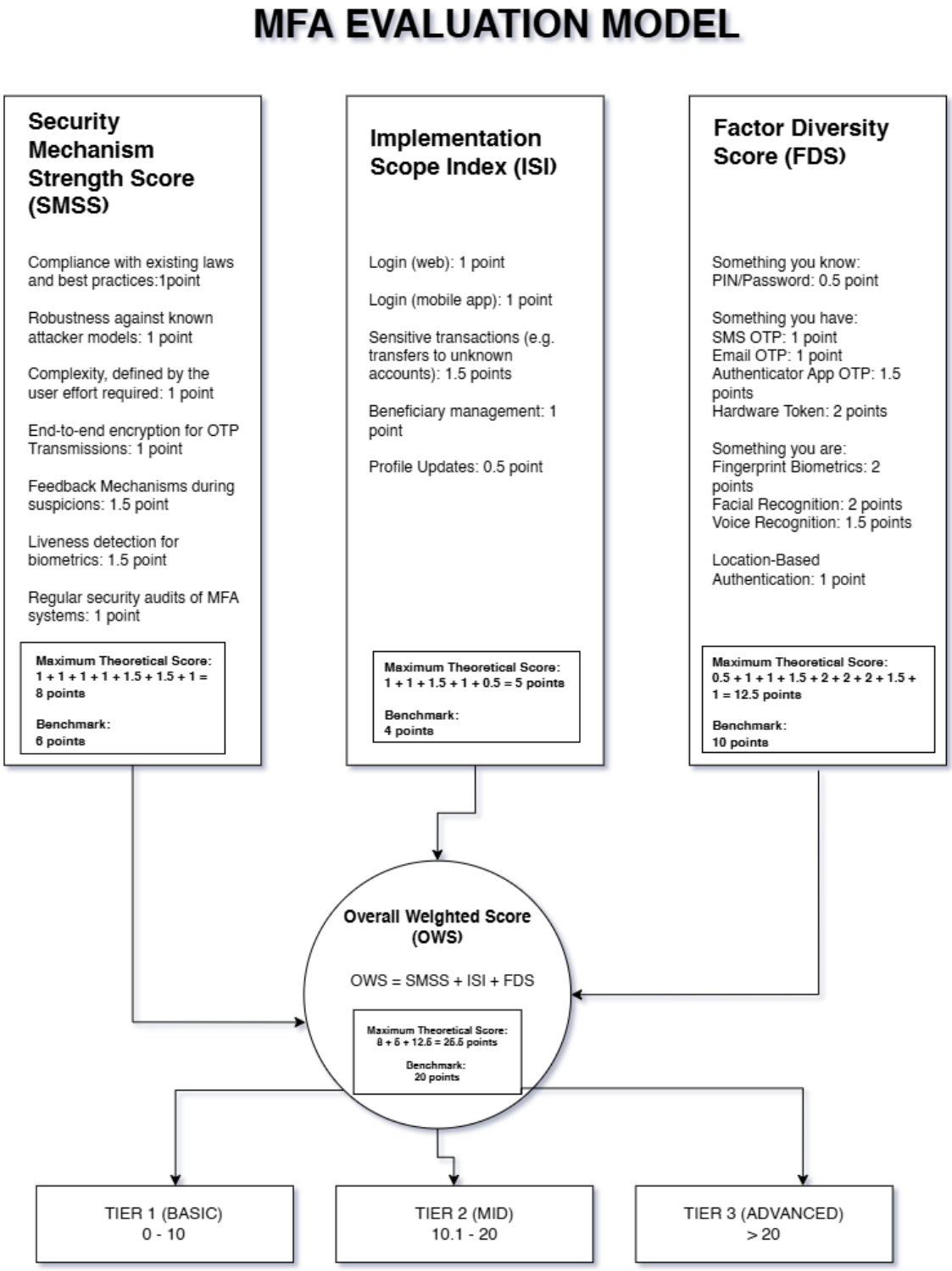


**Figure 1:** Pie Chart showing the distribution of MFA Levels across Nigerian banks

# 4. Results

This work explains the results gathered from examining how different commercial banks in Nigeria use multifactor authentication (MFA). The study looked at 19 banks in total. The findings are based on the types of authentication factors they use, how widely these methods are applied, and how strong their security systems are. In line with the objectives of this research, each bank's MFA was assessed and scored based on three key components: Factor Diversity Score (FDS), Implementation Scope Index (ISI), and Security Mechanism Strength Score (SMSS). The results are organized into four major sections:

- Security Mechanism Strength Score (SMSS) – evaluating encryption, feedback systems, biometric liveness, and audit protocols;
- Implementation Scope Index (ISI) – assessing the depth of MFA coverage across critical user interaction points;
- Factor Diversity Score (FDS) – examining the variety and uniqueness of MFA factors employed; and
- Overall Weighted Score (OWS) – representing a cumulative measure of MFA effectiveness and security assurance per bank.

The findings in this chapter not only provide a comparative view of how Nigerian banks approach user authentication but also serve as a foundation for identifying gaps and recommending future improvements. Tables and charts have been employed where necessary to enhance clarity and understanding of the data.

## 4.1. Security Mechanism Strength Score (SMSS)

The Security Mechanism Strength Score evaluated indicators such as the encryption of OTP transmissions, the presence of feedback mechanisms during suspicious activity, liveness detection for biometric systems, and the conduct of regular security audits. Each feature was scored based on verifiable implementation as published by the respective banks or industry-related sources as shown in Table 1.

**Table 1: Table showing data for Security Mechanism Strength Score (SMSS)**

| SECURITY MECHANISM STRENGTH SCORE | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *BANK* | Compliance (1pt) | Robustness (1pt) | Complexity (1pt) | Encryption (1pt) | Feedback Mecha-nism (1.5pt) | Liveness Detection (1.5pt) | Security Audits (1pt) | Total |
| Access Bank | 0.9 | 0.8 | 0.6 | 1 | 1.5 | 1.5 | 1 | 7.3 |
| Zenith Bank | 0.95 | 0.85 | 0.7 | 1 | 1.5 | 0 | 1 | 6 |
| First Bank | 0.85 | 0.75 | 0.65 | 1 | 1.5 | 0 | 1 | 5.75 |
| Sterling Bank | 0.8 | 0.7 | 0.6 | 1 | 1.5 | 0 | 1 | 5.6 |
| Union Bank | 0.7 | 0.6 | 0.5 | 1 | 1.5 | 1.5 | 1 | 6.8 |
| GTB | 0.9 | 0.8 | 0.65 | 1 | 1.5 | 1.5 | 1 | 7.35 |
| Wema Bank | 0.8 | 0.7 | 0.55 | 0 | 1.5 | 1.5 | 1 | 6.05 |
| Fidelity Bank | 0.75 | 0.65 | 0.55 | 1 | 1.5 | 1.5 | 1 | 6.95 |
| FCMB | 0.85 | 0.75 | 0.6 | 1 | 1.5 | 0 | 1 | 5.7 |
| UBA | 0.9 | 0.8 | 0.65 | 1 | 1.5 | 0 | 1 | 5.85 |
| Unity Bank | 0.65 | 0.55 | 0.5 | 1 | 1.5 | 0 | 1 | 5.2 |
| Keystone Bank | 0.7 | 0.6 | 0.55 | 1 | 1.5 | 0 | 1 | 5.35 |
| Optimus Bank | 0.8 | 0.7 | 0.55 | 1 | 1.5 | 0 | 1 | 5.55 |
| Parallex Bank | 0.8 | 0.7 | 0.55 | 1 | 1.5 | 0 | 1 | 5.55 |
| Stanbic IBTC | 0.95 | 0.9 | 0.7 | 1 | 1.5 | 1.5 | 1 | 7.55 |
| Polaris Bank | 0.75 | 0.65 | 0.55 | 1 | 1.5 | 0 | 1 | 5.45 |
| SunTrust Bank | 0.7 | 0.6 | 0.5 | 1 | 1.5 | 0 | 1 | 5.3 |
| Ecobank | 0.9 | 0.8 | 0.65 | 1 | 1.5 | 0 | 1 | 5.85 |
| Globus Bank | 0.8 | 0.7 | 0.55 | 1 | 1.5 | 0 | 1 | 5.55 |

Having examined the strength of the security mechanisms in place, it is essential to assess the scope of their application. The next section introduces the Implementation Scope Index (ISI), which explores how widely MFA is deployed across the various stages of user interaction.

