IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 5, Ser. II (Sep. – Oct. 2026), PP 31-41
www.iosrjournals.org

Examining The Effectiveness of Multi-Factor Authentication in Reducing Cyberattacks in Digital Banking

NWENYIM ONYEBUCHI[1], EMEWU BENEDICT MBANEFO[2], OGBAGA IGNATIUS[3], NWEKE HENRY[4], ANIKWE CHIOMA[5]

[1-5] *Department of Computer Science, Dave Umahi Federal University of Health Sciences, Uburu, Ebonyi State, Nigeria*

Corresponding author: nwenyimo@dufuhs.edu.ng

Abstract

Background: *The rapid expansion of digital banking has increased the exposure of financial institutions and customers to phishing, identity theft, malware, credential compromise, and unauthorized account access. Multi-Factor Authentication (MFA) provides an additional layer of security by requiring users to verify their identities through two or more independent authentication factors. However, its effectiveness may be influenced by usability, infrastructure reliability, user awareness, and the choice of authentication method. This study examined the effectiveness of MFA in reducing cyberattacks in digital banking, with particular attention to implementation challenges, vulnerabilities, and security outcomes.*

Methodology: *The study adopted a descriptive survey research design. Data were collected through a structured online questionnaire administered to digital banking users, bankers, cybersecurity professionals, IT administrators, and other relevant respondents. Fifty-two valid responses were analyzed using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics, particularly frequencies and percentages, were used to summarize respondents' perceptions of MFA effectiveness, adoption challenges, authentication vulnerabilities, and outcomes.*

Results: *The findings showed that 78.8% of respondents identified unauthorized login attempts as the cyber threat most effectively reduced by MFA, while 75.0% considered biometric authentication the most effective MFA method. Complexity of use (38.5%), delayed OTP delivery (48.1%), and poor network connectivity (86.5%) were major challenges affecting MFA adoption and use. Fingerprint recognition was identified by 76.9% as an improvement capable of enhancing MFA security, while 90.4% selected biometrics as the technology that could best strengthen MFA. Password authentication remained the most commonly used method (59.6%), although 88.5% considered password-only authentication the most vulnerable. Furthermore, 92.3% reported a strong positive impact of MFA on customer confidence, while 80.8% perceived that MFA greatly reduces financial losses.*

Conclusion: *MFA is an important digital-banking security control, particularly for reducing unauthorized access. Its effectiveness, however, depends on reliable infrastructure, usability, user awareness, and stronger authentication technologies. Greater adoption of biometrics and authenticator-based mechanisms, supported by phishing-resistant controls and continuous security monitoring, is recommended.*

Keywords: Multi-Factor Authentication, digital banking, cybersecurity, cyberattacks, biometric authentication, unauthorized access, authentication security.

Date of Submission: 14-09-2026 Date of Acceptance: 25-09-2026

I. Introduction

Digital transformation has made cybersecurity a central concern for financial institutions because banking services increasingly depend on internet platforms, mobile applications, cloud services, and electronic payment channels. These technologies improve accessibility, convenience, efficiency, and speed, but they also expand the attack surface available to cybercriminals. Phishing, identity theft, malware, ransomware, hacking, and unauthorized access can compromise information assets and produce financial and reputational consequences (Ahmed & Ahmed, 2019; Pulakhandam & Samudrala, 2020; Ali et al., 2020).

Authentication is a fundamental cybersecurity control because it determines whether a user is permitted to access a protected service. Passwords and personal identification numbers have traditionally been used as the principal authentication mechanism, yet weak, reused, stolen, or exposed credentials create opportunities for compromise (Mandru, 2018). Evidence concerning credential-related breaches has consequently strengthened the

case for authentication mechanisms that do not depend on a single secret. MFA addresses this weakness by requiring two or more independent verification factors before access is granted (Devarajan, 2020; Koppanathi, 2020).

MFA commonly combines knowledge factors such as passwords or PINs, possession factors such as mobile devices, smart cards, or tokens, and inherence factors such as fingerprints, facial characteristics, voice patterns, or iris features (Gollapalli, 2020; Obaidat et al., 2020). The central security advantage is that compromise of one factor does not automatically provide access to the protected account. MFA has therefore become relevant to banking, healthcare, government, and e-commerce environments and is supported by contemporary digital identity and information-security guidance (Bodepud; Gopireddy & Koppanathi, 2018; National Institute of Standards and Technology (NIST, 2020).

Digital banking is especially sensitive because financial systems contain valuable personal and transactional information and are continuously connected to external networks. Successful attacks may cause unauthorized transfers, fraud, service disruption, loss of confidential information, regulatory exposure, and reduced customer trust (Al-Alawi & Al-Bassam, 2020). Reported incidents affecting financial organizations and digital financial platforms demonstrate that cybersecurity failures can affect confidentiality, integrity, and availability. The increasing sophistication of cybercrime means that authentication must be treated as part of a broader, layered security architecture rather than as a stand-alone solution.

