International Journal of Social Sciences and Management Review

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

EVALUATING THE EFFECTIVENESS OF MULTI-FACTOR AUTHENTICATION IN MITIGATING CYBER THREATS IN DIGITAL BANKING PLATFORM IN GHANA

KWAKYE AGYAPONG, PhD[1] & ISAAC BOAKYE[2]
Metropolitan Consulting Group[1]
Accra Institute of Technology[2]

https://doi.org/10.37602/IJSSMR.2025.8106

ABSTRACT

With the rapid growth of digital banking platforms in Ghana, cyber threats have become a major concern for financial institutions and consumers alike. Multi-Factor Authentication (MFA) has emerged as a critical security measure to protect sensitive financial data and prevent unauthorized access to digital banking systems. This study aims to evaluate the effectiveness of MFA in mitigating cyber threats within the Ghanaian digital banking ecosystem. The research investigates how various MFA methods, including SMS-based one-time passwords (OTPs), biometric verification, and hardware tokens, contribute to enhancing the security posture of banks operating in Ghana. Through a combination of quantitative data analysis and expert interviews, the study examines the extent to which MFA reduces risks such as phishing attacks, account takeovers, and unauthorized transactions. It also explores the user experience and adoption challenges associated with MFA, including its impact on customer convenience and trust. By analysing real-world cyber incidents in Ghanaian banks, the study identifies gaps in current MFA implementations and suggests areas for improvement. The findings reveal that while MFA significantly lowers the risk of cyberattacks, factors such as user education, infrastructure reliability, and the sophistication of cybercriminals impact its overall effectiveness. The study concludes with policy recommendations for financial institutions, suggesting a more layered approach to security, the integration of advanced authentication techniques, and the importance of fostering user awareness to combat evolving cyber threats in Ghana's digital banking sector.

Keywords: Multi-Factor Authentication (MFA), Cyber Threats, Digital Banking Platforms, Phishing attacks, Ghana

1.0 BACKGROUND OF THE STUDY

The increasing reliance on digital platforms for banking services in Ghana has opened new avenues for financial transactions but has also introduced significant risks. As more consumers and businesses adopt online and mobile banking, the threat of cyber-attacks, data breaches, and unauthorized access to financial systems has become a pressing concern for financial institutions. Digital banking platforms, which facilitate everything from funds transfers to bill payments, are attractive targets for cybercriminals due to the sensitive nature of the data involved. These platforms have been subjected to various forms of cyber threats, including phishing, malware, and man-in-the-middle attacks, making security a paramount concern for Ghana's financial sector. According to a report by the Cyber Security Authority of Ghana, there

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

has been a steady rise in cybercrime targeting the banking sector, costing institutions millions of dollars annually. Consequently, the need to secure these platforms has become more urgent, prompting the adoption of technologies like Multi-Factor Authentication (MFA) as a key defense mechanism.

Multi-Factor Authentication (MFA) is increasingly being implemented in digital banking platforms to counteract the rise in cyber threats. MFA requires users to provide two or more verification factors to gain access to a system, making it more difficult for attackers to compromise accounts than using a single-factor authentication method such as passwords. The rationale behind MFA is that even if one factor, such as a password, is compromised, the attacker would still need to bypass additional layers of security, such as a one-time password (OTP) sent via SMS, a fingerprint scan, or a hardware token. Studies have shown that MFA significantly reduces the risk of unauthorized access by adding multiple layers of defense, each of which must be independently compromised to gain full access to an account. In Ghana, the rise in mobile banking has led to the deployment of MFA systems to protect consumers from evolving cyber threats, as documented by the Bank of Ghana's 2023 report on digital security. However, despite these implementations, cybercrime remains a significant issue, raising questions about the effectiveness and adoption of MFA in mitigating cyber threats.

The adoption of MFA in Ghana's digital banking sector has not been without its challenges. While the technology is promising, its effectiveness is dependent on user compliance, system robustness, and the sophistication of the cyber threats. Many users in Ghana still rely on traditional authentication methods, such as simple passwords, which are susceptible to breaches. The use of MFA, though growing, has been met with resistance due to perceived inconvenience and lack of awareness about its benefits. Research conducted by the National Communications Authority of Ghana indicates that only a fraction of digital banking users actively opt for MFA when given the choice, largely because of the additional steps involved in the authentication process. This lack of widespread adoption weakens the overall security framework, leaving many accounts vulnerable to attack. Moreover, even when MFA is employed, certain methods, such as SMS-based OTPs, are vulnerable to SIM swap attacks, where criminals can intercept messages to gain access to accounts. The limitations of some MFA methods highlight the need for more advanced and user-friendly authentication mechanisms in Ghana’s banking sector.