### 4.2. Implementation Scope Index (ISI)

The Implementation Scope Index measures the extent to which multifactor authentication is integrated into key aspects of digital banking services. These aspects include web and mobile logins, transaction authentication, beneficiary management, and profile updates. Each bank was scored based on how many of these areas it protects using MFA.

**Table 2: Table showing data for Implementation Scope Index (ISI)**

| IMPLEMENTATION SCOPE INDEX | | | | | | |
|---|---|---|---|---|---|---|
| *BANK* | Web Login (1pt) | Mobile App Login (1pt) | Sensitive Transactions (1.5pt) | Beneficiary Management (1pt) | Profile Update (1pt) | Total |
| Access Bank | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| Zenith Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| First Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| Sterling Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| Union Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| GTB | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| Wema Bank | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| Fidelity Bank | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| FCMB | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| UBA | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| Unity Bank | 1 | 1 | 1.5 | 0 | 0 | 3.5 |
| Keystone Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| Optimus Bank | 1 | 1 | 1.5 | 0 | 0 | 3.5 |
| Parallex Bank | 1 | 1 | 1.5 | 1 | 0 | 4.5 |
| Stanbic IBTC | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| Polaris Bank | 1 | 1 | 1.5 | 0 | 0 | 3.5 |
| SunTrust Bank | 1 | 1 | 1.5 | 0 | 0 | 3.5 |
| Ecobank | 1 | 1 | 1.5 | 1 | 1 | 5.5 |
| Globus Bank | 1 | 1 | 1.5 | 0 | 0 | 3.5 |

While ISI shows 2 where multifactor authentication is implemented, it is also crucial to understand what kind of authentication factors are used.

### 4.3. Factor Diversity Score (FDS)

The Factor Diversity Score is an assessment of how many different authentication methods a bank uses. It categorizes the MFA factors into “something you know”, “something you have”, “something you are”, and contextual elements like location-based authentication. Each factor is scored based on its uniqueness and security strength, with higher scores awarded to more advanced features like biometric authentication and hardware tokens. The distribution of these factors across the selected banks is presented in Table 3.

### 4.4. Overall Weighted Score (OWS)

The Overall Weighted Score (OWS) provides a wholesome evaluation of each bank’s multifactor authentication (MFA) implementation by summing the individual scores from the three core assessment models: Security Mechanism Strength Score (SMSS), Implementation Scope Index (ISI), and Factor Diversity Score (FDS). This composite score reflects not only how secure each system is, but also how widely and diversely MFA is applied within the bank’s digital infrastructure as shown in Table 4.

**Table 3: Table showing data for Factor Diversity Score (FDS)**

| FACTOR DIVERSITY SCORE | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *BANK* | SMS OTP | Email OTP | App OTP | Hardware Token | Finger Biometrics | Facial Recognition | Voice Recognition | Location Based | Total |
| Access Bank | 1 | 1 | 1.5 | 2 | 2 | 2 | 0 | 1 | 10.5 |
| Zenith Bank | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 3 |
| First Bank | 1 | 1 | 1.5 | 2 | 0 | 0 | 0 | 0 | 5.5 |
| Sterling Bank | 1 | 1 | 1.5 | 0 | 2 | 0 | 0 | 0 | 5.5 |
| Union Bank | 1 | 1 | 1.5 | 0 | 2 | 0 | 0 | 0 | 5.5 |
| GTB | 1 | 1 | 1.5 | 2 | 2 | 2 | 0 | 1 | 10.5 |
| Wema Bank | 1 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 5 |
| Fidelity Bank | 1 | 1 | 1.5 | 2 | 2 | 0 | 1.5 | 1 | 10 |
| FCMB | 1 | 0 | 1.5 | 0 | 2 | 0 | 0 | 0 | 4.5 |
| UBA | 1 | 1 | 1.5 | 2 | 2 | 2 | 0 | 1 | 10.5 |
| Unity Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Keystone Bank | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 3 |
| Optimus Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Parallex Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Stanbic IBTC | 1 | 1 | 1.5 | 2 | 2 | 2 | 0 | 1 | 10.5 |
| Polaris Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| SunTrust Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Ecobank | 1 | 1 | 1.5 | 2 | 0 | 0 | 0 | 1 | 6.5 |
| Globus Bank | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