The effectiveness of MFA also depends on implementation conditions. Complex authentication flows can frustrate users; delayed one-time passwords can interrupt transactions; unreliable networks can prevent legitimate users from completing verification; and inadequate awareness can encourage unsafe behavior. Privacy concerns may also emerge where biometric information is collected. Thus, the security value of MFA must be evaluated alongside usability, reliability, accessibility, infrastructure, awareness, and evolving attack techniques.

1.1 Problem Statement, Aim and Research Questions

Despite the expansion of digital banking, cyberattacks continue to threaten financial institutions and customers. Password compromise, phishing, identity theft, malware, and social engineering can provide attackers with direct routes into customer accounts. MFA is increasingly recommended as a countermeasure, yet implementation challenges can weaken its effectiveness. In particular, authentication processes that are complex, slow, dependent on unreliable networks, or poorly understood by users may reduce adoption and create operational friction.

The study's central problem is therefore not simply whether MFA exists, but whether it is effective in the operational conditions of digital banking and which implementation characteristics determine its security and acceptance. The research addresses the gap by combining perceptions of banking users and relevant technology/security stakeholders with evidence on authentication methods, vulnerabilities, and outcomes.

Aim. The study aimed to examine the effectiveness of multi-factor authentication in reducing cyberattacks in digital banking.

Specific objectives. The study sought to:
(1) assess the effectiveness of MFA in mitigating cyberattacks on digital banking platforms;
(2) examine challenges faced by users and institutions in adopting and implementing MFA;
(3) identify potential improvements in MFA methods that may enhance security and user adoption;
(4) assess current authentication methods and identify vulnerabilities; and
(5) analyze the impact of MFA on unauthorized access and cyber incidents.

Research questions. The investigation was guided by five questions corresponding to the objectives:
(1) How effective is MFA in mitigating cyber threats on digital banking platforms?
(2) What challenges do users and institutions face in adopting and implementing MFA?
(3) What improvements can enhance MFA security and adoption?
(4) What authentication methods are currently used, and what vulnerabilities exist?
(5) What impact does MFA have on unauthorized access and cyber incidents?

Significance. The study has practical significance for banks and security administrators because it identifies authentication factors and operational barriers that should receive attention. It also provides evidence for cybersecurity awareness initiatives and infrastructure improvement. Academically, it contributes empirical evidence on the interaction between authentication technology, perceived security, usability, and digital-banking confidence in a Nigerian context.

II. Literature Review

Cybersecurity in Digital Banking

Cybersecurity in digital banking encompasses technologies, policies, procedures, and human practices used to protect banking systems, networks, customer information, and transactions from unauthorized access, disruption, and misuse. Digital banking increases service availability but simultaneously creates interconnected attack surfaces. Security therefore depends on confidentiality, integrity, and availability, as well as effective governance and user behavior (Stallings & Brown, 2018; Kaspersky, 2020). Nigerian banking environments face additional concerns associated with rapid digital adoption, cybersecurity awareness, and infrastructure limitations.

Cyberattacks and Authentication Methods

Digital banking platforms are targeted by phishing, malware, ransomware, social engineering, insider threats, distributed denial-of-service attacks, identity theft, and credential-stuffing attacks. Phishing is particularly important because it manipulates users into revealing credentials or interacting with fraudulent services. Mobile banking has also become attractive to attackers because smartphones increasingly mediate financial transactions (Verizon, 2023).

Authentication methods are generally organized around knowledge, possession, and inherence factors. Passwords and PINs are knowledge factors; tokens, mobile devices, and smart cards are possession factors; and fingerprints, facial recognition, voice, and iris patterns are inherence factors (Whitman & Mattord, 2021). Password-only systems remain widespread because they are familiar and relatively inexpensive, but their weaknesses include reuse, guessing, phishing, credential theft, and social engineering (Bonneau et al., 2012; Florencio & Herley, 2007).

Multi-Factor Authentication Mechanisms

MFA combines independent authentication factors to increase assurance. Common digital-banking implementations include passwords plus SMS OTPs, app-generated codes, biometric verification, hardware tokens, and adaptive or risk-based authentication. (Grassi, P. A. et al., 2020) Identifies multi-factor mechanisms as an important means of strengthening identity assurance. Ometov et al. (2018) similarly describe MFA as a layered approach capable of improving resistance to credential theft and account takeover. Adaptive systems can incorporate device, location, behavioral, and transaction signals so that stronger verification is requested when risk increases (Dasgupta et al., 2017).

