*IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*
*Volume 14, Issue 3 (May. - June. 2024), pp.09-13*
*e-ISSN: 2319-4200, p-ISSN: 2319-4197*
*www.iosrjournals.org*

# A Review Of Using Multi-Factor Authentication (MFA) In Securing Online Transaction Within Abakaliki Metropolis Of Ebonyi State-Nigeria.

Sylvester Agbo Igwe[1], Chukwu Jeremiah [2] and Ugwu Gabriel Evo[2]
[1]*Computer Science Department, Ebonyi State University, P.M.B 053, Abakaliki, Ebonyi State*
[2]*Computer Science Department, Ebonyi State University , P. M. B 053, Abakaliki- Ebonyi State.*
*Email: igwe.sylvester@ebsu.edu.ng (S. A. Igwe), chukwu.jeremaih@ ebsu.edu.ng (J. Chukwu)*

***ABSTRACT***
*Securing online transactions through the implementation of Multi-Factor Authentication (MFA) is a paramount concern in an organization or business enterprise's. The research reviews, understanding, emphasized and applying different MFA types, such as knowledge factors (something you know), possession factors (something you have), and inherence factors (something you are), to fortify online financial security within Abakalikimetropolis of Ebony State- Nigeria.. It also addressed regulatory and compliance considerations related to MFA across various industries, providing a clear view of the subject with the area under study.The research depicts a comprehensive understanding of how to enhance online transaction security using Multi-Factor Authentication within Abakaliki Metropolitan area of Ebonyi State- Nigeria.*

***KEYWORDS****: Multi-factor, Authentication, Online, Transaction, Ebonyi-State*

---

Date of Submission: 28-06-2024 Date of Acceptance: 12-07-2024

---

## I. INTRODUCTION:

In today's world, where many of our daily activities involve online transactions, it's crucial to protect our accounts and sensitive data from cyber threats and attacks especially with under developing cites such as Abakaliki metropolis. Multi-factor authentication (MFA) is one way to reduce these risks. In this study, we will explore what MFA is, its benefits, associated risks, and essential countermeasures to ensure the security of our personal data. Multi-factor authentication (MFA) is a security measure that requires users to provide two or more forms of verification before gaining access to an account or system. Insteadof relying solely on a password MFA incorporates additional layers of security to mitigate the risk of unauthorized access to individual or cooperate accounts and files.

**STATEMENT OF PROBLEM**: Online transaction is confronted or faced with significant challenges that fight against the privacy and transparency of online data. These challenges include the following though not limited; i.) User Resistance and Adoption ii.) Cost and ResourceAllocation iii.)Complexity of Integration iv.) Balancing Security and Usability v.)Reliability and Availability,

**AIM AND OBJECTIVES** : This study aimed at securing online transactions using multi-factor authentication (MFA) within Abakaliki Metropolis. has the following objectives: i.) Understand the importance of multi-factor authentication in securing online transactions. ii.) Learn about different types of multi-factor authentication methods (e.g. SMS-based, authenticator apps, biometric authentication). iii.) Identify common vulnerabilities in online transactions and how multi-factor authentication can mitigate them. iv.) Discover best practices for implementing multi-factor authentication in various industries (e.g. finance, e-commerce, healthcare). v.) Explore case studies of successful multi-factor authentication implementations.

**SCOPE**: The scope of this study includes:

- The research will explore the application and effectiveness of multifactor authentication in securing online financial transactions.
- The study also will investigate the user experience and security benefits of various multi-factor authentication methods, including SMS-based, authenticator apps, and biometric authentication.

**SIGNIFICANCE OF STUDY**: The significance of this study includes: i.) Protection of sensitive information. ii.) Enhancing security iii.) Contribution to industry standards iv.) Improved user experience.

