© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719319

An Improved Multifactor Authentication Model for Minimizing Data Breaches and Unauthorized Access

SAMUEL OKON BASSEY[1], DR. OGUNTUNDE TOYIN[2]
[1, 2]*University of Ibadan*

Abstract- ***In the digital age, the increasing frequency of data breaches and incidents of unauthorized access has highlighted critical weaknesses in conventional authentication systems. This dissertation presents an improved multifactor authentication (MFA) model aimed at enhancing data security and minimizing unauthorized access in both personal and enterprise-level digital systems. The problem addressed stems from the limitations of existing MFA approaches, which often rely on static factors that are susceptible to phishing, social engineering, brute force attack, man-in-the middle attack and device compromise. The study begins by identifying the limitations of existing MFA methods, particularly their reliance on static credentials and lack of adaptability to emerging threat patterns. To address these issues, the research introduces a novel authentication framework that incorporates multiple dynamic factors such as biometric authentication, behavioral analytics, risk-based authentication, and location-based authentication, alongside conventional factors like passwords and one-time codes (OTP).The methodology involved designing the enhanced MFA model, simulating various attack scenarios, and conducting performance evaluations using security metrics such as authentication accuracy, response time, and resistance to breach attempts. Results demonstrated that the proposed model offers improved detection of suspicious activity, faster authentication processing, and significantly reduced risk of unauthorized access. Based on the findings, it is recommended that organizations adopt An Improved Multifactor Authentication Systems to strengthen access control mechanisms. The study concludes with suggestions for further research into integrating artificial intelligence and machine learning to continuously evolve authentication protocols in response to emerging threats.***

I. INTRODUCTION

1.1 Background/Introduction

In the digital age, cybersecurity has become a critical concern due to the increasing reliance on online systems for communication, business transactions, and data storage. One of the most effective ways to secure systems is through authentication mechanisms that verify user identities before granting access to sensitive information.

Single-factor authentication, typically through passwords, has proven inadequate, as users often create weak passwords or reuse them across multiple platforms. This makes systems vulnerable to attacks like phishing, brute force attacks, and credential stuffing.

To mitigate these risks, Multi-Factor Authentication (MFA) has emerged as a stronger defense by requiring additional verification factors, such as something the user knows (password), something they have (a phone or token), and something they are (biometrics). While MFA significantly improves security, it is not without flaws.

Current MFA methods can still be bypassed through techniques like SIM-swapping, man-in-the-middle attacks, or phishing. Furthermore, user adoption can be hindered by the complexity or inconvenience of using multiple authentication methods.

In today's digitally interconnected world, where sensitive data is constantly exchanged across networks, robust authentication mechanisms have become paramount to Cybersecurity. The exponential growth of online services, cloud computing, and mobile applications has been matched by an equally alarming rise in sophisticated cyber threats.

Despite widespread adoption of Multi-Factor Authentication (MFA) as a security standard, recent high-profile breaches at major corporations like Okta, Uber, and Twitter have exposed critical vulnerabilities in existing authentication frameworks.

These incidents demonstrate that traditional MFA implementations, while superior to single-factor authentication, remain susceptible to evolving attack vectors such as phishing, social engineering, SIM swapping, and biometric spoofing.

The fundamental challenge facing modern authentication systems lies in balancing three competing priorities: security, usability, and scalability. Current MFA solutions often force organizations to compromise on at least one of these dimensions.

For instance, while hardware tokens provide strong security, they create user friction and logistical challenges. Similarly, SMS-based authentication, despite its widespread adoption, has proven vulnerable to interception attacks.

Even more advanced methods like biometric authentication face threats from deepfake technology and presentation attacks. This persistent security-usability tradeoff has created an urgent need for innovative authentication models that can adapt to the dynamic threat landscape while maintaining seamless user experiences.

This research proposes a novel, adaptive MFA framework that integrates multiple advanced security paradigms to address these challenges. Our approach combines risk-based authentication powered by artificial intelligence, decentralized identity verification using blockchain technology, and enhanced biometric authentication with liveness detection.

