© IIJP 2026 | Volume 2, Issue 2, pp. 1900-1914 | ISSN: 2636-4484

ELECTRONIC-FRAUD IN ONLINE BANKING PAYMENTS AND AUTHENTICATING DETECTION TECHNIQUES IN BANKING INDUSTRY: A CASE STUDY OF ZENITH BANK PLC. IN CROSS RIVER STATE, NIGERIA

Nwosu Stanley Chigaemezu[1], Dr. Ayuk, Awunghe Achu[2], Dr. Ezikeudu, Chukwudi Charles[3], Dr. Egidi, Stephen Achuen[4] & Joseph Anthony Odama[5]

[1,2,3&5]Department of Criminology and Security Studies, University of Calabar, Calabar, Cross River State, Nigeria

[4]Department of Sociology and Social Work, Arthur Jarvis University, Akpabuyo Cross River State, Nigeria.

Corresponding E-mail: egidistephen36@gmail.com

ARTICLE INFO
Article No.: 0412
Accepted Date: 10/06/2026
Published Date: 30/06/2026
Type: Research

ABSTRACT

This study investigated electronic fraud in online banking payments and authentication detection techniques in the banking industry, using Zenith Bank Plc. in Cross River State, Nigeria, as a case study. Specifically, the study assessed how biometric verification mitigates electronic fraud in online banking and examined the effectiveness of automatic lockout mechanisms in reducing online banking fraud. The study was anchored on the Routine Activity Theory. A survey research design was adopted for the study. The target population comprised 1,268 respondents, consisting of 148 staff of Zenith Bank Plc. and 1,120 active online banking customers across selected branches in Calabar, Ikom, and Ogoja, Cross River State. Using Taro Yamane's formula. A sample size of 200 respondents was selected through purposive, stratified random, and simple random sampling techniques. Data were collected using a structured questionnaire. The reliability of the instrument was confirmed using Cronbach's Alpha coefficient of 0.85. Data were analyzed using the Chi-square at the 0.05 level of significance. The first hypothesis revealed a statistically significant relationship between biometric verification and the reduction of electronic fraud ($\chi^2 = 28.13$). The second hypothesis established a significant positive relationship between biometric verification and effective fraud prevention ($\chi^2 = 48.49$). The study concluded that digital banking has enhanced the efficiency and accessibility of financial services, it has simultaneously increased exposure to sophisticated electronic fraud. The study recommends that financial institutions should deploy multi-modal biometric authentication systems alongside real-time fraud monitoring solutions to enhance the detection and prevention of electronic fraud in online banking.

Keywords: Fraud, banking, techniques, authenticating and biometric

Introduction

Online banking payments have significantly improved financial accessibility, convenience, speed, and operational efficiency. However, the increasing dependence on digital financial services has also exposed banking institutions and customers to various forms of electronic fraud (e-fraud), including phishing, identity theft, malware attacks, account takeovers, payment card fraud, and unauthorized fund transfers (Kumar & Gupta, 2021). Globally, electronic fraud has emerged as one of the most significant threats to the banking sector. The expansion of e-commerce, internet banking, mobile banking, and real-time payment systems has increased opportunities for cybercriminals to exploit vulnerabilities in banking infrastructures. According to the International Monetary Fund (IMF, 2024), cyberattacks on financial institutions have increased substantially over the past decade, causing billions of dollars in annual losses and undermining customer confidence in digital financial services (International Monetary Fund [IMF], 2024). Fraudsters increasingly employ sophisticated techniques such as social engineering, ransomware, artificial intelligence-assisted attacks, and credential theft to bypass conventional security mechanisms. Banks are adopting advanced fraud detection technologies, including machine learning algorithms, artificial intelligence, biometric authentication, behavioral analytics, and real-time transaction monitoring systems to identify suspicious activities and mitigate fraud risks (Ngai, Hu, Wong, Chen & Sun, 2021).

Across Africa, the growth of digital banking and financial technology (FinTech) services has accelerated financial inclusion and economic development. Mobile money platforms, internet banking services, and digital payment systems have become increasingly popular, particularly in countries such as Kenya, South Africa, Ghana, and Nigeria. Despite these benefits, African financial institutions face significant cybersecurity challenges due to inadequate technological infrastructure, weak regulatory enforcement, limited cybersecurity awareness, and increasing cybercrime activities. Electronic fraud in Africa commonly manifests through mobile money fraud, SIM swap attacks, phishing schemes, identity fraud, and unauthorized electronic fund transfers (Interpol, 2023).