**Table 4: Table showing data for Overall Weighted Score(OWS)**

| OVERALL WEIGHTED SCORE | | | | |
|---|---|---|---|---|
| *BANK* | FDS | ISI | SMSS | TOTAL |
| Access Bank | 10.5 | 5.5 | 7.3 | 23.3 |
| Zenith Bank | 3 | 4.5 | 6 | 13.5 |
| First Bank | 5.5 | 4.5 | 4.9 | 14.9 |
| Sterling Bank | 5.5 | 4.5 | 4.9 | 14.9 |
| Union Bank | 5.5 | 4.5 | 6.8 | 16.8 |
| GTB | 10.5 | 5.5 | 7.35 | 23.35 |
| Wema Bank | 5 | 5.5 | 6.05 | 16.55 |
| Fidelity Bank | 10 | 5.5 | 6.95 | 22.45 |
| FCMB | 4.5 | 4.5 | 5.7 | 14.7 |
| UBA | 10.5 | 4.5 | 5.85 | 20.85 |
| Unity Bank | 1 | 3.5 | 5.2 | 9.7 |
| Keystone Bank | 3 | 4.5 | 5.35 | 12.85 |
| Optimus Bank | 1 | 3.5 | 5.55 | 10.05 |
| Parallex Bank | 1 | 4.5 | 5.55 | 11.05 |
| Stanbic IBTC | 10.5 | 5.5 | 7.55 | 23.55 |
| Polaris Bank | 1 | 3.5 | 5.45 | 9.95 |
| SunTrust Bank | 1 | 3.5 | 5.3 | 9.8 |
| Ecobank | 6.5 | 5.5 | 5.85 | 17.85 |
| Globus Bank | 1 | 3.5 | 5.55 | 10.05 |

This section effectively concludes the data analysis chapter by ranking banks based on both the technical robustness and functional spread of their authentication strategies.

## 5. Discussion

Each bank's total score was benchmarked against a 20-point scale (6 for SMSS, 4 for ISI, and 10 for FDS). The overall weighted scores of the 19 Nigerian banks surveyed were classified into three tiers based on their level of multifactor authentication (MFA) implementation and readiness. Scores ranging from 0.0–10.0 were classified as Low Tier, scores between 10.1–20.0 as Mid Tier, while scores above 20.0 were categorized as Top Tier.

From the analysis, five banks (26.3 percent) fell within the Top Tier. These include Stanbic IBTC (23.55) [26, 27], Guaranty Trust Bank (23.35) [28, 29], Access Bank (23.3), Fidelity Bank (22.45) [30], and United Bank for Africa (20.85) [31]. These institutions demonstrated strong security postures with consistent adoption of multiple authentication layers, integration of fraud detection systems, and robust underlying security mechanisms.

A larger proportion of the banks, eight institutions (42.1 percent), were placed in the Mid Tier. This category includes Zenith Bank (13.5) [32, 33], First Bank of Nigeria (14.9), Sterling Bank (14.9), First City Monument Bank (14.7), Union Bank (16.8), Wema Bank (16.55) [34–36], Ecobank (17.85), and Keystone Bank (12.85). These banks displayed moderate MFA readiness. They appear to have adopted baseline authentication strategies but show varying gaps in consistency, usability, or integration of fraud and data security enhancements.

Finally, six banks (31.6 percent) were classified in the Low Tier, namely Polaris Bank (9.95), SunTrust Bank (9.8), Unity Bank (9.7), Optimus Bank (10.05), Parallex Bank (11.05), and Globus Bank (10.05). These banks either had very minimal MFA deployment or weak integration of security protocols, highlighting significant vulnerabilities in their online banking authentication strategies.