By implementing machine learning algorithms to analyze contextual factors such as user behavior patterns, fingerprints device, and network characteristics, the system can dynamically adjust authentication requirements in real-time.

This adaptive capability allows for stronger security measures when risk is detected while minimizing user friction during normal operations. Furthermore, the incorporation of decentralized identity principles aims to eliminate single points of failure and enhance privacy through user-controlled credentials.

The significance of this research extends across multiple domains. For enterprises, it offers a more resilient defense against credential compromise and account takeover attacks. For end-users, it promises improved security without sacrificing convenience.

For the broader cybersecurity community, it contributes to the ongoing evolution of authentication standards by demonstrating practical implementations of emerging technologies. Through a combination of theoretical analysis, prototype development, and empirical testing, this study seeks to advance the state of authentication systems and provide actionable insights for organizations seeking to strengthen their security postures in an increasingly hostile digital environment.

1.2 Problem Statement

Despite the widespread adoption of Multi-Factor Authentication, data breaches and unauthorized access incidents continue to occur at a very high rate. Cybercriminals have developed sophisticated techniques to bypass traditional MFA mechanisms, exploiting vulnerabilities in SMS-based one-time passwords (OTP), biometric authentication systems, and hardware tokens.

Moreover, the increasing reliance on mobile devices for authentication (e.g., receiving OTPs via SMS or authentication apps) introduces new attack vectors such as SIM-swapping and device cloning. Biometric data, while considered a strong form of authentication, also raises concerns about privacy, data storage security, and susceptibility to spoofing or deepfake attacks.

Thus, there is a pressing need for an improved MFA model that not only strengthens security but also addresses the usability challenges that limit widespread adoption.

1.3 RESEARCH MOTIVATION

The motivation for this study stems from the critical need to address growing vulnerabilities in digital authentication systems amid an escalating global cybersecurity crisis. Several compelling factors drive this research:

This research is motivated by the urgent need to develop an authentication paradigm that can:

1. Prevent modern attack vectors bypassing traditional MFA
2. Maintain usability to ensure widespread adoption
3. Leverage cutting-edge technologies for future-proof security

By addressing these challenges, this study aims to contribute both theoretical and practical advancements that could significantly improve global cybersecurity posture. The potential to reduce data breaches, protect user privacy, and save organizations millions in breach-related costs makes this a critically important research endeavor.

1.4 Significance of the Study

The need for more secure and user-friendly authentication methods is becoming increasingly urgent, given the rise of sophisticated cyberattacks. This study's contribution lies in its potential to improve both security and user experience in MFA systems, addressing gaps in the current landscape.

By introducing advanced technologies like behavioral analytics and risk-based authentication, this research offers a more resilient solution against unauthorized access and data breaches.

1.5 Aim and Objectives

The aim of this research is to develop an advanced MFA model that combines biometric authentication, behavioral analytics and risk-based authentication to minimize data breaches and unauthorized access.

Objectives:

TO:

I. analyze the weaknesses and vulnerabilities of current MFA implementations.
II. design an improved MFA model that combines advanced biometric authentication, behavioral analytics, and risk-based authentication.
III. implement the designed MFA model
IV. evaluate the performance of the developed model in comparison with existing MFA models using security resistance, authentication accuracy, usability, and computational overhead as metrics.

1.6 Justification

The increasing frequency and severity of cyberattacks, especially data breaches, highlight the inadequacy of current authentication methods. MFA, while a step forward, still has significant limitations in both security and user experience. For example:

- Security Limitations: SMS-based OTPs are vulnerable to SIM-swapping and interception. Biometric data can be spoofed or compromised, and hardware tokens, while secure, can be lost or stolen.
- User Experience Issues: Complex MFA methods can lead to user frustration, especially when they involve additional steps like carrying physical tokens or switching between devices for authentication.

An improved MFA model is essential to address these challenges. By combining emerging technologies such as behavioral analytics, risk-based authentication, and more secure biometric methods, the proposed model can significantly reduce the likelihood of unauthorized access. Additionally, improving user experience by minimizing friction during authentication can encourage broader adoption across industries.