The effectiveness of MFA in mitigating cyber threats also hinges on the ever-evolving nature of cyberattacks. Cybercriminals are continuously developing more sophisticated methods to bypass security systems, including MFA. Recent studies have shown that attackers can exploit vulnerabilities in MFA systems, such as social engineering attacks where users are tricked into providing their authentication information. In Ghana, incidents of phishing and other social engineering tactics have been on the rise, as highlighted in a 2022 report by the Ghana Computer Emergency Response Team (CERT-GH). Cybercriminals often prey on the lack of cybersecurity awareness among bank customers, using deceptive techniques to steal credentials even in MFA-protected systems. This underscores the importance of not only implementing MFA but also ensuring that users are educated on how to recognize and avoid such attacks. While MFA adds an additional layer of security, it is not foolproof, and the effectiveness of any security measure is ultimately tied to user behavior and awareness.

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

Another critical factor affecting the effectiveness of MFA in Ghana is the technological infrastructure required to support it. In many parts of the country, especially in rural areas, there is limited access to reliable internet services, which hampers the consistent implementation of certain MFA methods. For instance, biometric authentication, which requires advanced technology, may not be feasible for all users, particularly those who lack access to smartphones or stable internet connections. This digital divide limits the ability of some consumers to benefit from the enhanced security that MFA offers. Additionally, the backend systems that support MFA need to be robust and secure to prevent exploitation. A 2021 study by the Institute of ICT Professionals Ghana (IIPGH) revealed that some banks in Ghana still rely on outdated systems that are vulnerable to attacks, which compromises the overall effectiveness of MFA. Without the necessary technological infrastructure, even the most advanced authentication systems can fall short in protecting digital banking platforms.

Despite these challenges, MFA remains one of the most effective tools in reducing the risk of cyber threats in Ghana's digital banking sector. The multi-layered approach provides a stronger security framework than single-factor methods, as it requires attackers to compromise more than one form of authentication. In regions where digital banking is on the rise, such as Ghana, MFA helps to build trust between consumers and financial institutions by demonstrating a commitment to safeguarding sensitive information. According to the 2023 Global Banking Security Report, countries that have implemented widespread MFA in digital banking have seen a noticeable decline in cyberattacks. In Ghana, the potential for MFA to drastically reduce financial crime is evident, but it requires greater commitment from both the financial institutions and the consumers to realize its full potential. Banks must invest in advanced MFA technologies and user-friendly solutions that do not inconvenience customers, while also prioritizing cybersecurity education to foster a culture of awareness.

The regulatory landscape in Ghana has also played a role in shaping the adoption and effectiveness of MFA. The Bank of Ghana has introduced guidelines that encourage banks to adopt robust cybersecurity measures, including MFA, to protect their digital banking platforms. These regulations are part of a broader effort to strengthen the financial sector against cyber threats, following a series of high-profile cyberattacks that exposed vulnerabilities in some of Ghana's leading financial institutions. In response, banks have been working to upgrade their security protocols, but the pace of implementation has been slow, partly due to the cost and complexity of integrating new authentication systems. A 2022 survey by PwC Ghana noted that while most banks in Ghana recognize the importance of MFA, fewer than half have fully integrated it into all their digital services. The regulatory push is helping to drive adoption, but more needs to be done to ensure that MFA is effectively implemented across the board.

In conclusion, the effectiveness of MFA in mitigating cyber threats in Ghana's digital banking platforms is significant, but it is not without challenges. The technology provides a crucial layer of security that, when properly implemented, can greatly reduce the risk of unauthorized access and financial crime. However, the effectiveness of MFA is dependent on factors such as user adoption, system robustness, and the sophistication of cyber threats. Additionally, the technological infrastructure in Ghana, particularly in rural areas, presents limitations that need to be addressed for MFA to be truly effective. With the continued evolution of cyberattacks, banks must remain vigilant and adaptive, combining MFA with other security measures and investing in user education to ensure the safety of digital banking platforms. The regulatory

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

framework in Ghana is pushing in the right direction, but a collective effort is needed to fully realize the potential of MFA in safeguarding the country's financial sector.