As a result, financial institutions and regulatory agencies across the continent have intensified efforts to strengthen cybersecurity frameworks, implement stronger authentication mechanisms, and promote digital literacy among customers. In Nigeria for instance, the banking industry has witnessed significant digital transformation through the adoption of internet banking, mobile banking applications, electronic payment channels, and cashless policy initiatives introduced by the Central Bank of Nigeria (CBN). These developments have improved financial inclusion and facilitated seamless transactions across the country. The increasing use of electronic banking channels has also led to a rise in electronic fraud incidents. Common forms of electronic fraud in Nigeria include phishing attacks, ATM fraud, identity theft, cyberstalking, account hijacking, unauthorized transfers, and social engineering scams (Central Bank of Nigeria, 2023). Reports from the Nigeria Inter-Bank Settlement System (NIBSS) indicate that financial losses resulting from electronic fraud continue to pose substantial challenges to banks and customers despite ongoing security improvements. Regulatory bodies such as the Central Bank of Nigeria and the Nigeria Inter-Bank Settlement System have introduced cybersecurity guidelines and risk management frameworks aimed at strengthening the resilience of the banking sector against electronic fraud.

Statement of the Problem

The rapid expansion of electronic banking systems has significantly transformed financial service delivery in Nigeria, particularly through online payment platforms that offer convenience, speed, and accessibility. However, this digital transformation has also introduced sophisticated forms of electronic fraud that threaten the integrity, confidentiality, and availability of banking transactions. Electronic fraud in online banking payments has

become a persistent challenge, characterized by phishing attacks, identity theft, unauthorized fund transfers, malware intrusion, and social engineering schemes targeting both customers and financial institutions (Adeyemi & Aluko, 2020). Despite the deployment of various security infrastructures by commercial banks, including multi-factor authentication, encryption protocols, and real-time fraud monitoring systems, fraudulent activities continue to escalate.

This suggests that existing authentication and fraud detection techniques may be insufficient, outdated, or inadequately implemented within some banking environments. In Nigeria, where digital financial inclusion is expanding rapidly, the vulnerability of online banking systems to cybercriminal activities poses a serious concern for both customer trust and institutional stability (Nwankwo & Eze, 2021). Zenith Bank Plc., as one of the leading financial institutions in Nigeria, has adopted several technological innovations to enhance online banking services. The persistence of these issues indicates a possible gap between technological deployment and actual fraud mitigation outcomes. While advanced authentication techniques such as biometrics, token-based systems, and behavioral analytics are increasingly being adopted globally, their effectiveness within the Nigerian banking context remains under-researched. There is also limited empirical evidence assessing how these tools perform in real-world banking operations, especially in relation to user behavior, infrastructural constraints, and cybercrime adaptability (Akinyemi & Oladipo, 2019). It is against this backdrop that this study seeks to investigate the nature and patterns of electronic fraud in online banking payments, and critically examine the effectiveness of authentication and fraud detection techniques employed by Zenith Bank Plc. in Cross River State, Nigeria.

Objectives of the study

1. To assess how biometric verification can mitigate E-fraud in online banking
2. To assess the effectiveness of automatic lockout mechanisms in mitigating online banking fraud

Research hypotheses

1. There is no significant relationship between biometric verification and E-fraud in online banking
2. There is no significant relationship between automatic lockout mechanisms and online banking fraud

Literature review

Electronic -fraud in online banking payments

Developed economies have reported increasing incidents of phishing attacks, ransomware targeting financial institutions, and credential theft through social engineering techniques. According to the Federal Bureau of Investigation's Internet Crime Report, phishing and spoofing remain among the most commonly reported cyber-enabled financial crimes, with losses amounting to billions of dollars annually (FBI IC3, 2024). In Europe, the European Central Bank (ECB, 2023) reports that card-not-present fraud and unauthorized electronic transfers constitute a significant proportion of digital payment fraud, especially as online commerce and contactless payments expand. Button, Lewis & Tapley (2024) argue that fraud in online banking is not only a technological issue but also a socio-technical problem, where user awareness, institutional trust, and regulatory enforcement interact. Emerging studies show that artificial intelligence is increasingly being used by fraudsters to automate attacks such as credential stuffing and synthetic identity creation, thereby increasing the scale and sophistication of fraud operations (OECD, 2022).

In Africa, the expansion of digital financial services, particularly mobile money and mobile banking, has significantly increased financial inclusion. However, this growth has been accompanied by rising cases of electronic fraud. The African Union (2021) notes that cybercrime, including online financial fraud, is one of the fastest-growing forms of crime on

the continent, largely due to gaps in cybersecurity infrastructure, regulatory enforcement, and digital literacy. In Nigeria, electronic fraud in online banking payments has become a major concern for financial institutions, regulators, and customers (Egidi, Obona, Ikpeme, & Aganyi, 2024). The rapid adoption of internet banking, USSD banking, and mobile applications has exposed users to various forms of cyber fraud, including phishing scams, unauthorized transfers, and SIM swap fraud linked to mobile banking authentication systems. Reports from the Central Bank of Nigeria (CBN, 2023) and the Economic and Financial Crimes Commission (EFCC, 2023) indicate that fraud cases in digital payment systems have increased steadily, with significant financial losses recorded across commercial banks and fintech platforms.