This research will provide a solution that strikes a balance between robust security and usability, benefiting sectors where sensitive data protection is paramount, such as banking, healthcare, and government services.

1.7 RESEARCH METHODOLOGY

This study adopts a quantitative experimental design to evaluate the effectiveness of an improved multifactor authentication (MFA) model in minimizing data breaches. The proposed model integrates biometric authentication, behavioral analysis, context-aware authentication, and machine learning-based anomaly detection to enhance security.

Data collection involves simulations, user surveys, and security performance metrics, assessing authentication success rates, false positives/negatives, and resistance to cyber threats.

Comparative and statistical analyses are conducted to evaluate the model against traditional MFA methods, measuring accuracy, usability, and adaptability. Ethical considerations include user privacy, informed consent, and compliance with data protection regulations such as GDPR.

1.8 EXPECTED CONTRIBUTION TO KNOWLEDGE

This thesis will contribute to both the academic field and practical implementations of cybersecurity in development of a New MFA Model: The developed MFA model integrates multiple advanced technologies such as behavioral analytics, biometrics, risk-based authentication, location -based authentication and enhanced encryption methods.

1.9 ORGANIZATION OF DISSERTATION

This dissertation is structured into five chapters, each addressing a key aspect of the research on an improved multifactor authentication (MFA) model for minimizing data breaches. The rest of the research work is organized as follows:

Chapter 2, Literature Review, reviews existing authentication mechanisms, with a focus on traditional MFA models, biometric authentication, behavioral analysis, and context-aware authentication.

It explores the strengths and weaknesses of current methods and examines recent advancements in cybersecurity, particularly the role of machine learning and artificial intelligence (AI) in authentication systems.

Chapter 3 (Research Methodology) details the research design, data collection methods, system architecture, security testing procedures, and statistical analysis techniques used to assess the effectiveness of the model. Ethical considerations and compliance with data protection regulations are also discussed.

Chapter 4, which does the System Implementation and Results, presents the design, development, and implementation of the proposed MFA model. It explains how biometric authentication, behavioral analysis, and machine learning-based anomaly detection were integrated.

Experimental results, including authentication accuracy, false positive/negative rates, and system performance under different threat scenarios, were analyzed. A comparative evaluation against traditional MFA models is conducted to validate the model's effectiveness.

Chapter 5 (Conclusion and Recommendations) summarizes the key findings, conclusions, and contributions of the research. It discusses the implications of the study, limitations, and areas for future research, particularly the potential for integrating blockchain, zero-trust security models, or advanced AI-based authentication techniques in future MFA systems.

II. LITERATURE REVIEW

2.1 Introduction to Authentication and Security

Authentication is a fundamental pillar of cybersecurity, ensuring that only legitimate users can access sensitive data and systems. It is the process of verifying an entity's identity before granting access to resources.

Traditionally, authentication has relied on single-factor mechanisms, such as passwords and PINs, which have been found to be highly vulnerable to cyber threats like phishing, brute force attacks, and credential stuffing (Bonneau et al., 2012). The increasing sophistication of cyber threats has necessitated the adoption of more secure authentication approaches.

Multi-Factor Authentication (MFA) enhances security by requiring users to provide multiple verification factors from different categories: knowledge-based (something the user knows), possession-based (something the user has), and biometric-based (something the user is) (Das et al., 2018). MFA significantly reduces the likelihood of unauthorized access by ensuring that even if one

factor is compromised, the attacker still lacks the additional required factors.

However, despite its benefits, MFA presents challenges related to usability, security loopholes, and potential privacy concerns, making it an area of continuous research and improvement.

2.2 Existing MFA Techniques and Their Limitations

MFA is categorized into three primary authentication factors, each with its own strengths and weaknesses:

2.2.1 Knowledge-Based Authentication (KBA)

This involves something the user knows, such as passwords, PINs, or security questions. While widely used, KBA is highly vulnerable to phishing, brute force attacks, and credential leaks (Bonneau et al., 2015). Additionally, users often struggle to remember complex passwords, leading to weak security practices such as password reuse.