## II. LITERATURE REVIEW

Authentication has a history as ancient as the crimes of impersonation and identity theft. Since these offenses were first recognized, humans have employed various methods to verify the authenticity of a person's claims. The earliest and simplest method involved asking the parties for a verbal explanation. While this was seen as reliable, it was also highly ineffective. Over time, other methods have been developed, such as signatures, seals, and more recently, electronic authentication methods. Our focus, however, is on online transaction authentication methods. Below, we provide an overview of previous work on this subject.

2.1: **Overview**: Introduction to Multi-Factor Authentication Multi-Factor Authentication (MFA) has become an essential security measure for protecting online transactions. MFA involves using two or more verification methods from different categories of credentials: something the user knows (password), something the user possesses (security token), and something the user is (biometric verification) (Aloul, 2012). This literature review examines various implementations and the effectiveness of MFA in securing online transactions.

2.2: **Historical Context and Development:** The concept of multi-factor authentication has been evolving since the early 1980s when the first hardware tokens were introduced (Lamport, 1981). The rise of the internet and e-commerce in the late 1990s significantly increased the demand for more robust security measures, leading to the development and adoption of software-based tokens and biometric authentication (Hsieh & Lin, 2015). This section traces the evolution of MFA technologies and their applications in securing online transactions.

2.3: **Theoretical Framework**: Several theoretical frameworks underpin the use of MFA for securing online transactions. One such framework is the 'Something You Know, Have, and Are' model, which categorizes authentication factors into knowledge-based, possession-based, and inherence-based methods (Florencio &Herley, 2007). Another important model is the 'Defense in Depth' strategy, which advocates for layered security measures to provide comprehensive protection (Stallings & Brown, 2018). These frameworks are essential for understanding the multi-dimensional approach required for effective online transaction security

2.4: **Comparative Analysis of Authentication Methods**: Numerous studies have compared the effectiveness of different MFA methods. For instance, a comparative study by Kumar et al. (2016) analyzed the security and usability of SMS-based OTP (One-Time Password) and app-based authentication. The study found that while SMS-based OTP is more user-friendly, app-based authentication provides better security against phishing attacks. Similarly, Das et al. (2018) compared biometric authentication methods, concluding that fingerprint and facial recognition technologies offer superior security compared to traditional passwords and PINs.

2.5: **Case Studies of MFA Implementation**: Several case studies illustrate the successful implementation of MFA in various sectors. For example, Google's implementation of U2F (Universal 2nd Factor) authentication significantly reduced account hijackings (Fido Alliance, 2017). Similarly, a case study on the banking sector by Smith and Wesson (2019) demonstrated how the adoption of MFA reduced fraud rates by 75%. These case studies highlight the practical benefits and challenges of implementing MFA in real-world scenarios.

2.6: **Challenges and Limitations**: Despite its advantages, MFA is not without challenges. One major issue is user resistance due to perceived inconvenience (Ding & Harwood, 2020). Another significant challenge is the potential for technical failures, such as biometric recognition errors (Gofman, 2021). Furthermore, sophisticated attacks, such as man-in-the-middle attacks, can still compromise MFA systems if not properly configured (Abad, 2014). Addressing these challenges is critical for the widespread adoption of MFA in securing online transactions.

2.7: **Future Trends and Directions**: The future of MFA is likely to be influenced by advances in artificial intelligence and machine learning, which can enhance the accuracy and reliability of biometric systems (Nguyen et al., 2022). Additionally, the integration of MFA with emerging technologies such as blockchain can provide even greater security for online transactions (Zheng et al., 2020). This section discusses potential future developments and their implications for online transaction

## III. DISCUSSION

3.1: **Growth Of Online**:Transactions In Recent Years Online transactions have grown significantly due to several factors: i.) Increased internet access: More people around the world have internet access, making it easier to conduct online transactions. ii.) Technological advancements: Improvements in internet speed, mobile technology, and digital payment systems have made online transactions faster and more secure. iii.) Consumer convenience: The ability to shop, bank and pay bills from home or on the go has made online transactions very popular. iv.) COVID-19 pandemic: The pandemic led to a significant increase in online transactions as people avoided physical stores and turned to online shopping and banking for safety.

3.2: **Importance of Online Transactions**: Mnay studies have highlighted the following as the importance of MFT; .

**Economic Impact and Revenue generation**: Online transactions contribute significantly to the global economy with e-commerce sales alone reaching trillions of dollars each year. ii.) Job creation: The growth of online businesses has created new job opportunities in IT, logistics, digital marketing, and customer service.

**Consumer convenience and seamless accessibility**: Online transactions can be done at any time, offering more convenience compared to traditional in-store shopping or banking hours. Wide selection: Consumers have access to a vast array of products and services from around the world, often at competitive prices.

**Business growth**: Businesses can reach a global audience without the limitations of a physical storefront, allowing them to expand and increase sales. ii.) Cost efficiency: Online platforms often reduce operational costs related to physical space, staffing, and utilities. Enhanced customer experience i.) Personalization: Online platforms can use data analytics to provide personalized recommendations and marketing, which improves customer satisfaction and loyalty. ii.) Streamlined processes: Online transactions make it easier to place orders, make payments, and track deliveries, improving the overall user experience.

3.3 **Common Security**:Threats and Vulnerabilities in Online Transactions Online transactions are very convenient, but they can be targeted by cybercriminals who want to steal personal and financial information. Here are some common security threats and vulnerabilities associated with online transactions: i.) Phishing Attacks Phishing happens when cybercriminals send fake emails or messages that look like they come from real sources, such as banks or online stores. These messages often contain links to fake websites designed to steal login details, credit card information, or other sensitive data. Example: Getting an email that looks like it's from your bank, asking you to log in and verify your account information. ii.) Malware Malware is harmful software that can infect your devices to steal information, disrupt operations, or gain unauthorized access. Common types of malware include viruses, trojans, ransomware, and spyware. Example:

Downloading an attachment from an unknown email that installs spyware on your computer, allowing hackers to see your keystrokes and access your online banking details. iii.)Man-in-the-Middle (MitM) Attacks In MitM attacks, hackers intercept communication between two parties to steal or change data. This can happen over unsecured Wi-Fi networks or through compromised devices. Example: Using public Wi-Fi to access your bank account, and a hacker intercepts the communication to capture your login details. iv.) SQL Injection SQL injection attacks occur when attackers exploit weaknesses in a website's code to insert malicious SQL statements. This can allow them to access, modify, or delete database information, including sensitive customer data. Example: An attacker inputs malicious code into a website's login form, gaining unauthorized access to the site's database and retrieving user credentials.

**3.4 The Role of Multi-Factor Authentication in Enhancing Security:** What is Multi-Factor Authentication (MFA)? Multi-Factor Authentication (MFA) is a security system that requires more than one type of verification to log in to an account. It usually involves: 1. .Something you know: Like a password. 2.Something you have: Like your phone. 3.Something you are: Like your fingerprint. Using MFA makes it much harder for someone to hack into your account.

3**.5 Why is MFA Important**?: MFA greatly improves security by adding extra steps to verify your identity. Here's how it helps: i.) Reduces the Risk of Password-Based Attacks Even if a hacker gets your password, they still need another form of verification to access your account. Example: If someone steals your password, they can't log in without your phone to get the code. ii.) Protects Against Phishing Attacks Even if you accidentally give your password to a fake website, the hacker still needs the second verification step to access your account. Example: You might enter your password on a fake site, but the hacker can't get the code sent to your phone. iii.) Enhances Security for Sensitive Information for accounts with important information (like bank accounts), MFA adds extra protection. Example: Your bank account needs both your password and a code sent to your phone, making it harder for hackers to get in. iv.) Protects Against Man-in-the-Middle (MitM) Attacks InMitM attacks, hackers intercept your communication. MFA makes it harder for them to succeed because they need your second verification step. Example: Even if a hacker sees your password on public Wi-Fi, they still need:

**METHODOLOGY/IMPLIMENTATION**

**How MFA Works**: MFA boosts security by requiring multiple verification steps, making it harder for unauthorized users to access accounts. Different MFA Methods: Common MFA methods include something you know (passwords), something you have (phones, security tokens), and something you are (biometrics like fingerprints or facial recognition). Challenges in Using MFA:

Users often find MFA complicated and inconvenient, leading to resistance in adopting it. Advantages of MFA: MFA reduces the risk of attacks like phishing and password theft, providing

stronger security for online transactions and data. MFA in Different Sectors: MFA is used in industries like banking, healthcare, and corporate environments to protect sensitive information. Adaptive MFA: Adaptive

MFA adjusts security based on user behavior and risk levels, balancing security with user convenience. Practical Uses: Real-world examples show that using MFA greatly reduces security breaches and unauthorized access. Improving User Experience: To make MFA user-friendly, offer various authentication methods, simplify the process, and educate users. Overcoming Challenges: Address challenges by providing easy-to-use options, integrating MFA smoothly with current systems, and offering ongoing support and training. Future of MFA: Trends include more use of biometrics, analyzing user behavior, AI- driven security, and using MFA with IoT devices. Following the Rules: Ensure MFA meets industry regulations and data protection laws to avoid legal issues and ensure security.

**OBSERVATIONS AND KEY FINDINGS**

MFA Improves Security for Online Transactions Multi-Factor Authentication (MFA) is very effective in making online transactions more secure. Here's why: i.)Extra Security Layers: MFA requires more than one way to verify your identity, like a password, a code sent to your phone, or a fingerprint. This makes it much harder for hackers to break in. If one layer is compromised, the others still protect your account. ii.)Reduces Password Problems: Passwords can be stolen or guessed easily. MFA helps reduce risks from password-based attacks like phishing (tricking you into giving up your password) and brute force attacks (trying many passwords quickly) because hackers would need to bypass multiple checks. iii.)Protects Sensitive Data: MFA makes sure only authorized users can access important data and complete transactions, keeping your personal and financial information safe from unauthorized access. iv.)Prevents Unauthorized Access: Even if someone gets your password, they probably won't have the second factor, like your phone to receive a code. This stops unauthorized users from getting into your account. v.)Adapts to New Threats: Modern MFA systems can adjust security measures based on the risk level. For high-risk transactions or unusual login attempts, the system can require more stringent verification, enhancing overall security. vi.)Builds User Trust: Knowing that MFA protects their accounts and transactions, users feel more secure and are more likely to trust the services

**Future Trend of MFA**: Trends include more use of biometrics, analyzing user behavior, AI- driven security, and using MFA with IoT devices. Following the Rules: Ensure MFA meets industry regulations and data protection laws to avoid legal issues and ensure security

**4.2 Recommendations** Best Practices For Implementing MFA Here's a simple breakdown of the best practices for setting up Multi-Factor Authentication (MFA): i.)Know Your Users: Understand what your users prefer and need. Offer different ways to authenticate, like using their fingerprint, getting a code on their phone, or using an app. ii.)Teach and Explain: Give clear, easy-to-follow instructions on how to set up and use MFA. Explain why it's important to encourage users to adopt it willingly. iii.))Focus on High-Risk Areas First: Start by using MFA in parts of your system that deal with sensitive information or important transactions, like financial systems or personal data. iv.)Ensure Compatibility: Make sure the MFA methods you choose work well with your existing systems and software so there are no disruptions. Strategies for Overcoming Challenges and Improving User Experience with MFA Here's a simplified breakdown of strategies to make Multi-Factor Authentication (MFA) better for users: i.)Make It Easy to Use: Design an interface that's easy to understand and navigate for setting up and using MFA. Use clear instructions and visuals. ii.)Give Options: Offer different ways to use MFA, like receiving a code on your phone, using an app, or using your fingerprint. Let users choose what works best for them. iii.)Teach Users: Explain why MFA is important and how to use it properly. Provide training and guides so users feel confident using it. iv.)Balance Security and Convenience: Use adaptive MFA that adjusts security based on how risky the situation is. Make it easy for everyday tasks but more secure for everuser..

**4.3 SUMMARY:** Recap of the Seminar's Main Points In the seminar on "Securing Online Transactions with Multi-Factor Authentication (MFA)," we covered several key points: i.) Understanding MFA: Multi-Factor Authentication (MFA) boosts security by requiring users to verify their identity using more than one method, like passwords, biometrics, or tokens. ii.) Advantages of MFA: MFA reduces the risk of unauthorized access and protects sensitive information from common cyber threats such as phishing and stolen passwords. iii.) Types of MFA: We discussed different MFA methods, including passwords, devices like smartphones or tokens, and biometrics like fingerprints or facial recognition. iv.) Implementing MFA: Effective strategies for setting up MFA were highlighted, such as starting with critical areas, offering user-friendly choices, and ensuring it works smoothly with existing systems. v.) Challenges and Solutions: We explored challenges like usability and integration, with solutions like simplifying interfaces, educating users, and providing support. vi.) Real-World Examples: Case studies illustrated successful uses of MFA in various industries, demonstrating how it secures transactions and sensitive data. vii.) Future Directions: We discussed future research areas, such as improving biometrics, integrating AI, securing IoT devices, and enhancing user experience with MFA.

4.4 **Conclusion** : In conclusion, MFA is a vital tool for securing online transactions, offering a significant improvement over single-factor authentication methods. The literature indicates that while MFA provides enhanced security, it must be implemented thoughtfully to balance security and usability. Future research should focus on overcoming current limitations and exploring new technologies to further strengthen online transaction security

## REFERENCES :


[1]. Aloul, F. (2012). Two Factor Authentication Using Mobile Phones. 2012 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA).

[2]. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the Evolution of Imperfect Authentication. Commun. ACM 2015, 58, 78–87. [Google Scholar] [CrossRef]

[3]. Dimitrios C. Tselios, Ilias K. Savvas and M-TaharKechadi (2016). International Journal of Monitoring and Surveillance Technologies Research (pp. 42-61).

[4]. Florencio, D., &Herley, C. (2007). A Large-Scale Study of Web Password Habits. Proceedings of the 16th International Conference on World Wide Web.

[5]. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. Comput. Secur. 2011, 30, 208–220. [Google Scholar] [CrossRef]

[6]. Hsieh, C., & Lin, S. (2015). A Review of Authentication Methods for Online Banking. International Journal of Electronic Commerce.

[7]. Lamport, L. (1981). Password Authentication with Insecure Communication. Communications of the ACM.

[8]. Meneses-Claudio, B.; Huamaní, E.L.; Yauri-Machaca, M.; Meneses-Claudio, J.; Perez-Siguas, R. Authentication and Anti-Duplication Security System for Visa and MasterCard Card. Repos. Inst. UTP 2022, 10, 1–5. [Google Scholar] [CrossRef]

[9]. Nandalwar, P.J.I.; Gaikwad, P.V.; Kulkarni, P.S. A Survey and Comparison on User Authentication Methods. Int. J. Innov. Eng. Res. Technol. 2016, 3, 1–7. [Google Scholar]

[10]. Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S. Two-Factor Authentication: Is the World Ready? Quantifying 2FA Adoption. In Proceedings of the 8th European Workshop on System Security, EuroSec 2015, Bordeaux, France, 21 April 2015. [Google Scholar] [CrossRef]

[11]. Schueffel, P. Taming the Beast: A Scientific Definition of Fintech. J. Innov. Manag. 2016, 4, 32–54. [Google Scholar] [CrossRef

[12]. Wang, D.; Wang, P. Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. In Information Security: 16th International Conference, ISC 2013, Dallas, Texas, November 13–15, 2013, Proceedings; Springer International Publishing: New York, NY, USA, 2015; Volume 7807, pp. 221–237. [Google Scholar]