Fraudsters often exploit weak authentication systems, compromised customer data, and inadequate cybersecurity awareness among users. For instance, Adeyemi (2020) found that many bank customers lack sufficient knowledge of secure online banking practices, making them vulnerable to phishing and impersonation attacks. Similarly, Okafor and Dike (2021) emphasize that insider threats and system vulnerabilities within banking institutions also contribute to fraud incidents. Despite the growing body of literature on electronic fraud in online banking payments, several gaps remain evident. First, much of the global literature focuses on developed economies, where cybersecurity infrastructure and regulatory systems differ significantly from those in developing countries. This limits the contextual applicability of such findings to Nigeria and other African economies. Second, while numerous studies in Nigeria have examined fraud in banking systems, there is still limited integrated research that simultaneously considers technological vulnerabilities, human behavioral factors, and institutional weaknesses within a unified analytical framework. Existing studies often treat these dimensions in isolation rather than as interconnected drivers of electronic fraud.

Biometric verification and mitigating E-fraud in online banking

Biometric verification has increasingly become a central pillar in strengthening authentication mechanisms within online banking systems. Unlike traditional knowledge-based (passwords) or possession-based (tokens) methods, biometrics rely on inherent physiological or behavioral traits, making them significantly more resistant to theft, duplication, or unauthorized sharing. Biometric identifiers such as fingerprints, facial features, iris patterns, and voice characteristics are inherently unique to individuals. This uniqueness reduces the probability of impersonation and unauthorized access, as attackers cannot easily replicate or transfer these traits. In online banking, this strengthens authentication during login and transaction approval processes, significantly reducing credential-stuffing and brute-force attacks (Omotubora & Basu, 2018). A major source of e-fraud in banking systems is weak or reused passwords, which are often compromised through phishing, malware, or data breaches. Biometric authentication reduces reliance on passwords, thereby eliminating risks associated with password reuse, theft, and social engineering attacks.

According to the National Institute of Standards and Technology, multi-factor authentication incorporating biometrics enhances resistance to credential compromise (NIST, 2017). According to Abomhara & Koien, (2015), modern banking systems integrate biometrics into transaction-level authentication, such as fingerprint or facial verification before approving fund transfers. Unlike static authentication methods, behavioral biometrics enable continuous verification throughout a user session. This means that deviations from normal behavioral patterns such as unusual mouse movements, typing speed, or navigation habits can trigger fraud alerts or session termination. This continuous authentication reduces the window of opportunity for fraudsters who manage to gain initial access (Patel, Connell & Bolle, 2016). Identity theft often involves the use of stolen personal information to impersonate legitimate users. Biometric verification significantly limits this risk because stolen data alone is insufficient to replicate biometric traits. Even if attackers obtain sensitive

personal details, they cannot bypass fingerprint or facial recognition systems without the physical presence of the account holder. Biometrics are commonly integrated as a second or third authentication factor in MFA systems. This layered security approach ensures that even if one factor is compromised (e.g., password leakage), unauthorized access is still prevented. NIST emphasizes that combining biometrics with other authentication factors significantly improves resilience against e-fraud (NIST, 2017). Biometric verification strengthens online banking security by providing a highly personalized, difficult-to-replicate authentication mechanism. Its integration into banking systems reduces reliance on vulnerable password-based systems, enhances transaction security, and improves fraud detection capabilities. Biometric authentication is grounded in the principle that certain human traits are sufficiently distinctive and stable to reliably distinguish one individual from another. These traits include fingerprints, facial structure, iris patterns, voice characteristics, and even behavioral patterns such as gait or typing rhythm. Unlike traditional knowledge-based or possession-based authentication factors, biometrics are inherently tied to the individual, making them difficult to replicate, share, or lose (Maltoni,Maio, Jain & Prabhakar, 2019). This intrinsic linkage between identity and biological characteristics forms the foundational principle upon which biometric systems operate.

According to Jain, Ross, & Nandakumar, (2011), the operational framework of biometric authentication systems typically involves four key processes: acquisition, feature extraction, template creation, and matching. During acquisition, a biometric sensor captures raw data from the user. This data is then processed to extract distinguishing features, which are converted into a digital representation known as a biometric template. During authentication, the system compares the stored template with the newly acquired sample to determine identity validity. The accuracy and efficiency of this process depend on the quality of feature extraction algorithms and matching techniques employed (Jain, Nandakumar & Ross, 2016). A fundamental principle underpinning biometric authentication is universality, which assumes that every individual possesses a measurable biometric trait. Another key principle is uniqueness, which ensures that biometric characteristics vary sufficiently across individuals to enable differentiation. Permanence is also essential, implying that biometric traits remain relatively stable over time, while collectability ensures that these traits can be measured quantitatively using available technology (Omotubora & Basu, 2018).