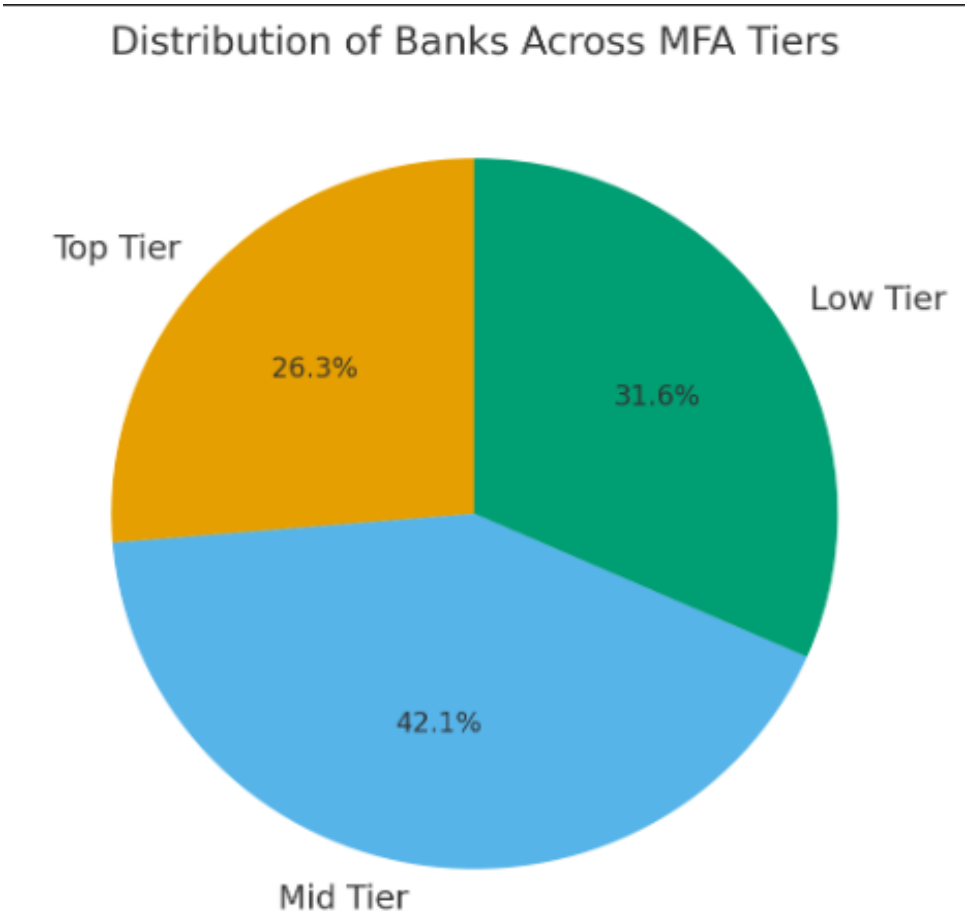


**Figure 2:** Pie Chart showing the distribution of MFA Levels across Nigerian banks

## 6. Conclusion

This study looked at how banks in Nigeria use multifactor authentication (MFA) to protect customers from fraud and data breaches. To compare the banks fairly, four measures were used: the Security Mechanism Strength Score (SMSS), Implementation Scope Index (ISI), Factor Diversity Score (FDS), and the Overall Weighted Score (OWS).

The results showed a clear gap between the bigger and smaller banks. Major banks like Access, Zenith, and GTBank use stronger methods such as biometrics, hardware tokens, and encrypted OTPs. In contrast, many mid-sized and smaller banks still depend mostly on simple SMS or email codes for authentication.

The study also found that banks use MFA most effectively in their main banking services, but it becomes less reliable in areas like customer support platforms and third-party apps. A big reason for this gap is resources—larger banks can afford better technology and frequent security audits, while smaller or newer banks face cost and infrastructure challenges.

Regulation and user experience also played a role. Some banks were proactive and adopted stronger MFA early, while others only upgraded when necessary or chose simpler methods so customers wouldn't find the process too stressful or confusing.