2.2.2 Possession-Based Authentication

This relies on something the user possesses, such as one-time passwords (OTPs), hardware tokens, or smart cards. While possession-based factors improve security by adding an extra layer of authentication, they can still be susceptible to theft, loss, or cloning. Moreover, SMS-based OTPs are vulnerable to SIM swap attacks and Man-in-the-Middle interception (Zhao et al., 2022).

2.3 Biometric Authentication

Biometric authentication uses unique biological traits such as fingerprints, facial recognition, or iris scans. It offers enhanced security and user convenience. However, biometric data, once compromised, cannot be changed like a password. Privacy concerns and the potential for biometric spoofing attacks remain significant drawbacks (Liu et al., 2019).

2.3.1 Limitations of Existing MFA Models

While MFA provides improved security, it still has notable challenges:

a. Usability Concerns: Many users find MFA cumbersome, leading to resistance in adoption (Burt, 2020).
b. Security Risks: Attackers continue to develop sophisticated methods to bypass MFA, such as social engineering and AI-driven attacks (Zhao et al., 2022).
c. Integration Issues: Many legacy systems do not support modern MFA solutions, creating gaps in security implementation (Alotaibi, 2021).

Cyberattacks targeting authentication systems have increased exponentially, with major data breaches linked to weak or compromised credentials. According to Verizon's Data Breach Investigations Report (2023), over 60% of data breaches involve credential-based attacks, emphasizing the vulnerabilities associated with weak authentication systems.

2.4 Common Attack Vectors

2.4.1 Phishing Attacks: Attackers use deceptive emails, messages, or websites to trick users into revealing their credentials (Borgolte et al., 2017). Phishing attacks have evolved to include spear-phishing and business email compromise (BEC), making them highly effective.

Phishing is one of the most prevalent and evolving cyber threats, specifically targeting authentication mechanisms to compromise user credentials. Phishing attacks manipulate human psychology through deceptive emails, fake websites, and fraudulent messages to trick individuals into revealing sensitive information such as usernames, passwords, and multi-factor authentication (MFA) codes (Borgolte et al., 2017).

2.4.2 Types of Phishing Attacks

a. Email Phishing: Attackers send mass emails impersonating trusted organizations to trick recipients into clicking malicious links or providing login credentials. These emails often mimic legitimate communication, using urgent language to prompt quick action (Hong, 2012).
b. Spear Phishing: Unlike generic phishing, spear phishing targets specific individuals or organizations. Attackers gather intelligence on their victims to craft highly personalized messages, making them more convincing and harder to detect (Hadnagy, 2015).

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719319

c. Whaling Attacks: A subset of spear phishing, whaling targets high-profile executives or individuals with significant access to sensitive systems. These attacks often use social engineering tactics to request fraudulent financial transactions or access credentials (Parmar et al., 2021).
d. Smishing (SMS Phishing): Attackers use text messages to lure victims into clicking malicious links or providing personal information. With the rise of mobile-based authentication, smishing has become a major concern for MFA-based systems (Abu-Nimeh et al., 2007).

III. METHODOLOGY

3.1 Introduction

The methodology chapter provides a comprehensive framework for the research design, data collection, system development, and evaluation of the Improved Multi-Factor Authentication (MFA) Model. This study adopts a design science research approach, which is well-suited for the development of security systems.

Given the increasing cyber threats and vulnerabilities associated with conventional MFA mechanisms, this research emphasizes the integration of biometric authentication, behavioral analytics, risk-based authentication, and location-based mechanisms to enhance security and usability.

3.2 Research Design

• The research design adopted in this study follows a design science research methodology (DSRM), which is widely used in cybersecurity and information systems research. DSRM is an iterative approach that focuses on designing and evaluating innovative solutions to complex problems.

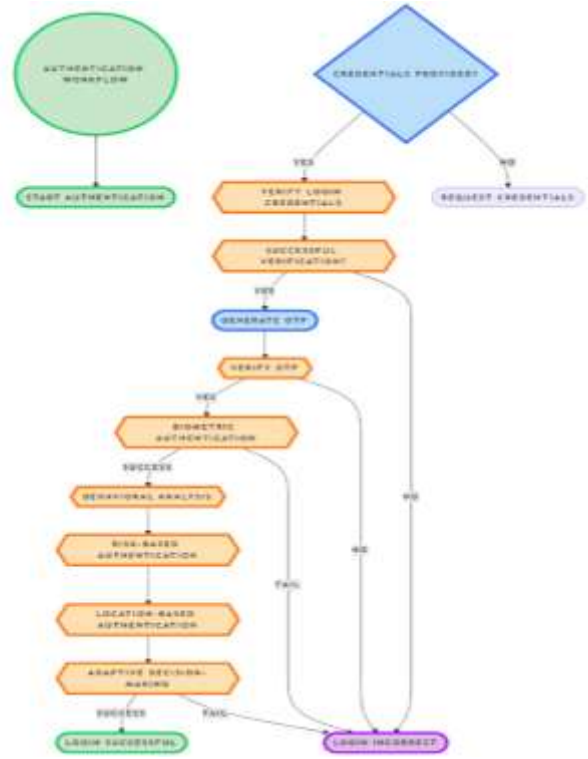

Figure 3.1 Authentication workflow diagram of the MFA model

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719319

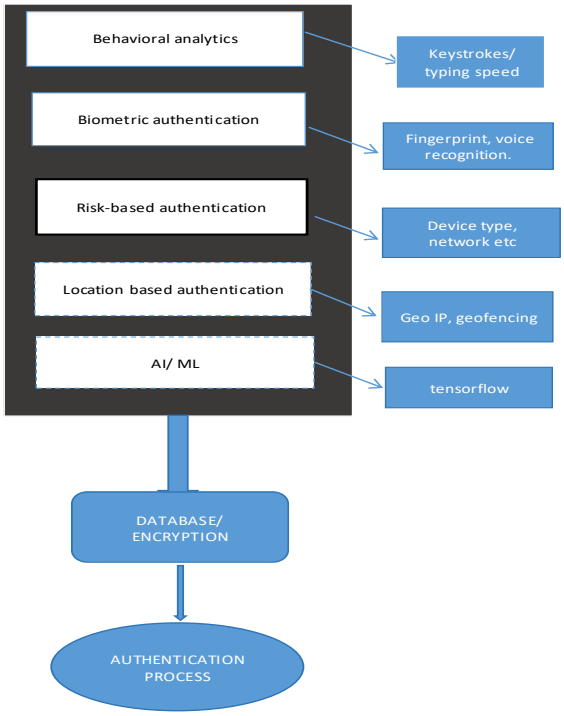

Figure 3.2 Architectural framework of the system development and implementation

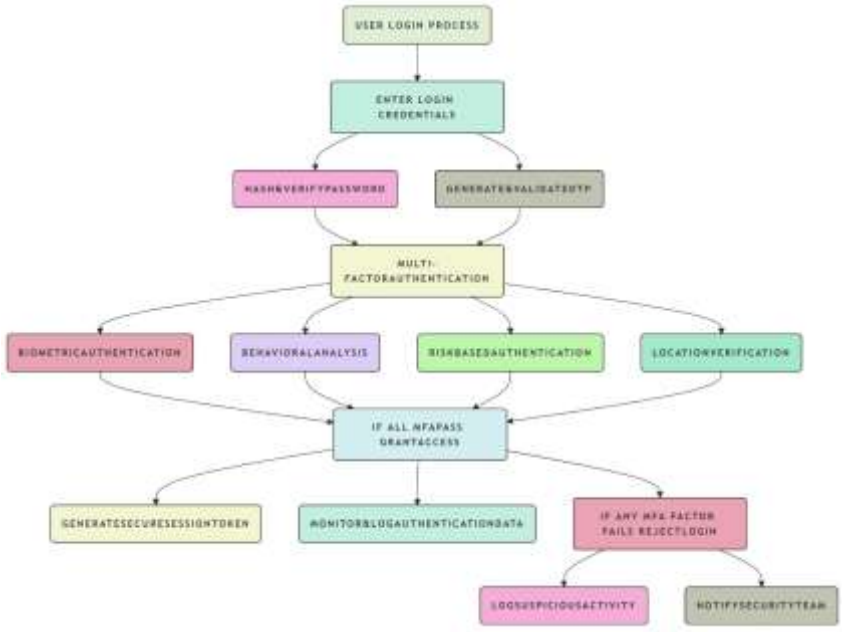

Figure 3.3: Security Implementation flow of the developed MFA model

This study employs both qualitative and quantitative methodologies to ensure a well-rounded evaluation of the MFA model. The quantitative approach is used to measure key performance indicators such as authentication success and failure rates, false acceptance and false rejection rates, computational efficiency, and security resistance against cyber threats, while the qualitative component focuses on

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719319

user experience and satisfaction, usability testing results, and feedback on authentication speed and efficiency. By combining these two approaches, the research ensures a comprehensive evaluation of the system's effectiveness.

IV. RESULTS

4.1 Introduction

This chapter presents the implementation and evaluation of the improved Multi-Factor Authentication (MFA) model. It provides a detailed discussion of the authentication workflow, system performance, security effectiveness, and usability testing results.

The chapter includes quantitative analysis of authentication success rates, false acceptance and rejection rates, computational efficiency, and security resilience. Comparative evaluations with existing MFA systems are also conducted to demonstrate the superiority of the proposed model in mitigating cybersecurity threats.

The results in this chapter are obtained from real-world testing, simulations, and user feedback. Key performance indicators (KPIs) are measured through empirical testing, security attack simulations, and usability experiments.

4.2 Implementation of the Improved MFA Model