Biometrics are particularly relevant because physiological characteristics are not normally forgotten or voluntarily disclosed in the same way as passwords. Fingerprint and facial recognition can also reduce authentication friction when integrated into mobile devices. Nevertheless, biometric systems require careful attention to privacy, spoofing resistance, template protection, and accessibility (Jain et al., 2016; Ratha et al., 2001; Bolle et al., 2014). Authenticator applications can also provide stronger alternatives to SMS because time-based codes are less dependent on mobile-network delivery and can reduce exposure to some SIM-swap risks (Bonneau et al., 2012; Grassi et al., 2017).

Effectiveness of MFA

Evidence reviewed in the original study generally indicates that MFA reduces successful account compromise compared with password-only authentication. Microsoft (2023) has reported very high protection against automated account-compromise attempts when MFA is appropriately deployed. Aloul et al. (2009), Ometov et al. (2018), and Shafqat et al. (2020) likewise support the security value of additional factors. However, MFA does not prevent all attacks. Phishing, social engineering, SIM swapping, compromised recovery processes and poorly designed verification channels can still undermine security. MFA should therefore be integrated with monitoring, user education, secure transaction controls and incident response.

Challenges of MFA Adoption

MFA creates a security–usability trade-off. Additional verification steps can make authentication more cumbersome, and users may prefer convenience when the perceived security benefit is unclear (Furnell & Esmael, 2017; Braz et al., 2007). Studies of two-factor authentication have identified differences among methods in terms of usability, accessibility, setup effort, and perceived security (Das et al., 2014; Reese et al., 2019). For banking, even short delays can become significant because authentication often occurs during time-sensitive transactions.

Infrastructure is another critical constraint. SMS and app-based authentication depend on functioning telecommunications or internet connectivity. Poor connectivity can cause delayed codes, repeated attempts, and failed logins. Integration with legacy banking applications, device incompatibility, system errors, and maintenance costs can also affect implementation (Shafqat et al., 2020). In developing contexts, these challenges can be amplified by uneven network coverage and varying levels of digital literacy.

Awareness and behavior are equally important. Users who do not understand why MFA is required may perceive additional verification as an unnecessary burden. Security awareness campaigns therefore need to explain not only how MFA works but also why users should protect codes, avoid phishing links, and maintain secure credentials. Bada et al. (2019) emphasize the difficulty of converting awareness into sustained behavior, while Venkatesh et al. (2012) show that perceived usefulness and facilitating conditions influence technology acceptance.

Theoretical Framework: Technology Acceptance Model

The study is anchored in the Technology Acceptance Model (TAM), developed by Davis (1989). TAM proposes that perceived usefulness and perceived ease of use shape users' attitudes and intentions toward technology. In digital banking, users are more likely to adopt MFA when they believe it improves account security and can be used without excessive effort. Venkatesh and Davis (2000) extended the model by examining additional determinants of technology acceptance, while Venkatesh et al. (2012) further addressed consumer technology adoption.

TAM is relevant because MFA effectiveness depends not only on cryptographic or authentication strength but also on whether users consistently enable and correctly use the technology. A technically strong mechanism that customers avoid, disable, or circumvent may provide less practical protection than a secure mechanism that users readily accept. The theory therefore supports the study's emphasis on complexity, convenience, awareness, customer confidence, and technological reliability alongside security.

Empirical Review and Research Gap

Empirical literature reviewed in the source study generally reports stronger protection from MFA than password-only authentication, while also identifying usability and infrastructure barriers. reported the importance of cybersecurity awareness and implementation practices in Nigerian banking, while highlighting phishing as a continuing challenge. The literature nevertheless contains gaps in localized evidence, comparisons among authentication modalities, user-centered analysis, infrastructure constraints, and the relationship between MFA and perceived financial/customer outcomes. The present study addresses these gaps through a multi-stakeholder survey in Nigeria.

III. Methodology

Research Design

The study adopted a descriptive survey research design. The design was appropriate because the study sought to describe respondents' assessments of MFA effectiveness, implementation challenges, authentication vulnerabilities, and outcomes without manipulating the study environment. The design also allowed perspectives from several stakeholder groups to be captured through a common structured instrument.

Population and Sample

The target population comprised digital banking users, cybersecurity professionals, IT administrators, bankers, and other relevant respondents. Customers were included because they directly experience authentication processes, while technical and banking personnel contribute knowledge of implementation and security management. The original study analyzed 52 valid questionnaire responses.

Instrument and Data Collection

Data were collected primarily through a structured online questionnaire. Secondary information was obtained from books, journal articles, reports, and other relevant materials used in the conceptual and empirical review. The questionnaire covered the five research questions and included items addressing threat reduction, MFA methods, adoption challenges, improvement technologies, existing authentication methods, vulnerabilities, customer confidence, and financial-loss reduction.

Data Analysis

The responses were coded and analyzed using the Statistical Package for the Social Sciences (SPSS). Descriptive statistics, particularly frequencies and percentages, were used to summarize categorical responses. Results are presented in tables and a reconstructed state-distribution figure. Because the study used a relatively small, non-probability online sample and descriptive analysis, the results should be interpreted primarily as evidence of respondent perceptions rather than as population-wide causal estimates.