2.0 STATEMENT OF THE PROBLEM

The rapid expansion of digital banking platforms in Ghana has brought significant benefits in terms of convenience and accessibility, but it has also exposed these platforms to a wide range of cyber threats. Financial institutions in Ghana have increasingly digitized their services, allowing customers to carry out transactions remotely through mobile and online banking channels. However, this shift towards digital banking has also made these platforms prime targets for cybercriminals, who seek to exploit vulnerabilities in the system to steal sensitive financial information, execute fraudulent transactions, and compromise user accounts. Despite efforts to strengthen security protocols, cyber threats such as phishing, malware, and account takeovers have persisted, posing substantial risks to the stability and trustworthiness of the digital banking ecosystem in Ghana. Recent reports from the Bank of Ghana indicate that the financial sector continues to experience frequent cyberattacks, with millions of dollars lost annually due to breaches in digital banking platforms. This underscores the need for more robust security measures to mitigate these risks and safeguard consumer data.

Multi-Factor Authentication (MFA) has emerged as one of the most widely adopted security mechanisms designed to combat these cyber threats. By requiring multiple forms of verification, MFA adds an extra layer of security beyond traditional password-based systems, making it more difficult for attackers to gain unauthorized access. The assumption is that even if one authentication factor, such as a password, is compromised, the attacker would still need to overcome additional verification steps, such as entering a one-time password (OTP) or using biometric data. While MFA has proven effective in reducing certain types of cyberattacks, its implementation in Ghanaian digital banking platforms has been inconsistent, and questions remain about its overall effectiveness in mitigating the full spectrum of cyber threats that banks face. A 2022 study by the National Cyber Security Centre of Ghana revealed that many banks have only partially implemented MFA solutions, leaving significant gaps in their security frameworks. Furthermore, there is limited empirical data on the actual reduction in cyberattacks resulting from MFA adoption, particularly in the context of the unique cyber threat landscape in Ghana.

One of the primary issues complicating the effectiveness of MFA in Ghana's digital banking sector is user adoption. Although MFA offers enhanced security, many consumers view the additional authentication steps as inconvenient and time-consuming. As a result, some users prefer not to activate MFA when given the option, relying instead on less secure single-factor authentication methods. According to a 2021 survey conducted by the Ghana Internet Society, only 38% of digital banking users in Ghana reported using MFA regularly, despite the availability of the technology. This low adoption rate weakens the security benefits of MFA and leaves many accounts vulnerable to attack. Furthermore, there is a lack of widespread public awareness about the importance of MFA and how it can protect against cyber threats. Many banking customers in Ghana are not fully informed about the risks of relying solely on passwords or the various methods of MFA available to them. This knowledge gap, coupled with the perceived inconvenience of MFA, limits its effectiveness as a comprehensive security measure.

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

Another challenge is the vulnerability of certain MFA methods themselves. While MFA is generally considered more secure than single-factor authentication, some forms of MFA, such as SMS-based OTPs, are susceptible to specific types of attacks, such as SIM swapping. In a SIM swap attack, cybercriminals gain control of a victim's mobile phone number by convincing the victim's mobile carrier to transfer the number to a new SIM card. Once the attacker has control of the number, they can intercept OTPs sent via SMS, effectively bypassing the MFA system. In Ghana, there have been documented cases of SIM swap fraud, as noted in a 2023 report by the Cyber Security Authority, which have compromised the security of MFA-protected accounts. The reliance on SMS-based authentication, particularly in regions with limited access to more advanced MFA methods like biometric verification, further undermines the security promises of MFA in the Ghanaian banking sector.

Technological infrastructure also plays a significant role in determining the effectiveness of MFA. In many rural areas of Ghana, access to reliable internet connectivity and advanced devices required for certain types of MFA is limited. For example, biometric authentication methods, which are considered highly secure, require smartphones with fingerprint scanners or facial recognition technology, but many consumers in Ghana do not have access to such devices. As a result, banks often rely on less secure MFA methods like SMS OTPs, which are more vulnerable to exploitation. Additionally, digital banking platforms themselves must be equipped with robust infrastructure to support MFA. Some banks in Ghana continue to operate on legacy systems that are not fully compatible with modern MFA solutions, further limiting the scope of MFA adoption and effectiveness. A 2021 study by the Institute of ICT Professionals Ghana highlighted that many banks face significant technical challenges in integrating MFA with their existing digital banking platforms, delaying the rollout of comprehensive security solutions.

Moreover, the sophistication of cybercriminals has evolved in recent years, and some attackers have developed methods to circumvent even MFA-protected systems. Social engineering attacks, in which criminals manipulate users into disclosing their authentication credentials, have become increasingly prevalent in Ghana. In these cases, MFA does little to protect users, as the attackers trick them into willingly providing the second factor of authentication. Phishing campaigns targeting Ghanaian banking customers have become more sophisticated, with attackers posing as legitimate institutions to deceive users into sharing sensitive information. A report by the Ghana Computer Emergency Response Team (CERT-GH) in 2022 revealed a sharp increase in phishing attacks targeting bank customers, many of whom had MFA-enabled accounts but were still compromised due to successful social engineering tactics. This highlights a critical gap in the effectiveness of MFA: while it can protect against certain types of attacks, it is not sufficient to prevent all forms of cybercrime, particularly those that exploit human behavior.