Overall, the study shows that MFA adoption across Nigerian banks is uneven. About a quarter of the banks are ahead of the curve, nearly half are somewhere in the middle, and roughly a third are still far behind. Even though there's been progress, these gaps create openings that attackers can take advantage of.

The study emphasizes that MFA isn't just a technical upgrade — it's a strategic move that helps protect customers, strengthen trust, and keep the financial system stable. To close the security gap, smaller banks will need clearer guidelines and more investment so the entire sector can move closer to international standards.

### Article Information

**Disclaimer (Artificial Intelligence):** The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

**Competing Interests:** Authors have declared that no competing interests exist.

## References

[1] S. C. Nwokolo, E. L. Meyer, and C. C. Ahia. Credible pathways to catching up with climate goals in nigeria. *Climate*, 11(9):196, 2023. doi: 10.3390/cli11090196.

[2] J. N. Nwakpa. Evaluation of nigerian government's new cashless policy: Insights from select national dailies. *British Journal of Marketing Studies*, 11(3):1–16, 2023. doi: 10.37745/bjms.2013/vol11n3116.

[3] O. J. Ayagbekun, B. O. Felix, and B. A. Saka. Analysis of security mechanisms in nigeria e-banking platform. *International Journal of Electrical and Computer Engineering*, 4(6):837–847, 2014. doi: 10.11591/ijece.v4i6.6857.

[4] Central Bank of Nigeria. Payment system vision 2020, 2020. URL https://www.cbn.gov.ng/PaymentsSystem/PSV2020.html. Accessed online.

[5] A. M. Alabi, F. N. Oguntoyinbo, K. M. Abioye, A. A. John-Ladega, A. N. Obiki-Osafiel, and C. Daraojimba. Risk management in africa's financial landscape: A review. *International Journal of Advanced Economics*, 5(8):19, 2023. doi: 10.51594/ijae.v5i8.573.

[6] S. O. Dawodu, A. Omotosho, O. J. Akindote, A. O. Adegbite, and S. K. Ewuga. Cybersecurity risk assessment in banking: Methodologies and best practices. *Computer Science and IT Research Journal*, 4(3):220–243, 2023. doi: 10.51594/csitrj.v4i3.659.

[7] J. Garba and E. N. M. Ibrahim. Design of a conceptual framework for cybersecurity culture amongst online banking users in nigeria. *Nigerian Journal of Technology*, 42(3):399–405, 2023. doi: 10.4314/njt.v42i3.13.

[8] allAfrica. Nigeria: As global financial fraud hits $485bn, access holdings shows africa how to fight back, May 2025. URL https://allafrica.com/stories/202505190203.html. Accessed Aug 16, 2025.

[9] NIBSS. Annual fraud landscape, Dec 2023. URL https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf. Accessed Aug 16, 2025.

[10] FITC. Reports on fraud and forgeries in nigerian banks, 2024. URL https://fitc-ng.com/wp-content/uploads/2024/09/Fraud-and-Forgery-2024-2nd-Quarter.pdf. Accessed Aug 2025.

[11] Punch Nigeria. Nigeria's data privacy breaches surge amid regulatory pressure, Feb 2025. URL https://punchng.com/nigerias-data-privacy-breaches-surge-amid-regulatory-pressure/.

[12] O Reis, J.S Ohila, F Osasona, and O.C Obi. Cybersecurity dynamics in nigerian banking: trends and strategies review. *Comput Sci IT Res J*, 5(2):336–364, 2024. doi: 10.51594/csitrj.v5i2.761.

[13] European Union. Supplementing directive (eu) 2015/2366 concerning strong customer authentication, Sep 2023. URL https://eur-lex.europa.eu/eli/reg_del/2018/389/oj.

[14] Department of Homeland Security. About hspd-12: Homeland security presidential directive 12, Sep 2012. URL https://web.archive.org/web/20120916062033/http:/hspd12.usda.gov/about.html.

[15] Bruce Schneier. Nist is no longer recommending two-factor authentication using sms, Aug 2016. URL https://www.schneier.com/blog/archives/2016/08/.

[16] NIST. Digital identity guidelines. Technical Report Special Publication 800-63-3, National Institute of Standards and Technology, Jun 2017.

[17] Fraud.com. Multifactor authentication: how does it work?, 2024. URL https://www.fraud.com/post/multi-factor-authentication.

[18] M.M Althobaiti. *Assessing usable security of multifactor authentication*. PhD thesis, University of East Anglia, School of Computing Sciences, Norwich, UK, Jun 2016. URL https://ueaeprints.uea.ac.uk/id/eprint/61540/.

[19] F Sinigaglia, R Carbone, G Costa, and N Zannone. A survey on multifactor authentication for online banking in the wild. *Journal of Computer Security*, 95:101745, 2020. doi: 10.1016/j.cose.2020.101745.

[20] W Chai. What is the cia triad (confidentiality, integrity and availability)?, Dec 2023. URL https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

[21] J Choubey and B Choubey. Secure user authentication in internet banking: a qualitative survey. *International Journal of Innovation, Management and Technology*, 4(2):198–203, 2013. doi: 10.7763/IJIMT.2013.V4.391.

[22] S Kiljan, K Simoens, D De Cock, M Van Eekelen, and H Vranken. A survey of authentication and communications security in online banking. *ACM Computing Surveys*, 49(4):61, 2017. doi: 10.1145/3002170.

[23] A Dmitrienko, C Liebchen, C Rossow, and A.R Sadeghi. Security analysis of mobile two-factor authentication schemes. *Intel Technology Journal*, 18(4), 2014. URL https://www.christian-rossow.de/publications/mobile2FA-intel2014.pdf.

[24] K Krol, E Philippou, E De Cristofaro, and M.A Sasse. They brought in the horrible key ring thing!: analysing the usability of two-factor authentication in uk online banking. *arXiv preprint arXiv:1501.04434*, 2015. URL https://arxiv.org/abs/1501.04434.

[25] B.B Oguejiofor, A Omotosho, K.M Abioye, A.M Alabi, F.N Oguntoyinbo, and A.I Daraojimba. A review on data-driven regulatory compliance in nigeria. *International Journal of Applied Research in Social Sciences*, 5(8):231–234, 2023. doi: 10.51594/ijarss.v5i8.571.

[26] Stanbic IBTC Bank. Security centre, 2025. URL https://www.stanbicibtccapital.com/nigeriacapital/Investment-Banking/about-us/Legal/Security-Centre.

[27] Wikipedia. Stanbic ibtc holdings, Jun 2025. URL https://en.wikipedia.org/wiki/Stanbic_IBTC_Holdings. Wikipedia: The Free Encyclopedia.

[28] Guaranty Trust Bank. Biometric verification data consent notice, 2025. URL https://www.gtbank.com/biometric-verification-data-consent.

[29] Guaranty Trust Bank. Privacy policy, 2025. URL https://www.gtbank.com/privacy-policy.

[30] Wikipedia. Fidelity bank nigeria, Jun 2025. URL https://en.wikipedia.org/wiki/Fidelity_Bank_Nigeria. Wikipedia: The Free Encyclopedia.

[31] Alex Corbado. Banking security in nigeria with biometrics and passkeys, Feb 2025. URL https://www.corbado.com/blog/nigeria-banking-biometrics-passkeys. Corbado: Passkey Adoption Platform.

[32] Zenith Bank. About the zenith etoken app, 2024. URL https://www.zenithbank.com/personal-banking/etoken-app/.

[33] Zenith Bank. Customer service faqs, 2025. URL https://www.zenithbank.com/customer-service/faqs/.

[34] A Ajibade. Wema bank enhances security with facial recognition tech after a 685 million fraud loss, Jun 2024. URL https://techpoint.africa/news/wema-bank-adopts-facial-recognition/.

[35] Wema Bank. How to onboard on the alat xplore app: a comprehensive guide, Oct 2024. URL https://wemabank.com/blog/how-to-onboard-on-the-alat-xplore-app-a-comprehensive-guide-1.

[36] Wema Bank. Data protection (ndpa) policy statement, 2025. URL https://wemabank.com/data-protection-policy.