Ethical and Methodological Considerations

The online questionnaire allowed respondents to participate without necessarily disclosing their identities. The study did not report the collection of unnecessary personal identifiers. Nevertheless, for a journal submission, the

authors should ensure that the final manuscript explicitly states the institutional ethical approval or exemption status, informed-consent procedure, data-retention policy, and anonymization approach if these were obtained during the research process. These details are important for international publication and should not be invented where they are unavailable.

Respondent Distribution

Respondents were drawn from eleven Nigerian states. Anambra and Ebonyi accounted for the largest shares, while smaller numbers came from Imo, Enugu, and seven other states. The concentration in the South-East provides useful contextual evidence but limits geographic representativeness.

IV. Results and Discussion

Respondents by State

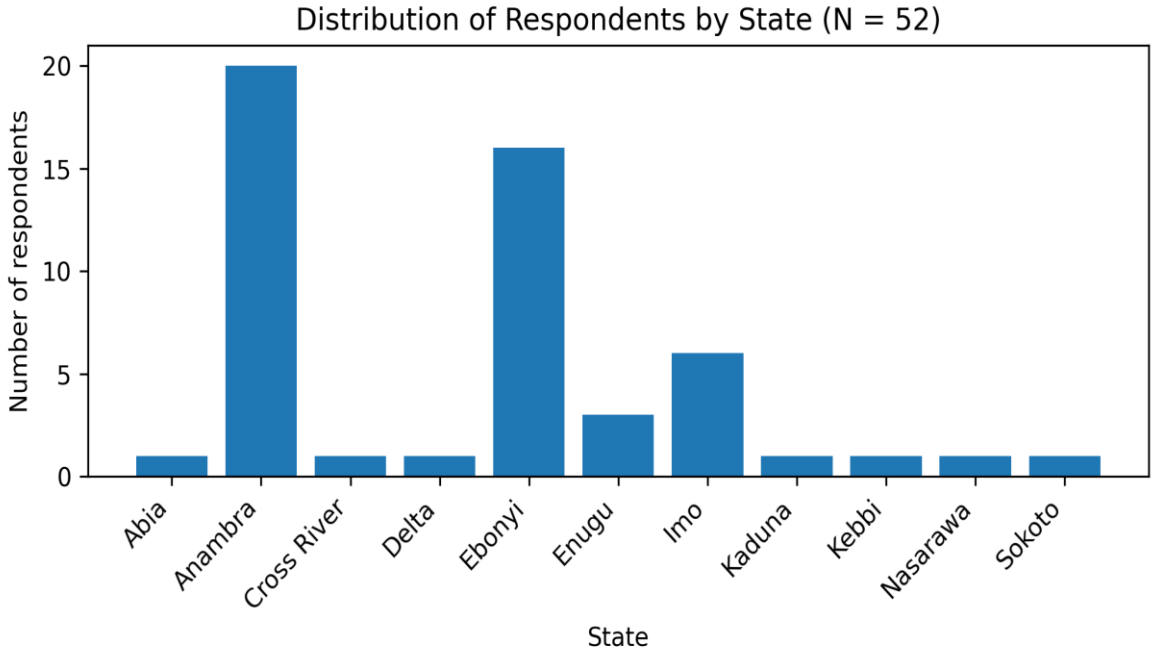

***Figure 1**. Distribution of respondents by state (N = 52).*

Anambra contributed 20 respondents (38.5%) and Ebonyi 16 (30.8%), together accounting for 69.3% of the sample. Imo contributed six (11.5%), Enugu three (5.8%), and Abia, Cross River, Delta, Kaduna, Kebbi, Nasarawa, and Sokoto each contributed one respondent (1.9%). The geographical spread provides some diversity, but the concentration in two states means that the results should not be generalized to all Nigerian digital banking users without further evidence.

Table 1. Distribution of respondents by role

Role	*Frequency*	*Percentage*
Cybersecurity professional	6	11.5%
IT administrator	3	5.8%
Bankers	9	17.3%
Bank customers	3	5.8%
Others	31	59.6%
Total	52	100.0%

The largest category was “Others” (59.6%), followed by bankers (17.3%) and cybersecurity professionals (11.5%). IT administrators and bank customers each accounted for 5.8%. The mix brings together operational, technical, and user perspectives, although the large “Others” category reduces the precision with which stakeholder-specific conclusions can be drawn.