These principles collectively determine the feasibility and reliability of biometric systems in practical applications. Biometric authentication is not without challenges for instance, issues such as sensor noise, environmental interference, spoofing attacks, and concerns about privacy and data protection continue to shape its development and deployment. Unlike passwords, biometric data cannot be easily changed once compromised, raising significant security and ethical considerations. In contemporary digital ecosystems, biometric authentication plays a central role in enhancing security while improving user convenience. Its adoption spans mobile devices, border control systems, banking platforms, and national identification programs. As technological advancements such as artificial intelligence and machine learning continue to improve pattern recognition and liveness detection, biometric systems are expected to become even more accurate and resilient. Unlike passwords or identity cards, biometric traits are inherently permanent and cannot be easily replaced once compromised. This permanence introduces a significant security concern: if biometric data is stolen or replicated, the affected individual may face irreversible identity exposure

As biometric technologies become more integrated into critical infrastructure and digital ecosystems, the attack surface targeting these systems has expanded, raising concerns about their robustness and resilience. A fundamental issue in biometric authentication systems lies in their dependence on pattern recognition rather than exact matching. This

characteristic makes them vulnerable to spoofing and presentation attacks, where adversaries attempt to deceive sensors using fake biometric artifacts such as printed fingerprints, high-resolution facial images, or recorded voice samples (Marcel, Nixon, & Li, 2014). Advances in artificial intelligence and deepfake technologies have further amplified these threats by enabling the generation of highly realistic synthetic biometric data that can bypass traditional verification mechanisms. Another critical vulnerability arises from the storage and transmission of biometric templates. In most systems, raw biometric data is transformed into digital templates for storage and matching. If these templates are poorly protected, they can be intercepted or compromised during transmission or breached from databases. Unlike passwords, biometric templates cannot be simply reissued once exposed, making encryption, secure template protection, and cancelable biometrics essential components of system design (Uludag, Pankanti, Prabhakar& Jain, 2004).

Biometric systems are also susceptible to issues such as false acceptance and false rejection errors, which can be exploited by attackers or result in usability challenges. Environmental factors, sensor quality, and algorithmic bias may also affect system accuracy and fairness, potentially leading to unequal performance across different demographic groups (Jain, Nandakumar, K., & Ross, 2016). These limitations highlight the trade-off between usability, security, and inclusiveness in biometric authentication design. In addition, the increasing integration of biometric systems with cloud computing and mobile platforms has introduced new cybersecurity risks. Cloud-based biometric databases, while scalable and efficient, are attractive targets for large-scale cyberattacks. Similarly, mobile biometric systems, such as facial recognition on smartphones, may be compromised through device-level malware or sensor manipulation (Bhargava, Lu, & Zhang, 2017). while biometric systems represent a significant advancement in authentication technology, their vulnerabilities present serious challenges that must be addressed to ensure secure and reliable deployment.

Theoretical framework

Routine Activity Theory

The theory was formulated by Marcus Felson and Lawrence E. Cohen in 1979 as a macro-level explanation of crime occurrence, emphasizing the situational conditions under which criminal acts are likely to take place rather than focusing solely on offender motivation. The theory assumes that crime is not random but is facilitated by the routine activities of individuals and organizations that expose them to risk, particularly in environments where guardianship is weak. Routine Activity Theory is highly relevant in explaining electronic fraud in online banking payment systems because digital financial transactions inherently increase exposure to risk factors outlined in the theory. The widespread use of online banking platforms, mobile payment systems, and electronic transfers increases the availability of "suitable targets" due to the constant generation and transmission of sensitive financial data.

Motivated offenders in cyberspace exploit vulnerabilities such as phishing attacks, credential theft, malware injection, and man-in-the-browser attacks. These crimes are facilitated when authentication mechanisms are weak or poorly implemented. For instance, reliance on single-factor authentication increases exposure, while stronger systems such as multi-factor authentication, biometric verification, and real-time fraud analytics act as "capable guardianship." Fraud detection techniques in the banking industry such as behavioral analytics, anomaly detection systems, and machine learning-based monitoring can be interpreted as modern extensions of guardianship within RAT. When these systems are robust, they reduce the convergence of the three elements required for fraud, thereby lowering the likelihood of successful attacks. Despite its usefulness, Routine Activity Theory has several limitations when applied to electronic banking fraud. For instance, the theory focuses heavily on opportunity structures and neglects deeper psychological, economic, or

social motivations behind cybercriminal behavior. And also, electronic fraud often involves sophisticated networks, transnational actors, and automated tools, which extend beyond the simple offender–target–guardian model. However, the theoy has been adopted as a framework to the study.

Methodology

This study adopted the survey research design. The survey design was considered appropriate because it enables the researcher to obtain first-hand information from respondents regarding electronic fraud in online banking payments and the authentication detection techniques employed by Zenith Bank Plc. The study was conducted in Cross River State, Nigeria, focusing on selected branches of Zenith Bank Plc located in Calabar, Ikom, and Ogoja. These branches were selected because they provide extensive electronic banking services, including internet banking, mobile banking, Automated Teller Machine (ATM) services, Point-of-Sale (POS) services, and electronic fund transfer platforms, thereby exposing both staff and customers to issues relating to electronic fraud and fraud detection mechanisms. The target population comprised all staff of Zenith Bank Plc in Cross River State and selected active electronic banking customers.

In this study, the selected Zenith Bank Staff were 148, while active Online Banking Customers were 1,120 making a total population of 1,268. The staff population of 148 corresponds to the five Zenith Bank branches operating within Cross River State, while the customer population was obtained from the customer service units of the selected branches based on active electronic banking users. The total study population was therefore 1,268 respondents.

The sample size for the study was determined using Taro Yamane's (1967) formula.

$$n = \frac{N}{I + N(e)^2}$$

Where

n =Sample size

N =total population

e= Error limits

The researcher adopted 200 respondents because of time constraints, accessibility of respondents, and financial considerations. A sample of 200 remains adequate for survey research and provides sufficient statistical power for the planned analyses.

In sampling technique, the researcher purposively selected Zenith Bank Plc. The study also adopted a stratified random sampling technique were the study population was divided into two strata: Zenith Bank Staff and Active Online Banking Customers. Thereafter, respondents were selected using simple random sampling within each stratum.

Table 1: Sample Breakdown by Stratum

S/n	Stratum	Population	Percentage	Sample
1	Staff	148	11.7%	24
2	Customers	1,120	88.3%	176
Total		1,268	100%	200

The major instrument for data collection was a structured questionnaire developed by the researcher after reviewing relevant literature on electronic fraud, online banking payment systems, cyber security, and authentication detection technologies.

The questionnaire employed a five-point Likert Scale:

i. Strongly Agree (5)
ii. Agree (4)
iii. Undecided (3)
iv. Disagree (2)
v. Strongly Disagree (1)

The validity of the instrument was established through face validity and content validity. The draft questionnaire was submitted to three experts in Banking and Finance, Measurement and Evaluation, and Information Systems Security for critical assessment. Their observations regarding clarity, relevance, adequacy, language, and alignment with the research objectives were incorporated before the final administration of the instrument. The reliability of the questionnaire was determined through a pilot study involving 20 respondents drawn from a Zenith Bank branch in Akwa Ibom State, which was outside the study area. The responses obtained were analyzed using Cronbach's Alpha. The overall Cronbach's Alpha coefficient of 0.85 exceeded the recommended benchmark of 0.70, indicating that the instrument possessed high internal consistency and was suitable for the study. The researcher personally administered the questionnaires with the assistance of two trained research assistants. Permission was obtained from the management of the selected Zenith Bank branches before administering the questionnaires. Respondents were allowed adequate time to complete the questionnaires, after which they were collected immediately to minimize non-response and incomplete responses.

The hypotheses were tested at the 0.05 level of significance using chi-square as a statistical tool. Ethical approval and permission were obtained from the appropriate academic authority and the management of the selected Zenith Bank branches before data collection commenced. Participation in the study was entirely voluntary, and informed consent was obtained from all respondents after explaining the purpose of the research.

Result of findings

Table 2: Analysis of biometric verification and E-fraud in online banking

Chi-Square Analysis of the Relationship Between Biometric Verification and E-Fraud in Online Banking

Table 3: Observed Frequency Table

Biometric Verification	**E-Fraud Experienced**	**No E-Fraud Experienced**	**Row Total**
Effective	30	90	120
Not Effective	50	30	80
Column Total	80	120	200

Expected Frequency Table

$$EF=\frac{(\text{Row Total}) \times (\text{Column Total})}{\text{Grand total}}$$

Cell (Effective × E-Fraud) $E= \frac{120\times80}{200}=48$

Cell (Effective × No E-Fraud) $E= \frac{120\times120}{200}=72$

Cell (Not Effective × E-Fraud) $E= \frac{80\times80}{200}=32$

Cell (Not Effective × No E-Fraud) $E = \frac{80 \times 120}{200} = 48$

Table 4: Expected Frequency Table

Biometric Verification	**E-Fraud Experienced**	**No E-Fraud Experienced**	**Row Total**
Effective	48	72	120
Not Effective	32	48	80
Column Total	**80**	**120**	**200**

Table 4: Chi-Square Statistic Computation

The Chi-Square statistic is computed using:

$$\chi^2 = \frac{(O-E)^2}{E}$$

Cell	**O**	**E**	**O−E**	**$(O-E)^2$**	**$(O-E)^2/E$**
Effective & E-Fraud	30	48	-18	324	6.75
Effective & No E-Fraud	90	72	18	324	4.50
Not Effective & E-Fraud	50	32	18	324	10.13
Not Effective & No E-Fraud	30	48	-18	324	6.75
Total χ^2					**28.13**

Therefore,

$\chi^2 = 6.75 + 4.50 + 10.13 + 6.75 = 28.13$

$df = (r-1)(c-1)$

$df = (2-1)(2-1) = 1$

At the 5% level of significance and 1 degree of freedom, the critical Chi-Square value is:

$\chi^2_{0.05,1} = 3.841$

Decision rule:

Reject H_0 if χ^2 calculated > χ^2 critical.

Decision: Because the calculated Chi-Square value (28.13) exceeds the critical value (3.841), the null hypothesis is rejected. The result indicates a statistically significant association between biometric verification and e-fraud in online banking. This suggests that stronger biometric authentication measures are associated with reduced vulnerability to electronic fraud in online banking transactions.

Table 5: Observed Frequency (O)

Relationship between Biometric Verification and E-Fraud in Online Banking

Biometric Verification	E-Fraud Reduced (Yes)	E-Fraud Not Reduced (No)	Row Total
Agree	90	30	120
Disagree	20	60	80
Column Total	120	90	200

Expected Frequency Table

$$EF = \frac{(\text{Row Total}) \times (\text{Column Total})}{\text{Grand total}}$$

$E_{11} = (120 \times 110) / 200 = 66$

$E_{12} = (120 \times 90) / 200 = 54$

$E_{21} = (80 \times 110) / 200 = 44$

$E_{22} = (80 \times 90) / 200 = 36$

Biometric Verification	Yes	No	Row Total
Agree	66	54	120
Disagree	44	36	80
Column Total	110	90	200

Table 6: Chi-Square Statistic Computation

The Chi-Square statistic is computed using:

$$\chi^2 = \frac{(O-E)^2}{E}$$

Cell	O	E	O−E	(O−E)²	(O−E)²/E
Agree–Yes	90	66	24	576	8.73
Agree–No	30	54	-24	576	10.67
Disagree–Yes	20	44	-24	576	13.09
Disagree–No	60	36	24	576	16.00
Total χ^2					48.49

$df=(r-1)(c-1)$

$df=(2-1)(2-1)=1$

At the 5% level of significance and 1 degree of freedom. The critical Chi-Square value is:

$\chi^2_{0.05,1}=3.841$. Since, $48.49>3.841$. The null hypothesis (H_0) is rejected.

The analysis indicates a statistically significant relationship between biometric verification and e-fraud in online banking among the 200 respondents ($\chi^2 = 48.49$, df = 1, $p < 0.05$). This finding suggests that respondents generally believe biometric verification contributes significantly to reducing electronic fraud in online banking transactions.

Discussion of findings

The findings of this study revealed that biometric verification has a significant negative relationship with e-fraud in online banking, indicating that the adoption of biometric authentication mechanisms contributes substantially to reducing fraudulent activities in digital banking platforms. This finding suggests that stronger customer authentication through biometric technologies such as fingerprint recognition, facial recognition, voice authentication, and iris scanning enhances the security of online banking systems by making unauthorized access considerably more difficult. The result supports the growing argument that biometric verification represents one of the most effective security innovations in the financial technology sector. Financial institutions increasingly rely on biometric authentication because it strengthens identity verification while simultaneously improving customer convenience. The implication is that banks implementing robust biometric systems are likely to experience lower incidences of account takeover, unauthorized transactions, phishing-related losses, and identity fraud.

This finding is consistent with the work of Bolle, Connell, Pankanti, Ratha & Senior, (2024), who argued that biometric authentication provides stronger user verification than conventional knowledge-based authentication methods because physiological characteristics are unique and difficult to duplicate. Also, Jain, Ross, and Nandakumar (2016) found that biometric technologies significantly improve the security of financial transactions by minimizing identity fraud and unauthorized access. However, the present finding contrasts with the study of Ratha, Connell, and Bolle (2021), who reported that biometric authentication alone cannot completely eliminate fraud because sophisticated attacks such as spoofing, synthetic fingerprints, replay attacks, and presentation attacks may still compromise biometric systems. Their findings suggested that fraudsters continually develop techniques to bypass biometric verification, particularly where biometric systems lack liveness detection or

are poorly implemented. The disparity between their findings and the present study may be explained by technological advancements over the past two decades.

Modern biometric systems incorporate artificial intelligence, deep learning, multi-factor authentication, behavioral analytics, and liveness detection, making them considerably more secure than earlier biometric technologies examined by Ratha et al. (2021). The findings also differ from those of Anderson (2020), who argued that biometric verification may create a false sense of security because many successful banking fraud incidents result from social engineering, phishing attacks, malware, and insider compromise rather than authentication weaknesses. According to Anderson (2020), cybercriminals increasingly exploit human vulnerabilities instead of directly attacking authentication systems. This difference may be attributed to contextual variations in banking environments. While Anderson's study focused broadly on cybersecurity threats affecting digital ecosystems, the present study specifically examined the effectiveness of biometric verification in reducing unauthorized account access within online banking. The findings have important practical implications for financial institutions, regulators, and policymakers.

Automatic Lockout and Online Banking Fraud

The findings of this study indicate that automatic lockout mechanisms have a significant negative relationship with online banking fraud, suggesting that the implementation of automatic account lockout after multiple failed login attempts contributes substantially to reducing fraudulent access to customers' online banking accounts. This finding supports the argument that automatic lockout serves as an effective preventive security control by limiting unauthorized login attempts and reducing the likelihood of successful brute-force attacks, credential stuffing, and password-guessing techniques commonly employed by cybercriminals. The result aligns with the principles of layered security, which emphasize the importance of combining authentication controls with access restrictions to minimize cyber risks. The effectiveness of automatic lockout may also be attributed to the increasing sophistication of banking security systems, where lockout mechanisms are integrated with fraud monitoring tools, real-time alerts, and multi-factor authentication. The present finding differs from the study conducted by Alalwan, Dwivedi, Rana, & Williams, (2018), who reported that account lockout policies alone did not significantly reduce online banking fraud because many financial institutions experienced an increase in customer service requests and account recovery processes, leading some organizations to relax lockout thresholds. Their findings suggested that cybercriminals could exploit lockout mechanisms through denial-of-service tactics by intentionally triggering repeated failed login attempts to lock legitimate customers out of their accounts. The difference between their findings and the present study is based on advancements in cybersecurity technologies since their study was conducted. Modern banking systems increasingly incorporate adaptive authentication, intelligent fraud detection, and risk-based access controls that distinguish between legitimate user errors and malicious login attempts, thereby reducing the unintended consequences associated with automatic lockout. Similarly, the findings contrast with those of Bonneau, Herley, Van, Oorschot & Stajano, (2015), who argued that strict account lockout policies often create usability challenges that encourage users to adopt insecure password practices, such as writing passwords down or creating overly simple passwords that are easier to remember.

According to their study, the inconvenience associated with frequent account lockouts could inadvertently weaken overall security by encouraging risky user behaviour. The discrepancy between their findings and those of the present study may be attributed to differences in user awareness and banking security practices. The implications of these findings are significant for banking institutions, regulators, and policymakers. For financial

institutions, the results reinforce the need to maintain appropriately configured lockout thresholds that balance security with customer convenience.

Conclusion

This study established that while the adoption of digital banking platforms has significantly improved the speed, convenience, and accessibility of financial services, it has also increased the exposure of banks and customers to sophisticated electronic fraud. Authentication technologies such as multi-factor authentication, biometric verification, one-time passwords (OTPs), transaction monitoring systems, and artificial intelligence-based fraud detection have contributed substantially to reducing fraudulent activities. The persistence of cybercriminals, evolving fraud strategies, insider threats, and low levels of customer cybersecurity awareness continue to undermine the effectiveness of these security measures. The study further revealed that effective fraud prevention requires a combination of advanced technological solutions, strong internal control mechanisms, regulatory compliance, continuous staff training, and customer education. A unique contribution of this study lies in its integration of technological authentication techniques with organizational and behavioural factors influencing electronic fraud management within a Nigerian commercial banking environment. Unlike studies that primarily focus on technological solutions, this research provides context-specific evidence from Zenith Bank Plc. in Cross River State, thereby contributing empirical insights into the practical effectiveness of authentication detection techniques in a developing economy. Despite these contributions, the study has certain limitations. First, the research was limited to Zenith Bank Plc. branches in Cross River State, which may restrict the generalizability of the findings to other commercial banks or geographical regions within Nigeria. Second, the study relied primarily on questionnaire responses and participants' perceptions, which may be influenced by personal bias, incomplete disclosure, or social desirability bias. Future research should expand the scope by conducting comparative studies across multiple commercial banks and different regions of Nigeria to improve the generalizability of findings. Longitudinal studies are also recommended to evaluate the evolving nature of electronic fraud and the long-term effectiveness of emerging authentication technologies.

Recommendations

1. Financial institutions (banks and fintech providers) should take the lead in deploying multi-modal biometric verification systems.
2. Banks should implement layered biometric authentication, combining at least two biometric factors (e.g., fingerprint + facial recognition) to reduce spoofing risks.
3. Technology providers and cybersecurity vendors should be responsible for developing secure biometric frameworks that include liveness detection mechanisms to prevent spoofing through photographs, masks, or synthetic media.
4. Financial institutions (banks and digital banking platforms) should implement automatic lockout systems that trigger after a predefined number of failed login attempts (commonly 3–5 attempts). This should occur immediately during the authentication process.
5. Fraud monitoring and cybersecurity teams within banks should continuously analyze login attempt logs in real time using behavioral analytics and AI-driven fraud detection systems. These systems should identify abnormal patterns such as rapid password guessing, multiple IP address changes, or access attempts outside normal user behavior hours.
6. Technology vendors and system architects should design banking platforms with secure session management protocols, ensuring that lockout mechanisms cannot be bypassed through API manipulation or session replay attacks. This should be embedded at the system development and infrastructure design stage.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security*, 4(1), 65–82.

Adeyemi, K. (2020). Cybersecurity awareness and online banking fraud vulnerability among bank users in Nigeria. *Journal of Financial Security Studies*, 8(2), 45–60.

Adeyemi, K. S., & Aluko, O. A. (2020). Electronic banking fraud and its implications on financial institutions in Nigeria. *Journal of Banking and Finance Management*, 8(2), 45–60.

African Union. (2021). *African cybersecurity and cybercrime report*. African Union Commission.

Akinyemi, T. O., & Oladipo, B. F. (2019). Cybersecurity challenges and fraud prevention in Nigerian banking sector. *International Journal of Computer Science and Information Security*, 17(6), 112–120.

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2018). Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and trust. *International Journal of Information Management*, 37(3), 99–110.

Alzoubi, H. M. (2022). Cybersecurity challenges and fraud prevention in digital banking systems. *International Journal of Financial Studies*, 10(4), 1–15.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements.