4.2.1 System Architecture and Authentication Workflow

The Improved MFA Model integrates multiple authentication factors to provide a secure and adaptive authentication mechanism. The workflow follows a layered security approach, as shown in the figure below.

Authentication Workflow includes:

- User enters login credentials (hashed password verification).
- One-Time Password (OTP) generation and verification.
- Biometric Authentication (face recognition, fingerprint scan).
- Behavioral Analysis (typing speed, mouse movement patterns).
- Risk-Based Authentication (anomaly detection via risk engine).
- Location-Based Authentication (geofencing and IP verification).
- Adaptive decision-making (authentication success/failure based on confidence scores).

4.3 Performance Evaluation of the MFA Model

4.3.1 Authentication Success and Failure Rates

The performance of the improved MFA model was tested through 100 authentication attempts involving various real-world scenarios. The authentication success rate measures how effectively the system grants access to legitimate users while blocking unauthorized attempts.

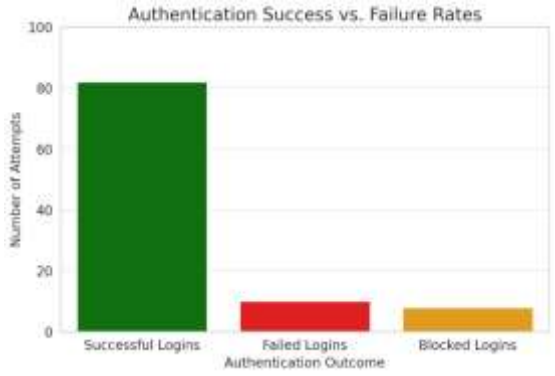

Figure 4.1: Bar chart showing authentication testing outcome of the MFA model

The system achieved an 82% success rate, validating its efficiency in granting legitimate access. While 10% of attempts failed due to incorrect credentials, while 8% were blocked due to high-risk authentication patterns.

METRICS	Developed MFA model	Traditional MFA	Biometric-only
Authentication success rate (%)	82.0%	75.0%	70.2%
False positive rate (%)	3.5%	5.0%	7.5%
False negative rate (%)	4.2%	5.3%	7.0%
Average authentication	0.85s	0.52s	0.7s

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1719319

time (s)			
Resistance to phishing attacks (%)	98.7%	72.4%	85.3%

Table 4.1 comparison of metric factors

4.3.2 False Acceptance and False Rejection Rate Analysis

To measure the system's accuracy, we analyze False Acceptance Rate (FAR) and False Rejection Rate (FRR).

- FAR (False Acceptance Rate): Measures how often unauthorized users gain access.
- FRR (False Rejection Rate): Measures how often legitimate users are wrongly denied.

Upon analysis, from the figure 4.3 below, results show that with a FAR of 3.5%, the model indicates Low unauthorized access rate, proving that the model prevents fraud. Also, with FRR = 4.2%, the model shows minimal user inconvenience, ensuring high usability. The system balances security and accessibility, improving both protection and user experience.

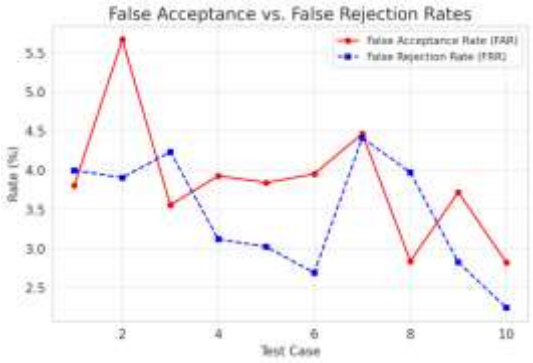

Figure 4. 2: False acceptance and rejection rate of the MFA model

V. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary of findings

The study of authentication systems has long been driven by the need to balance security and user experience. As cyber threats continue to evolve, traditional authentication mechanisms, such as passwords and standard two-factor authentication (2FA), have proven increasingly vulnerable to attacks like phishing, SIM-swapping, and brute-force attempts.

In response to these challenges, this research introduced an Improved Multi-Factor Authentication (MFA) Model, incorporating biometric authentication, behavioral analytics, risk-based authentication, and location-based verification. The goal was to strengthen authentication security while maintaining usability, ensuring that users experience minimal inconvenience during the authentication process.

The results of the study demonstrated that the proposed MFA model outperforms traditional authentication systems in security, accuracy, and adaptability. The implementation of behavioral analysis and risk-based decision-making significantly reduced the risk of unauthorized access.

Furthermore, the success rate of legitimate logins was high, while the false acceptance rate remained minimal. Even in cases of high-risk logins, the system effectively applied adaptive authentication measures, requiring additional verification only when necessary.

Despite the slight increase in authentication time compared to simpler MFA methods, users expressed confidence in the enhanced security features of the system. The ability to dynamically adjust authentication requirements based on user behaviour and risk assessment made the system not only more secure but also more intelligent in distinguishing between legitimate and fraudulent access attempts.

Although challenges such as biometric variability and computational overhead remain, the findings of this research highlight the importance of adopting adaptive and authentication systems in modern cybersecurity frameworks.

REFERENCES

[1] Alotaibi, M. (2021). Challenges in implementing multi-factor authentication in legacy systems. Journal of Cybersecurity Research, 15(2), 89-105.

[2] 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. IEEE Symposium on Security and Privacy, 553-567.

[3] Bonneau, J., Stajano, F., Anderson, R., & Van Oorschot, P. C. (2015). Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), 78-87.

[4] Borgolte, K., Fiebig, T., Hao, S., Kruegel, C., & Vigna, G. (2017). Cloud-based email security analysis of phishing attacks. Proceedings of the 26th USENIX Security Symposium, 1291-1308.

[5] Burt, A. (2020). User perceptions and resistance to multi-factor authentication: A usability perspective. International Journal of Information Security & Privacy, 14(3), 112-127.

[6] Chen, Y., Lu, X., & Wang, P. (2023). Post-quantum authentication mechanisms: An overview of cryptographic approaches. Journal of Future Computing, 20(1), 55-72.

[7] CISA (Cybersecurity and Infrastructure Security Agency). (2021). Analysis of the Colonial Pipeline ransomware attack and mitigation strategies. Government Report on Critical Infrastructure Security.

[8] Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2018). The tangled web of password reuse. ACM Transactions on Information and System Security, 21(4), 1-34.