Research Question 1: Effectiveness of MFA in Mitigating Cyber Threats

Table 2. Perceived effectiveness of MFA in mitigating cyber threats

Questions	Options	Frequency	Percentage
5. Which cyber threat is most effectively reduced by MFA?	Phishing attacks	7	13.5
	identity theft	3	
	Unauthorized login attempts	41	5.8
	Malware attacks	1	78.8
	Total	52	1.9
			100.0
6. Which MFA method do you consider most effective for digital banking security?	SMS OTP	7	13.5
	Biometric authentication,	39	75.0
	Email verification	4	7.7
	Security questions	2	3.8
	Total	52	100.0

Unauthorized login attempts were identified by 78.8% of respondents as the threat most effectively reduced by MFA. Only 13.5% selected phishing, 5.8% identity theft, and 1.9% malware. This pattern is consistent with the central function of MFA: preventing a stolen password from being sufficient to complete account authentication. It is also consistent with prior findings that layered verification reduces the likelihood of credential-based account compromise (Ahmed & Ahmed, 2019; Ometov et al., 2018).

Biometric authentication was the preferred MFA method, selected by 75.0% of respondents. SMS OTP was selected by 13.5%, email verification by 7.7%, and security questions by 3.8%. The preference is compatible with the security and usability characteristics associated with biometric verification (Jain et al., 2016; Ratha et al., 2001). However, lower preference for phishing reduction is important: MFA should not be interpreted as a substitute for anti-phishing controls, user education, secure communication channels, and transaction monitoring.

Interpretation

The result supports the view that MFA is especially valuable at the access-control boundary. Its strongest practical contribution is reducing the probability that possession of a compromised password alone will result in successful login. This does not mean that MFA directly prevents every malware, phishing, or ransomware event. Rather, it reduces the ability of some attacks to translate compromised credentials into unauthorized account access.

Research Question 2: Challenges of MFA Adoption and Implementation

Table 3. Challenges affecting MFA adoption and use

Questions	Options	Frequency	Percentage
7. What is the major challenge users face when using MFA?	Complexity of use	20	38.5
	High internet consumption	5	9.6
	Long login process	15	28.8
	Lack of awareness	12	23.1
		52	100.0
	Total		
8. Which factor discourages customers from adopting MFA the most?	Delayed OTP delivery	25	48.1
	Cost of devices	3	5.8
	Privacy concerns	11	21.2
	Technical difficulties	13	25.0
	Total	52	100.0
9. Which technological issue most affects MFA usage?	Poor network connectivity	45	86.5
	Device incompatibility	2	3.8
	System errors	3	5.8
	Software updates	2	3.8
	Total	52	100.0
10. How does customer awareness affect MFA adoption?	Greatly affects	37	71.2
	Moderately affects	7	13.5
	Slightly affects	4	7.7
	Does not affect	4	7.7
	Total	52	100.0

Complexity of use was the leading user challenge (38.5%), followed by long login processes (28.8%) and lack of awareness (23.1%). Delayed OTP delivery was the strongest adoption deterrent (48.1%), followed by technical difficulties (25.0%) and privacy concerns (21.2%). These findings reinforce the security–usability trade-off reported in the literature (Braz et al., 2017; Das et al., 2018; Reese et al., 2019).

Poor network connectivity was by far the most important technological problem, reported by 86.5% of respondents. This is particularly significant where authentication depends on real-time SMS or internet

communication. The finding supports the literature's emphasis on infrastructure as a condition for effective authentication in developing environments (Ometov et al., 2018; Shafqat et al., 2020). Awareness also matters: 71.2% said customer awareness greatly affects adoption, consistent with technology-acceptance research emphasizing perceived usefulness and facilitating conditions (Venkatesh et al., 2012).

The practical implication is that banks should not evaluate MFA solely by cryptographic strength. Authentication services need resilient network dependencies, fast and reliable verification, simple user journeys, accessible recovery processes, and sustained cybersecurity education.

Research Question 3: Potential Improvements to MFA

Table 4. Proposed improvements and preferred authentication technologies

Questions	Options	Frequency	Percentage
11. Which improvement would most enhance MFA security?	Fingerprint recognition	40	76.9
	SMS OTP	11	21.2
	Email verification	1	1.9
	Total	52	100.0
12. Which MFA method is most convenient for users?	Artificial Intelligence	34	65.4
	Block chain	6	11.5
	Cloud computing	9	17.3
	Data analytics	3	5.8
	Total	52	100.0
13. Which technology can best strengthen MFA systems?	Biometrics	47	90.4
	Passwords	2	3.8
	PIN codes	1	1.9
	Security questions	2	3.8
	Total	52	100.0
14. Which authentication factor provides the highest security level?	Mobile authenticator apps	29	55.8
	Email authentication	13	25.0
	PIN verification	9	17.3
	Username authentication	1	1.9
	Total	52	100.0

Fingerprint recognition was selected by 76.9% as the improvement most likely to enhance MFA security, while 90.4% selected biometrics as the technology that could best strengthen MFA. These findings indicate strong respondent confidence in biometric authentication and are consistent with literature describing biometrics as a high-assurance authentication factor (Jain et al., 2016; Bolle et al., 2014; Ometov et al., 2018).