Bhargava, B., Lu, Y., & Zhang, W. (2017). Security and privacy in mobile biometric systems: A survey. *IEEE Access*, 5, 24386–24403. https://doi.org/10.1109/ACCESS.2017.2769791

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2024). *Guide to biometrics*. Springer.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM*, 58(7), 78–87.

Button, M., Lewis, C., & Tapley, J. (2024). Fraud typologies and the victimization of banking customers. *Security Journal*, 27(1), 1–20.

Central Bank of Nigeria. (2023). *Annual report on electronic payment fraud in Nigeria*. CBN Publications.

Diallo, A., War, A., Diouf, M. A., Samhi, J., Arzt, S., Bissyande, T. F., & Klein, J. (2024). *Security assessment of mobile banking apps in West African Economic and Monetary Union*. arXiv. https://arxiv.org/abs/2411.04068

Economic and Financial Crimes Commission. (2023). *Cybercrime and financial fraud report*. EFCC Press.

Egidi, S. A., Obona, A. A., Ikpeme, D. C., & Aganyi, I. O. (2024). Settlement patterns and census taking in Nigeria. In M. O. Odiong, E. E. Enang, & M. Z. Ismail (Eds.), *Proceedings of the Population Association of Nigeria (PAN) 12th International Conference on Population and Housing Census; Prospects for Demographic Dividend and Sustainable Development* (pp. 15–21). https://popan.ng/conference.php

European Central Bank. (2023). *Report on card fraud and digital payment security in the euro area*. ECB Publications.

Federal Bureau of Investigation Internet Crime Complaint Center. (2024). *Internet crime report*. U.S. Department of Justice.

International Monetary Fund. (2024). *Global financial stability report: Cyber risks to financial stability*. IMF.

Interpol. (2023). *African cyberthreat assessment report 2023*. INTERPOL.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80–105.

Jain, A. K., Ross, A., & Prabhakar, S. (2011). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20.

Kumar, A., & Gupta, R. (2021). Electronic fraud and cybersecurity challenges in digital banking systems. *International Journal of Financial Technology*, 8(2), 45–59.

Kumar, P., & Gupta, S. (2023). Emerging cyber threats and fraud detection mechanisms in digital banking. *Journal of Information Security and Applications*, 72, Article 103402.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62, Article 100415.

Malik, M. (2020). A review of empirical research on internet and mobile banking in developing countries using UTAUT model during the period 2015 to April 2020. *Journal of Internet Banking and Commerce*, 25(2), 1–22.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2019). *Handbook of fingerprint recognition* (2nd ed.). Springer.

Marcel, S., Nixon, M. S., & Li, S. Z. (2014). *Handbook of biometric anti-spoofing: Trusted biometrics under spoofing attacks*. Springer. https://doi.org/10.1007/978-1-4471-6524-8

National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). https://doi.org/10.6028/NIST.SP.800-63b

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2021). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569.

Nigeria Inter-Bank Settlement System. (2023). *Annual fraud landscape report*. NIBSS.

Nwankwo, O. C., & Eze, G. O. (2021). Digital banking security and fraud management in emerging economies: Evidence from Nigeria. *African Journal of Accounting and Financial Research*, 4(1), 23–38.

Odusina, O. A., & Ogunbanwo, A. S. (2020). Biometric authentication and fraud prevention in mobile banking in Nigeria. *Journal of Cybersecurity and Digital Trust*, 4(2), 55–70.

OECD. (2022). *Cybersecurity in the financial sector: Risks, challenges, and policy responses*. Organisation for Economic Co-operation and Development.

Okafor, J., & Dike, L. (2021). Internal control weaknesses and electronic banking fraud in Nigerian deposit money banks. *African Journal of Accounting and Finance*, 12(3), 77–92.

Omotubora, A., & Basu, S. (2018). Regulation for e-payment systems: Analytical approaches beyond private ordering. *Journal of African Law*, 62(2), 281–303.

Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4), 49–61.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2021). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634.

Sabi, H. M. (2014). Research trends in the diffusion of internet banking in developing countries. *Journal of Internet Banking and Commerce*, 19(1), 1–20.

Stallings, W. (2022). *Effective cybersecurity: A guide to using best practices and standards* (2nd ed.). Addison-Wesley

Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology*, 64(16), 1623–1648.

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE*, 92(6), 948–960.

United Nations Conference on Trade and Development. (2008). *E-banking and e-payments: Implications for developing and transition economies*. United Nations Publications.

Ushie, C. A., Ushie, M. A., & Egidi, S. A. (2023). Environmental and demographic implications on internally displaced persons (IDPs). *Journal of Environmental and Tourism Education*, 6(2), Special Edition.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2018). Examining trust in information systems: A multi-factor authentication perspective. *MIS Quarterly*, 42(3), 845–868.

Vyas, S. D. (2012). *Impact of e-banking on traditional banking services*. arXiv. https://arxiv.org/abs/1209.2368

World Bank. (2023). *Digital financial services and cybersecurity challenges in developing economies*. World Bank.