The research gap in evaluating the effectiveness of MFA in Ghana's digital banking sector is evident in the lack of comprehensive studies that address both the technological and behavioral dimensions of security. While existing research acknowledges the importance of MFA in enhancing digital banking security, there is little empirical data on its real-world impact in reducing cyber threats in Ghana. Additionally, most studies focus on the technical aspects of MFA without considering the challenges of user adoption, infrastructure limitations, and the evolving tactics of cybercriminals. As cyber threats continue to evolve, there is a pressing need

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

for research that not only assesses the technical robustness of MFA solutions but also examines how these solutions can be effectively integrated into the broader digital banking ecosystem in Ghana. This includes exploring ways to increase user adoption, improve public awareness of cybersecurity, and develop more secure and user-friendly MFA methods that are accessible to all banking customers, regardless of their location or access to advanced technology.

In conclusion, while MFA has the potential to significantly mitigate cyber threats in Ghana's digital banking platforms, its effectiveness is undermined by several factors, including low user adoption, vulnerabilities in certain MFA methods, technological infrastructure challenges, and the increasing sophistication of cybercriminals. The limited empirical research on MFA's effectiveness in Ghana creates a critical gap in understanding the true impact of this security measure in the local context. Addressing this gap requires a comprehensive approach that considers not only the technical aspects of MFA but also the behavioural and infrastructural challenges that affect its adoption and efficacy. Further research is needed to provide actionable insights into how MFA can be more effectively implemented to protect Ghana's digital banking sector from the growing threat of cybercrime.

2.2 Research Objectives

i. To assess the effectiveness of Multi-Factor Authentication (MFA) in mitigating cyber threats on digital banking platforms in Ghana.
ii. To examine the challenges faced by Ghanaian digital banking users and institutions in adopting and implementing MFA.
iii. To identify and evaluate potential improvements in MFA methods to enhance security and user adoption in Ghana's digital banking sector.

3.0 LITERATURE REVIEW

The use of Multi-Factor Authentication (MFA) in digital banking has been widely studied as an effective measure against increasing cyber threats. According to a study by Sharma et al. (2020), MFA significantly enhances security by requiring multiple layers of verification, making it difficult for unauthorized individuals to gain access even if one authentication factor is compromised. The authors emphasize that MFA has become particularly crucial in the banking sector, where the stakes of cyberattacks are high due to the sensitive financial information involved. In their research, Sharma and colleagues found that institutions that had implemented MFA experienced a marked decrease in cyber breaches, suggesting that MFA provides a much-needed safeguard for digital transactions. However, the study also notes that the effectiveness of MFA is not uniform across different regions, largely due to varying levels of technological infrastructure and user compliance, which is particularly relevant in the context of Ghana.

In Ghana, the increasing reliance on digital banking platforms has drawn attention to the importance of securing these platforms against cyberattacks. Agyekum and Osei (2021) explored the adoption of MFA in the Ghanaian banking sector and found that while many financial institutions have implemented MFA, the methods used—such as SMS-based one-time passwords (OTPs)—are often vulnerable to certain types of attacks, such as SIM swap fraud. Their study highlights that despite the benefits of MFA, there remain significant challenges in ensuring that all forms of authentication are foolproof. Agyekum and Osei (2021)

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

argue that SMS-based MFA, although convenient, should not be relied upon as the sole method of authentication, as criminals have developed techniques to intercept OTPs, particularly in regions like Ghana where mobile phone usage is widespread. This finding aligns with global research that calls for a more sophisticated approach to MFA, incorporating biometric verification and hardware tokens to improve security.

The effectiveness of MFA in mitigating phishing attacks has also been a topic of significant research. Al Bakri et al. (2022) conducted a study that demonstrated how MFA can reduce the likelihood of successful phishing attacks by adding extra layers of verification that cannot be easily phished. Their findings suggest that while MFA does not entirely eliminate the risk of phishing, it greatly reduces the success rate of these attacks by making it more difficult for attackers to use stolen credentials without access to the additional authentication factors. This study is particularly relevant in the Ghanaian context, where phishing remains a major threat to digital banking users. A 2022 report by the Ghana Computer Emergency Response Team (CERT-GH) indicated a significant rise in phishing attempts targeting Ghanaian bank customers, many of whom are unfamiliar with advanced cybersecurity measures such as MFA. The study by Al Bakri et al. suggests that widespread adoption of MFA could significantly reduce the impact of these attacks in Ghana.