Artificial Intelligence was selected by 65.4% as the most convenient technology. In practical terms, AI can support adaptive or risk-based authentication by analyzing contextual and behavioral signals and requesting additional verification when risk rises. This is consistent with the broader cybersecurity literature on machine learning, automated threat detection, and intelligent risk assessment (Buczak & Guven, 2016; Sarker, 2021). The result should nevertheless be interpreted as a respondent preference rather than empirical evidence that AI-based MFA is objectively more convenient.

Mobile authenticator applications were regarded as the highest-security factor by 55.8%, ahead of email authentication (25.0%), PIN verification (17.3%) and username authentication (1.9%). App-generated codes can reduce dependence on SMS delivery and can mitigate some SIM-swap and interception risks, although they remain vulnerable to phishing and device compromise. The combined findings suggest a practical direction toward biometric authentication, app-based verification, and adaptive risk controls rather than continued dependence on password-plus-SMS models.

Research Question 4: Current Authentication Methods and Vulnerabilities

Table 5. Authentication methods and perceived vulnerabilities

Questions	Options	Frequency	Percentage
15. Which authentication method is most commonly used in organizations?	Password authentication	31	59.6
	Biometric authentication	11	21.2
	Smart cards	4	7.7
	Token-based authentication	6	11.5
	Total	52	100.0
16. Which authentication method is most vulnerable to cyberattacks?	Password-only authentication	46	88.5
	Biometrics,	2	3.8
	Hardware tokens	3	5.8
	Multi-factor authentication	1	1.9
	Total	52	100.0

17. Which cyberattack exploits authentication weaknesses commonly?	Phishing	25	48.1
	DDoS attacks	10	19.2
	Ransomware	8	15.4
	Data corruption	9	17.3
	Total	52	100.0
18. Which factor increases the vulnerability of password systems?	Failure to update passwords	43	82.7
	Strong password encryption	3	5.8
	Use of biometrics	2	3.8
	Security monitoring	4	7.7
	Total	52	100.0

Password authentication remained the most common method (59.6%), despite 88.5% of respondents identifying password-only authentication as the most vulnerable. This apparent contradiction illustrates the difference between prevalence and security strength: passwords persist because of familiarity, low cost and operational simplicity, not because they are intrinsically resistant to modern attacks. The finding agrees with literature describing the continuing dominance and weaknesses of passwords (Bonneau et al., 2012; Florencio & Herley, 2007).

Phishing was the most frequently identified attack exploiting authentication weaknesses (48.1%), followed by DDoS attacks (19.2%), data corruption (17.3%), and ransomware (15.4%). The result reinforces the continuing importance of human-centered attacks and supports prior evidence concerning phishing and stolen credentials (Jagatic et al., 2007; Verizon, 2024).

Failure to update passwords was identified by 82.7% as the factor that increases password-system vulnerability. The result is consistent with evidence that poor password practices, reuse, and weak credential management can increase compromise risk (Florencio & Herley, 2007; Ur et al., 2015). The practical lesson is that MFA should be accompanied by secure credential management and phishing-resistant authentication rather than treated as an isolated technology.

Research Question 5: Impact of MFA on Unauthorized Access and Cyber Incidents

Table 6. Perceived impact of MFA

Questions	**Options**	**Frequency**	**Percentage**
19. What impact does MFA have on customer confidence?	Strong positive impact	46	92.3
	No impact	0	0
	Moderate positive impact	4	5.8
	Slight positive impact	2	1.9
	Total	52	100.0
20. How does MFA affect financial losses from cyberattacks?	Greatly reduces losses	42	80.8
	Moderately reduces losses	10	19.2
	Does not reduce losses	0	0
	Total	52	100.0

Customer confidence showed the strongest positive response in the study. A total of 92.3% reported a strong positive impact from MFA, while 5.8% reported a moderate positive impact and 1.9% a slight positive impact; none reported no impact. This suggests that visible security controls can influence users' perceptions of safety and trust in digital banking. The finding is consistent with technology-acceptance research in which perceived usefulness and security influence willingness to use digital systems (Davis, 1989; Venkatesh et al., 2012).

Regarding financial losses, 80.8% reported that MFA greatly reduces losses associated with cyberattacks and 19.2% reported a moderate reduction; none reported that MFA does not reduce losses. These perceptions are consistent with the logic that preventing unauthorized account access can prevent downstream fraud and unauthorized transactions. They are also directionally consistent with evidence that MFA blocks a large proportion of automated account-compromise attempts (Microsoft, 2023).

In summary, across the five research questions, a consistent pattern emerges. Respondents recognize MFA as a strong access-control measure, especially for preventing unauthorized logins, but they also identify operational conditions that can weaken its practical value. Biometrics and authenticator applications are preferred over password-only and SMS-centered approaches, while poor network connectivity and delayed OTP delivery are major barriers. This supports a layered model in which authentication strength, usability, infrastructure, and user awareness jointly determine security outcomes.