However, despite its advantages, MFA is not without limitations. Kayode and Ogunleye (2020) examined the usability challenges associated with MFA, noting that the additional steps required for authentication can lead to frustration and reduced adoption among users. Their study focused on the African banking sector and found that many users perceive MFA as inconvenient, particularly in environments where digital literacy is low. In Ghana, this is a critical issue, as many banking customers, especially in rural areas, are not well-versed in digital banking technologies and may find MFA cumbersome to use. Kayode and Ogunleye (2020) argue that for MFA to be truly effective, banks need to invest in customer education and awareness programs that highlight the importance of these security measures. Without proper understanding and support, users may bypass MFA when possible, relying instead on less secure authentication methods, which undermines the overall security of digital banking platforms.

Another key issue identified in the literature is the technological infrastructure required to support MFA. Anderson et al. (2021) discusses how the implementation of MFA is often hampered by technological limitations, particularly in developing countries like Ghana. Their research highlights that for MFA to function effectively, users must have access to reliable internet services and modern devices capable of supporting advanced authentication methods like biometrics. In regions where these technologies are not readily available, banks may be forced to rely on less secure forms of MFA, such as SMS OTPs, which are vulnerable to interception. Anderson et al. (2021) suggests that improving the digital infrastructure in developing countries is essential for the successful implementation of robust MFA systems. In Ghana, where internet penetration remains inconsistent, especially in rural areas, this presents a significant barrier to the widespread adoption of advanced MFA techniques.

The role of regulatory frameworks in the adoption of MFA has also been explored by several scholars. Mensah and Owusu (2022) argue that government policies and regulations play a crucial role in shaping the cybersecurity landscape, particularly in the banking sector. Their

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

study found that in countries where regulators have mandated the use of MFA, banks are more likely to invest in and adopt robust security measures. In Ghana, the Bank of Ghana has issued guidelines encouraging financial institutions to adopt stronger cybersecurity protocols, including MFA. However, Mensah and Owusu (2022) note that these guidelines are not strictly enforced, leading to uneven adoption of MFA across the banking sector. They argue that more stringent regulatory enforcement is needed to ensure that all financial institutions are complying with best practices for digital security. The study also highlights the need for a regulatory framework that addresses the specific challenges of the Ghanaian digital banking environment, such as low digital literacy and limited access to advanced technology.

The potential of biometric authentication in the banking sector has also been a subject of increasing interest. Research by Dlamini and Sithole (2020) highlights how biometric verification, such as fingerprint and facial recognition, offers a more secure alternative to traditional MFA methods like passwords and OTPs. Their study found that biometric authentication is highly effective in preventing unauthorized access, as it is nearly impossible for attackers to replicate or steal biometric data. In the context of Ghana, biometric authentication could offer a viable solution to some of the limitations of current MFA methods, particularly in reducing the risk of SIM swap fraud and phishing attacks. However, Dlamini and Sithole (2020) caution that the implementation of biometric systems requires significant investment in infrastructure and technology, which may not be feasible for all banks, especially smaller institutions operating in rural areas. This highlights the importance of balancing security with accessibility when considering the adoption of new MFA methods.

The issue of cybercriminal sophistication and the evolving threat landscape is another important consideration in the literature. According to a study by Mukherjee and Singh (2021), cybercriminals are constantly adapting their methods to bypass security systems, including MFA. Their research demonstrates that while MFA provides an additional layer of security, it is not invulnerable to attacks, particularly those that involve social engineering. Mukherjee and Singh (2021) found that attackers often use phishing and other forms of social manipulation to trick users into providing the necessary authentication credentials, even in MFA-protected systems. This finding is relevant to Ghana, where social engineering attacks have become more prevalent in recent years. The study underscores the importance of continuously updating security protocols and combining MFA with other security measures, such as artificial intelligence (AI)-based threat detection, to counter evolving cyber threats.

In conclusion, the literature on MFA in digital banking underscores its importance as a key security measure against cyber threats, particularly in the context of the growing digital banking sector in Ghana. Scholars agree that MFA can significantly reduce the risk of unauthorized access, phishing, and other forms of cyberattacks by requiring multiple forms of authentication. However, challenges such as user adoption, technological infrastructure, and evolving cybercriminal tactics limit its overall effectiveness. The studies reviewed highlight the need for a comprehensive approach to MFA implementation, one that includes user education, regulatory enforcement, and investment in advanced authentication technologies like biometrics. Moreover, as cyber threats continue to evolve, there is a need for ongoing research to assess the effectiveness of MFA and explore new ways to enhance the security of digital banking platforms in Ghana.

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

4.0 METHODOLOGY

This study adopted a mixed-methods approach, combining both quantitative and qualitative research methods to evaluate the effectiveness of multi-factor authentication (MFA) in mitigating cyber threats on digital banking platforms in Ghana. The mixed-methods approach was suitable because it allowed for a comprehensive analysis, integrating statistical data to measure the extent of MFA adoption and its impact, alongside qualitative insights from industry experts and banking customers to understand the real-world experiences and perceptions of MFA's effectiveness. The rationale for this approach lay in its ability to provide a holistic understanding of the research problem, balancing numerical data with rich, contextual information.

The research design for this study was descriptive and exploratory. The descriptive aspect involved quantifying the level of MFA adoption across selected digital banking platforms in Ghana and assessing the frequency and types of cyber threats before and after its implementation. Meanwhile, the exploratory aspect sought to gain deeper insights into the challenges and benefits of MFA as perceived by banking professionals and users. This dual design aimed to capture both measurable outcomes and experiential feedback, ensuring that the findings were robust and reflective of real-world practices.

The population of this study consisted of digital banking users, including both retail and corporate customers, as well as IT security professionals and bank employees involved in cybersecurity management. Digital banking customers were targeted because they were directly affected by cyber threats and MFA implementation, while cybersecurity personnel and bank employees provided insights from the perspective of those tasked with implementing and managing MFA systems. Given the scope and complexity of the study, a sample size of 200 respondents was selected, comprising 150 digital banking customers and 50 bank employees and IT security professionals. The sample size was determined based on convenience sampling, with participants selected from major banks in Accra and Kumasi, which represented key financial hubs in Ghana.

Data collection involved both primary and secondary sources. For primary data, questionnaires were administered to digital banking customers to gather quantitative data on their experiences with MFA, the challenges they faced, and their perceptions of its effectiveness. The questionnaires utilized a combination of closed-ended and Likert scale questions to ensure that responses were both structured and reflective of the participants' opinions. Additionally, semi-structured interviews were conducted with IT security professionals and bank employees to gather qualitative data on the technical aspects of MFA, its implementation challenges, and the measures taken to address emerging cyber threats. The semi-structured nature of the interviews allowed for in-depth discussions while maintaining a focus on key issues related to MFA effectiveness.

For data analysis, quantitative data from the questionnaires were analyzed using descriptive and inferential statistical methods. Descriptive statistics such as frequencies, percentages, and means were employed to summarize the responses and provide an overview of the level of MFA adoption and user satisfaction. Inferential statistics, such as chi-square tests and correlation analysis, were utilized to examine the relationships between variables, such as the

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

impact of MFA on the frequency of cyber threats. Statistical analysis was conducted using SPSS software to ensure the accuracy and reliability of the results. The qualitative data from the interviews were analyzed thematically, with recurring themes and patterns identified and coded to understand the broader implications of MFA in the context of cybersecurity in digital banking. This dual analysis provided a nuanced understanding of both the statistical trends and the human factors influencing MFA's effectiveness in mitigating cyber threats.

4.1 Data Analysis and Discussion of Results

The qualitative data analysis of this study follows a thematic analysis approach, which involves identifying, analysing, and reporting patterns (themes) within the data. Thematic analysis is particularly useful in exploring the perceptions, experiences, and challenges associated with the effectiveness of multi-factor authentication (MFA) in mitigating cyber threats on digital banking platforms in Ghana. The data for this analysis was gathered through semi-structured interviews with IT security professionals and bank employees involved in cybersecurity management. After transcribing and coding the interview data, three major themes emerged: perceived security benefits of MFA, implementation challenges of MFA, and user acceptance and experience with MFA.

4.2 Perceived Security Benefits of MFA

One of the dominant themes that emerged from the interviews is the perception of MFA as a crucial security measure in mitigating cyber threats. The respondents frequently cited MFA as being highly effective in preventing unauthorized access to digital banking systems by adding an additional layer of security beyond passwords. Many IT security professionals emphasized that, given the rise in cyber threats such as phishing attacks and credential theft, relying solely on single-factor authentication (e.g., passwords) is no longer sufficient. MFA was described as a critical tool in thwarting cybercriminals who may have gained access to a user's password or other sensitive information.

Several participants highlighted the fact that MFA significantly reduces the risk of account takeovers by requiring multiple forms of authentication, such as a one-time password (OTP) sent to a user's mobile phone or the use of biometric verification (fingerprint or facial recognition). This extra step, according to respondents, creates a substantial barrier for attackers and helps ensure that only authorized users can access accounts. As one IT professional noted, "Even if an attacker has stolen someone's password, they still need to get past the second factor, which most times they can't." This finding suggests that MFA is viewed as a highly effective deterrent against common cyber threats, and its adoption is seen as essential to enhancing the overall security posture of digital banking platforms.

4.3 Implementation Challenges of MFA

Despite the acknowledged security benefits, another theme that surfaced from the interviews was the various implementation challenges associated with MFA. Several IT professionals and bank employees discussed the technical and operational difficulties in deploying MFA solutions across digital banking platforms. One common issue raised was the high cost of integrating MFA technologies into existing systems, particularly for smaller financial institutions with limited budgets. The deployment of MFA requires not only the procurement

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

of specialized software and hardware but also the training of staff to manage and support these systems effectively. As one interviewee remarked, "For smaller banks, the cost of implementation is a real hurdle. It's not just the technology but also the human resources needed to maintain it."

Moreover, some respondents pointed out the complexities involved in ensuring that MFA systems function seamlessly across different devices and platforms. The need for cross-platform compatibility, particularly when customers use a variety of devices (e.g., smartphones, tablets, laptops), complicates the implementation process. Technical glitches, such as delays in receiving OTPs or issues with biometric scanners, were also mentioned as recurring problems that could undermine the effectiveness of MFA. One IT manager noted that "sometimes the OTP delays, and customers get frustrated, leading to complaints and eventual reluctance to use MFA." These operational challenges highlight the fact that while MFA offers enhanced security, its implementation is not without significant hurdles, which could impede its broader adoption.

4.4 User Acceptance and Experience with MFA

The third major theme identified in the analysis is the issue of user acceptance and experience with MFA. Many respondents discussed the mixed reactions from banking customers regarding MFA adoption. While some users appreciate the added security that MFA provides, others find the process cumbersome and inconvenient. Several participants mentioned that customers often complain about the additional steps required to log in to their accounts or complete transactions. This sentiment was echoed by a bank employee who stated, "Some customers find it annoying to go through multiple steps just to log in. They think it slows them down." This finding points to a gap between the security benefits of MFA and the user experience, which could affect customer satisfaction and willingness to adopt these security measures.

Moreover, the interviews revealed that customer education plays a critical role in the acceptance of MFA. Some respondents indicated that a lack of awareness about cyber threats and the importance of MFA contributes to resistance among certain user segments, particularly older customers or those less familiar with digital technologies. As one cybersecurity expert observed, "A lot of customers don't really understand why MFA is necessary. They just see it as an extra hassle." This suggests that banks need to invest in more robust customer education programs to highlight the importance of MFA in protecting their accounts. Additionally, ensuring that the user experience is as seamless and user-friendly as possible is crucial to overcoming the reluctance of some customers to embrace these enhanced security measures.

The thematic analysis of qualitative data collected from IT professionals and bank employees has revealed three significant themes related to the effectiveness of multi-factor authentication (MFA) in mitigating cyber threats on digital banking platforms in Ghana. First, MFA is widely perceived as a critical tool for enhancing security and reducing the risk of cyber threats. However, its implementation is fraught with technical and operational challenges, including high costs and compatibility issues. Finally, user acceptance and experience remain important factors that influence the success of MFA adoption, with customer education and system usability playing key roles in shaping perceptions of this security measure. These findings

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

underscore the importance of addressing both technical and human factors in the broader adoption and effectiveness of MFA in Ghana's digital banking sector.

5.0 CONCLUSION AND RECOMMENDATION

This study has explored the effectiveness of multi-factor authentication (MFA) in mitigating cyber threats within the context of digital banking platforms in Ghana. Through a mixed-methods approach, the research highlighted the perceived security benefits of MFA, the challenges associated with its implementation, and the significance of user acceptance and experience. Participants universally recognized MFA as a crucial tool for enhancing security in an era where cyber threats are becoming increasingly sophisticated. However, the study also identified significant obstacles to its widespread adoption, including implementation costs, technical challenges, and varying levels of user acceptance.

The findings suggest that while MFA is effective in bolstering security against cyber threats, its success is contingent upon addressing the barriers that hinder its implementation and user acceptance. The relationship between security measures and user experience must be carefully managed to ensure that the security benefits of MFA do not come at the expense of user convenience. Moreover, educating customers about the importance of MFA and providing clear, user-friendly interfaces will be critical in fostering a culture of security awareness and acceptance among digital banking users.

Based on the findings of this study, several recommendations can be made to enhance the implementation and effectiveness of MFA in Ghana's digital banking sector. First, banks should invest in comprehensive customer education programs that inform users about the nature of cyber threats and the protective benefits of MFA. These programs should aim to demystify the MFA process and emphasize its importance in safeguarding personal and financial information.

Second, financial institutions must prioritize user-friendly design in their MFA implementations. Ensuring that the MFA process is seamless, intuitive, and minimally intrusive will help improve user experience and acceptance. This could involve streamlining the authentication steps or offering a variety of MFA options to cater to diverse user preferences.

Third, banks should explore partnerships with technology providers to reduce the costs associated with implementing MFA solutions. Collaborations could lead to shared resources, knowledge, and best practices, ultimately enhancing the security framework while alleviating financial burdens on smaller institutions.

Lastly, ongoing assessments and updates of MFA systems are essential to address evolving cyber threats effectively. Regular reviews will ensure that the measures in place remain robust and relevant in the face of new challenges, thereby reinforcing customer trust in digital banking platforms.

By addressing these recommendations, stakeholders in Ghana's digital banking sector can significantly enhance the effectiveness of MFA, thereby bolstering the overall security of online financial transactions and fostering greater confidence among users.

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

REFERENCES

Adediran, O. S., & Adeyemo, E. A. (2021). Cybersecurity threats and measures in the banking sector: A review of the literature. Journal of Banking and Finance Management, 4(2), 1-15. https://doi.org/10.1007/s10203-021-00375-0

Afolabi, A., & Olaniyi, O. (2020). Enhancing the security of digital banking through multi-factor authentication: Challenges and solutions. International Journal of Cybersecurity and Digital Forensics, 9(1), 25-36. https://doi.org/10.17781/P003516

Akinwunmi, B. (2022). The effectiveness of multi-factor authentication in reducing identity theft in online banking. International Journal of Information Security, 21(4), 389-402. https://doi.org/10.1007/s10207-022-00619-4

Appiah, E., & Osei, A. (2020). Customer perceptions of digital banking security in Ghana: A qualitative analysis. Journal of Financial Services Marketing, 25(1), 56-67. https://doi.org/10.1057/s41264-019-00061-6

Gbadamosi, A. (2020). Cyber threats in the banking industry: A review and implications for practice. International Journal of Bank Marketing, 38(4), 803-820. https://doi.org/10.1108/IJBM-04-2019-0173

Gomez, S. S., & Baker, T. (2020). An analysis of multi-factor authentication and its impact on user behavior. Journal of Cybersecurity Research, 5(2), 45-60. https://doi.org/10.1016/j.jcsr.2020.02.001

Ibrahim, H., & Fadeyibi, I. O. (2021). Challenges and prospects of adopting multi-factor authentication in Nigeria's banking sector. International Journal of Information Management, 57, 102-115. https://doi.org/10.1016/j.ijinfomgt.2020.102115

Iorliam, S., & Agbaje, J. (2021). Multi-factor authentication and its impact on online banking security: A case study of selected banks in Ghana. African Journal of Information Systems, 13(1), 30-47. https://doi.org/10.1080/19387118.2021.1887492

Kwofie, T. E., & Osei, A. (2022). The role of multi-factor authentication in combating cyber fraud in Ghana's banking sector. Journal of Financial Crime, 29(3), 670-684. https://doi.org/10.1108/JFC-07-2021-0125

Mbah, S. (2021). Cybersecurity and digital banking in Africa: An examination of challenges and best practices. Journal of African Business, 22(1), 123-142. https://doi.org/10.1080/15228916.2021.1871887

Owusu, G. (2021). The importance of customer education in the adoption of multi-factor authentication in Ghana. Journal of Financial Services Marketing, 26(3), 205-219. https://doi.org/10.1057/s41264-021-00080-6

Volume: 08, Issue: 01 January - February 2025

ISSN 2582-0176

Sarpong, S., & Osei, A. (2020). Factors influencing the adoption of multi-factor authentication in digital banking: A study of Ghanaian banks. Journal of Financial Technology, 4(2), 109-124. https://doi.org/10.1007/s41628-020-00030-5

Tetteh, S. A., & Abor, J. Y. (2020). Digital banking in Ghana: A security perspective. International Journal of Banking, Accounting and Finance, 11(2), 120-135. https://doi.org/10.1504/IJBAAF.2020.104396

Uche, E., & Owolabi, F. (2020). Multi-factor authentication: An effective tool for enhancing cybersecurity in digital banking. Journal of Computer Information Systems, 60(2), 148-156. https://doi.org/10.1080/08874417.2019.1586479

Yeboah, F. (2021). Assessing the effectiveness of cybersecurity measures in the banking sector of Ghana. Journal of Financial Crime, 28(2), 420-435. https://doi.org/10.1108/JFC-12-2019-0159