The findings also reinforce TAM. Perceived usefulness is reflected in the strong association between MFA and customer confidence, while perceived ease of use is reflected in concerns about complexity, login length, and OTP delays. Thus, security design and adoption cannot be separated. A mechanism that is difficult to use may produce lower compliance even when it is technically strong.

V. Conclusion

This study examined the effectiveness of Multi-Factor Authentication in reducing cyberattacks in digital banking using evidence from 52 respondents drawn from digital banking, cybersecurity, IT, and banking-related groups. The descriptive findings indicate that MFA is widely perceived as an important security control, with its strongest contribution occurring at the point of account access. Almost four-fifths of respondents identified unauthorized login attempts as the threat most effectively reduced by MFA, and three-quarters regarded biometric authentication as the most effective MFA method.

The study also demonstrates that the effectiveness of MFA is conditional rather than absolute. Complexity, long login processes, delayed OTP delivery, and poor network connectivity can reduce user acceptance and operational reliability. These barriers are especially relevant in settings where mobile and internet infrastructure is inconsistent. Customer awareness is another important determinant, with most respondents reporting that awareness substantially affects MFA adoption.

Biometric authentication emerged as the clearest preferred direction for strengthening MFA, especially fingerprint recognition. Mobile authenticator applications were also viewed favorably, while AI was perceived as a promising technology for convenience and adaptive verification. These findings support a shift from static password-and-SMS models toward authentication architectures that combine strong identity factors with contextual risk assessment and user-centered design.

Password authentication nevertheless remains common, illustrating that adoption of stronger mechanisms does not automatically replace established practices. The finding that 88.5% considered password-only authentication the most vulnerable, while 59.6% still identified passwords as the most commonly used method, highlights a persistent security–convenience gap. Phishing and poor password management remain important attack-enabling conditions.

In all, MFA should therefore be understood as a critical component of digital-banking defense rather than a complete cybersecurity solution. Its greatest value is achieved when strong authentication is combined with reliable infrastructure, user-centered design, phishing resistance, awareness, transaction monitoring, and continuous security governance. The empirical pattern in this study supports broader adoption of biometrics and authenticator-based verification while emphasizing that technology choice must be accompanied by practical measures that enable users to complete authentication reliably and securely.

VI. Recommendations

• Financial institutions should make MFA a core component of digital-banking cybersecurity and progressively reduce reliance on password-only authentication.
• Biometric authentication, particularly fingerprint verification where appropriate, should be expanded while privacy, spoofing resistance, accessibility and secure biometric-template handling are maintained.
• Authenticator applications should be promoted as alternatives to SMS-dependent verification where infrastructure and user circumstances permit.
• Banks should improve network and authentication-service reliability to reduce OTP delays, failed logins and repeated verification attempts.
• Authentication interfaces should be simplified so that stronger security does not create unnecessary friction or encourage users to circumvent controls.
• Continuous cybersecurity awareness should teach customers and employees to recognize phishing, protect verification codes and report suspicious activity.
• Banks should continuously monitor MFA systems, review recovery processes, patch vulnerabilities and introduce risk-based or adaptive authentication as threats evolve.

VII. Limitations and Implications for Future Research

The study has several limitations that should be considered when interpreting the results. First, the sample consisted of only 52 respondents and was geographically concentrated, with 69.3% located in Anambra and Ebonyi. Second, the use of an online survey and a descriptive design limits representativeness and prevents strong causal claims. Third, several outcomes—including reductions in financial loss and cyber incidents—were measured through respondents' perceptions rather than audited banking incident records. Consequently, the findings should be understood as evidence of stakeholder assessment rather than direct estimates of the percentage reduction in real-world attacks.

Future research should use larger probability-based samples across Nigeria's geopolitical zones and compare responses among customers, bankers, security professionals, and IT administrators. Longitudinal studies could examine MFA adoption and incident rates before and after implementation. Experimental or quasi-experimental research could compare SMS OTP, authenticator applications, biometrics, and adaptive authentication under controlled conditions. Future work should also investigate phishing-resistant authentication,

behavioral analytics, AI-assisted risk scoring, privacy-preserving biometrics, and the security of account-recovery mechanisms.

References

[1] Ahmed, A. A., & Ahmed, W. A. (2019). An effective multifactor authentication mechanism based on combiners of hash functions over the Internet of Things. Sensors, 19(17), 3663. https://doi.org/10.3390/s19173663

[2] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity systems in helping manage risk in the banking and financial sector. Journal of Xidian University, 14(7), 1523–1536. https://doi.org/10.37896/jxu14.7/174.

[3] Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. Future Internet, 12(10), 160. https://doi.org/10.3390/fi12100160.

[4] Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two-factor authentication using mobile phones. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641–644). IEEE. https://doi.org/10.1109/AICCSA.2009.5069395

[5] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672

[6] Bodepudi, A., & Reddy, M. (2020). Spoofing attacks and mitigation strategies in biometrics-as-a-service systems. Eigenpub Review of Science and Technology, 4(1), 1–14. https://studies.eigenpub.com/index.php/erst

[7] Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2014). Guide to biometrics. Springer. https://doi.org/10.1007/978-0-387-36582-4

[8] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553–567). IEEE. https://doi.org/10.1109/SP.2012.44

[9] Braz, C., Seffah, A., M'Raihi, D. (2007). Designing a Trade-Off Between Usability and Security: A Metrics-Based Model. In: Baranauskas, C., Palanque, P., Abascal, J., Barbosa, S.D.J. (eds) Human-Computer Interaction – INTERACT 2007. INTERACT 2007. Lecture Notes in Computer Science, vol 4663. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74800-7_9

[10] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[11] Das, S., Kim, T. H.-J., Dabbish, L. A., & Hong, J. I. (2014). *The effect of social influence on security sensitivity.* In Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014), 143–157. USENIX Association.

[12] Dasgupta, D., Roy, A., & Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. Computers & Security, 63, 85–116. https://doi.org/10.1016/j.cose.2016.09.012

[13] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319 -340.https://doi.org/10.2307/249008,http://www.jstor.org/stable/249008.

[14] Devarajan, M. V. (2021). Improving security control in cloud computing for healthcare environments. Journal of Science and Technology, 5(6). DOI:10.46243/jst. 2021.v6. i06.pp244-255

[15] Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In Proceedings of the 16th International Conference on World Wide Web (pp. 657–666). https://doi.org/10.1145/1242572.1242661.

[16] Furnell, S., & Esmael, R. (2017). Evaluating the effect of guidance and feedback upon password compliance, Computer Fraud & Security, Volume 2017, Issue 1, Pages 5-10, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(17)30005-2.

[17] Gollapalli, V. S. T. (2020a). Enhancing disease stratification using federated learning and big data analytics in healthcare systems. International Journal of Management Research and Business Strategy, 10(4), 19–38.

[18] Gollapalli, V. S. T. (2020b). Scalable healthcare analytics in the cloud: Applying Bayesian networks, genetic algorithms, and LightGBM for pediatric readmission forecasting. International Journal of Life Sciences Biotechnology and Pharma Sciences, 16(2).

[19] Gopireddy, R. R., & Koppanathi, S. R. (2018). Post-breach data security: Strategies for recovery and future protection. International Journal of Science and Research, 7(12), 1609–1614. DOI:10.21275/SR24731204000

[20] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B

[21] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2020). *Digital identity guidelines* (NIST Special Publication 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

[22] Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer. https://doi.org/10.1007/978-0-387-77326-1

[23] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

[24] Kaspersky. (2021). *Financial cyberthreats in 2020*. Securelist. https://securelist.com/financial-cyberthreats-in-2020/101638/

[25] Koppanathi, S. R. (2020). Enhancing security in Salesforce: A comprehensive evaluation of multi-factor authentication (MFA). *European Journal of Advances in Engineering and Technology, 7*(1), 55–60. https://doi.org/10.5281/zenodo.13762517

[25] Mandru, S. (2018). The role of cybersecurity in protecting financial transactions. *Journal of Scientific and Engineering Research, 5*(3), 503–510. https://doi.org/10.5281/zenodo.13605493

[26] Microsoft. (2023). *Microsoft digital defense report 2023*. Microsoft. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023/

[27] Obaidat, M., Brown, J., Obeidat, S., & Rawashdeh, M. (2020). A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication. Sensors, 20(15), 4212. https://doi.org/10.3390/s20154212

[28] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1–37. https://doi.org/10.3390/cryptography2010001

[29] Pulakhandam, W., & Samudrala, V. K. (2020). Automated threat intelligence integration to strengthen SHACS for robust security in cloud-based healthcare applications. International Journal of Engineering & Science Research, 10(4).

[30] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614–634. https://doi.org/10.1147/sj.403.0614

[31] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. E. (2019). A usability study of five two-factor authentication methods. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 357–370). USENIX Association. https://www.usenix.org/conference/soups2019/presentation/reese

[32] Sarker, I. H. (2020). Cybersecurity data science: An overview from a machine learning perspective. Journal of Big Data, 8(1), 1–29. https://doi.org/10.1186/s40537-021-00444-1

[33] Shafqat, A., Byun, Y. C., & Kim, D. H. (2020). Enhancing cybersecurity and user authentication in digital systems through secure multi-factor authentication techniques. Electronics, 9(10), 1650. https://doi.org/10.3390/electronics9101650

[34] Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.
Symposium (USENIX Security 12), 65–80. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur
[35] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926
[36] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178. https://doi.org/10.2307/41410412
[37] Verizon. (2023). *2023 data breach investigations report*. Verizon Business.
[38] Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning.