The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 3, June 2025
https://doi.org/10.33022/ijcs.v14i3.4830

Five-Factor Authentication System with a Track and Trace Capability for Online Banking Platforms

Glen Lehlohonolo Moepi[1], Topside Ehleketani Mathonsi[2]
MoepiGL@tut.ac.za[1], MathonsiTE@tut.ac.za[2]
[1,2] Department of Information Technology, Tshwane University of Technology, South Africa.

Article Information

Received : 3 Apr 2025
Revised : 30 Apr 2025
Accepted : 9 Jun 2025

Keywords

Security, Multi-Factor Authentication, Online Banking, Biometrics, Vulnerability

Abstract

Online banking is a rapidly growing customer service platform, but increasing cyber threats require constant security improvements. This study developed an enhanced Multi-Factor Authentication (MFA) scheme with track-and-trace capabilities to mitigate risks. The proposed system includes five authentication modalities: username, password, PIN, OTP, biometrics (fingerprint or facial scan), registered smart devices, and a time-locked user location. Its ability to detect suspicious activities and send alerts via secretly obtained photos and location triangulation is a significant feature. Using design science methodology, three prototype schemes were developed and compared with First National Bank (FNB) and Standard Bank (STD) security systems. Evaluated with Datadog and AppDynamics APM tools, the best prototype achieved 80% security, slightly below FNB and STD's 90%. It matched them in resource efficiency and outperformed them in response time, averaging 500 milliseconds compared to FNB's 700 ms and STD's 1000 ms.

A. Introduction

Online banking has become an integral part of modern finance, with customers relying on it for convenient transactions. However, this convenience has also attracted a surge in online attacks [1][2]. While most banks employ Two-Factor Authentication (2FA), such as mobile codes alongside usernames and passwords, these strategies are no longer enough to combat evolving threats [2]. The need for a more robust solution is evident. This study addresses the problem of increasing online attacks by proposing an enhanced Five-Factor Authentication (5FA) system with a built-in track and trace feature as a solution. The proposed Multi-Factor Authentication (MFA) adds additional layers of protection by combining traditional authentication techniques, biometrics, device-specific ID, and geolocation [3][4].

This research employed a quantitative approach, using literature reviews and prototyping [5]. The aim was to develop an enhanced MFA system for online banking without compromising the user experience [3][6], thus setting the stage for future research in the authentication domain [7][8]. The proposed 5FA system aims to improve online banking security while providing an excellent user experience, contributing to Information Security (IS) and Human-Computer Interface (HCI) fields.

B. Research Method

Related work

The Internet of Things (IoT) unleashed a new wave of online service deliveries. This revolutionized how institutions offered services to their customers. More services have been migrated to online platforms. This development of online services increased the probability of attacks on user information. Credentials harvesting through phishing, identity thefts, interception of network communication devices, and many other deceptive Social Engineering (SE) media attacks are on the rise [9]. The banking industry is constantly looking for novel approaches that are efficient at fending off online threats, user-friendly, simple to deploy, monitor, and manage, and don't adversely influence the Quality of Service (QoS) delivery to keep one step ahead of cyberattacks. Identification of authorized and unauthorized users is accomplished using authentication [10]. Users can be protected against assaults by using authentication techniques properly. A user-friendly and secure form of authentication is necessary for an online business to be successful. The study concluded that there has been little research on the benefits of usable security and the evaluation of user authentication techniques. The lack of these authentication studies negatively impacts the user's convenience and the purpose of the authentication process. The usability and security of MFA methods were explored in a study by [11]. The study's primary focus was on user viewpoints essential to the deployment and authentication processes. The goal of this study is to provide a better, secure online banking platform while keeping in mind how important it is to provide consumers with a platform and interface that are simple to use.

The study by [11] observed an increase in the usage of online banking services. Most banks deployed a range of MFA systems to provide consumers with security. The different MFA designs and features offered a non-homogeneous level of security

and user experience. The study evaluated the MFA design decisions adopted by the thirty banks operating in other countries. Following that, the study assessed the implemented MFA systems for complexity, security robustness, compliance with the legislation, and best practices. Although most banks chose to use MFA to boost online banking security, the level of security was not as good as anticipated. In conclusion, [11] painted a grim outlook on information security. Half of the banks have adopted at least one authentication factor. According to this study, security is an empirical cornerstone of online banking services. Hence, it is proposed that at least three criteria should be used to build a strong protocol for online banking transactions.

A study by [12] proposed an authentication system that enables people to register multiple devices. These devices can either be physical or virtual. The authentication scheme provided flexibility; users can choose any registered device for the online authentication. The user does not need to create or remember credentials, thus mitigating the risks associated with username and password combinations. However, the scheme mainly focused on user flexibility rather than stronger security for online transactions. Using multiple registered devices increased the attack surface for online transactions. If user devices are stolen or lost, user access and authentication may be jeopardized. The proposed MFA will only allow users to register a maximum of three smart devices. This will allow the user device flexibility while balancing access and security.

A study by [13] and [14] highlighted the essence of authentication using human behaviour. The study centred on the necessity for implementing strong authentication schemes. Through the expedition on the authentication challenges on security and efficiency, they noted that most existing studies do not detect weaknesses based on user behaviour. The focus of [13] proposed an MFA that can withstand attacks, based on the user behaviour, and maintain optimum efficiency. According to [13], despite the additional security measures, the MFA scheme's experiment findings indicated that its processing time was shorter than those of popular MFA schemes. The scheme used a combination of the user biometric matching procedure and the attack recognition technique to authenticate users. The attack recognition technique could predict the impostor's actions and offer a solution based on those actions. The system provided increased security. The majority of current authentication methods ignore the value of user-centric controls. This study incorporates biometrics and user behaviour as necessary authentication variables because it recognizes the significance of innate and inherent user features.

According to [15], the systems are easily attacked when users access services. Their research proposed employing a smart card with elliptic curve cryptography (ECC) to perform Three-Factor Authentication (3FA) for remote user authentication. AVISPA and Proverif were used to simulate the system, and the simulation showed that it was secure against both active and passive attacks. Furthermore, the authentication technique performed better in defence against attacks, in terms of effectiveness, computing cost, and security characteristics, than the other existing schemes. However, the program provided a way to cancel a user's smart card that had been lost or stolen. This study aims to replace physical tokens, which are vulnerable to theft and can be lost by the user. Security vulnerabilities

have increased since tangible tokens like smart cards are not password-secured. This study will use registered security-protected devices enforced with biometric user recognition features to provide strong multimodal authentication without using tokens. The authors [16] researched popular authentication strategies for online banking services. The study's objective was to identify and comprehend the widely used authentication methods to propose a more sensible mix of authentication methods. The authors [16] concluded that fingerprint authentication is the most secure and user-friendly method. However, the study allowed the user to use any of the three available authentication factors. The main goal of the choice was to make things easier for the user. The MFA highlighted some gaps, where it was determined that the card reader was the weakest link. A compromised user profile could result from a user misplacing it or in the event of theft. The study is identical to this proposed scientific design study in many ways, except for a card reader system or user option. The proposed innate and inherent five factors are interconnected to provide impenetrable security.

This research aims to improve MFA with integrated track and trace functionality for user authentication on online banking platforms. In this study, the effectiveness, qualities, risk exposure, and often utilized vectors in well-known online banking platforms were qualitatively assessed. Additionally, the created MFA scheme was contrasted with well-known authentication techniques. Several of these established schemes use fewer modalities than the proposed MFA. The proposed MFA groups five modalities to fill the gaps that have been identified. In the present literature evaluations, none of the authentication schemes exploited five modalities simultaneously or provided track and trace functionality. Once more, the static nature of the modalities utilized makes some authentication schemes more vulnerable to being easily bridged. The five factors were the login, PIN, OTP, facial and fingerprint biometrics, registered device, and time-based location.

Proposed Solution

This study proposed an enhanced 5FA system for online banking platforms with a track-and-trace feature. As illustrated in Figure 1, the authentication flow procedure starts in stage one, and the user registration begins with this step. At this critical stage, user profiles are created and stored in the online services database. The primary user identity is a thirteen-digit Identity Number. The system uses the traditional user ID along with a pre-determined four-digit PIN or password. The complexity policy requirements for both the PIN and the password must be met.
The MFA moves to Stage two if the User ID and the correct password or PIN match. The user only has three chances to type in the correct PIN or password. If all three attempts are incorrectly matched, the system blocks the user and stops future authentication steps. The customer must alert the bank and reactivate their profiles to avoid the information being compromised in this situation. To move on to stage two, stage one must be successful. An OTP is required for this verification level; it is produced randomly by an online system and sent to the client's registered mobile number. The customer will then confirm their account information by entering their OTP on the online banking platform. These entries will be compared, and the additional authentication will be approved.

The third authentication stage is launched as soon as stage two authentication is completed. The customer will use a fingerprint or facial scan that was obtained and saved at the initial registration of their profile to authenticate it at this point. The proposed system would move to stage four if the client's biometrics were appropriately validated and linked to the user profile. This stage involves processing an investigation into the registered device using the abstraction of various MAC addresses. The consumer may utilize three devices to do business on the web platform. Another crucial element of the suggested method is device authentication. The devices that can access the client's profile are so restricted.

The MFA scheme moves to stage five after the device is confirmed. This is the last stage of the proposed plan. The scheme will actively verify the user's location after the earlier stages have been completed to ensure that the transactions are done within the pre-set or preferred radius and within the allotted time frames. The system will leverage the user's flexible behaviour to verify their identity. The security of user profiles is enhanced using GPS, geo-fencing technology, and time limits. Verified users will only be allowed to perform transactions under this enhanced 5FA on registered devices, in their desired locations, and during their chosen time frames, as shown in the flowchart in Figure 1 below.

Digital security is based on intricate computations that control various authentication techniques. The precise mathematical procedures that underpin each strategy to protect user data and privacy are explored in this section. Calculations employ multiple methods, including cryptographic hashing, comparing usernames, validating Personal Identification Numbers (PINS), and creating One-Time Pins (OTPS). Additionally, complex mathematical modelling is used in biometric authentication to compare recorded templates with live fingerprint or face feature scans. Geolocation-based verification uses sophisticated algorithms to check that user-declared locations correspond to actual data. Lastly, secure communication protocols, device profiling, and encryption computations are all necessary for smart device authentication. These calculations are at the core of authentication, contributing to digital security and user trust. PINS and OTPS calculations are based on the communication between the client and the server, ensuring the safe administration and verification of PINS supplied by users.

1. PIN Storage

Equation 1 explains how to secure the Application PIN. The bidirectional arrow ($\Leftrightarrow$) signifies the mutual interaction, where the client (C) offers their PIN [$k1$] for authentication, and the server (S) safely retains the user's secret parameter string.

$$S[SK_1] \Leftrightarrow C[k_1] , \qquad \text{equation} \qquad (1)$$

Therefore $S[SK_1] \rightarrow Data_1$, let $Data_1$ be the data generated by S at this step.

The client's PIN, $C[k_1]$ will be stored in a secret compartment parameter string within the server, $S[SK_1]$. This process will be to prompt the client,C to create an initial PIN

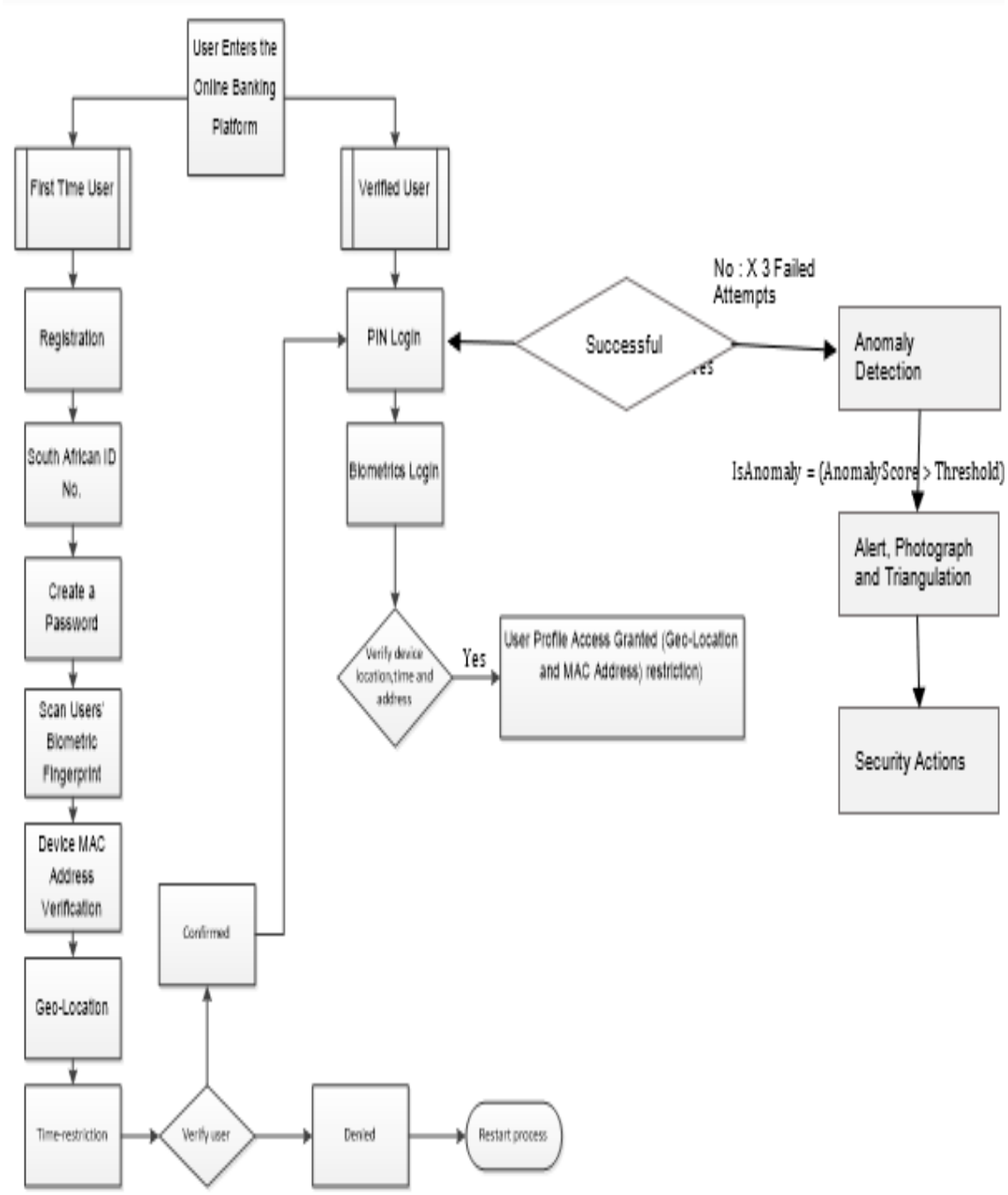

Figure 1. The Adaptive MFA Flow Chart.

Moving to biometric authentication, the core of this method is feature extraction and facial data classification. Fisher's Linear Discriminant (FLD) method extracts pertinent facial data to optimise the ratio between inter-class and intra-class scatter matrices. This process results in feature vectors, enhancing data separability.

2. Fisher's Linear Discriminant Function J

$$J(w) = \frac{W^T S_B W}{W^T S_W W} \quad \text{equation} \quad (2)$$

Equation 2 represents Fisher's linear discriminant function J. It optimizes the contrast between within- and between-class variations. Better class separability, essential for classification and pattern recognition tasks, correlates with a higher J value.

3. Fingerprint Extraction- Genetic Bio Data

$$j = Gen(BioData) \rightarrow (R, P) \quad \text{equation} \quad (3)$$

The implementation of biometric authentication involves the use of fuzzy extractors. When a client inputs their fingerprint, a pair (R, P) is generated using the client's biometric template and the Gen algorithm within the fuzzy extractor. Equation 3 shows the conversion of genetic bio data into (R, P), where Gen processes the client's biometric data, creating an essential computational array.

Additionally, geolocation-based verification necessitates calculations for the secure handling of user-declared locations. Equation 4 shows the storage of a client's restriction location (C[r]) in the server's secret compartment parameter string$S[SK_6]$. The server decrypts this location using a random value and checks for authentication, thus ensuring the user's authenticity.

4. Fingerprint Extraction- Genetic Bio Data

$$S[SK_6] \Leftrightarrow C[r] \text{ , therefore} S[SK_6] \rightarrow Data_6, \quad \text{equation} \quad (4)$$

These calculations highlight the complex procedures that strengthen digital security, permitting various forms of authentication while protecting the integrity and privacy of user data. Figure 2 mathematically represents all the steps to implement the enhanced 5FA scheme. Each stage encapsulates the functions each factor in the proposed scheme has to play.

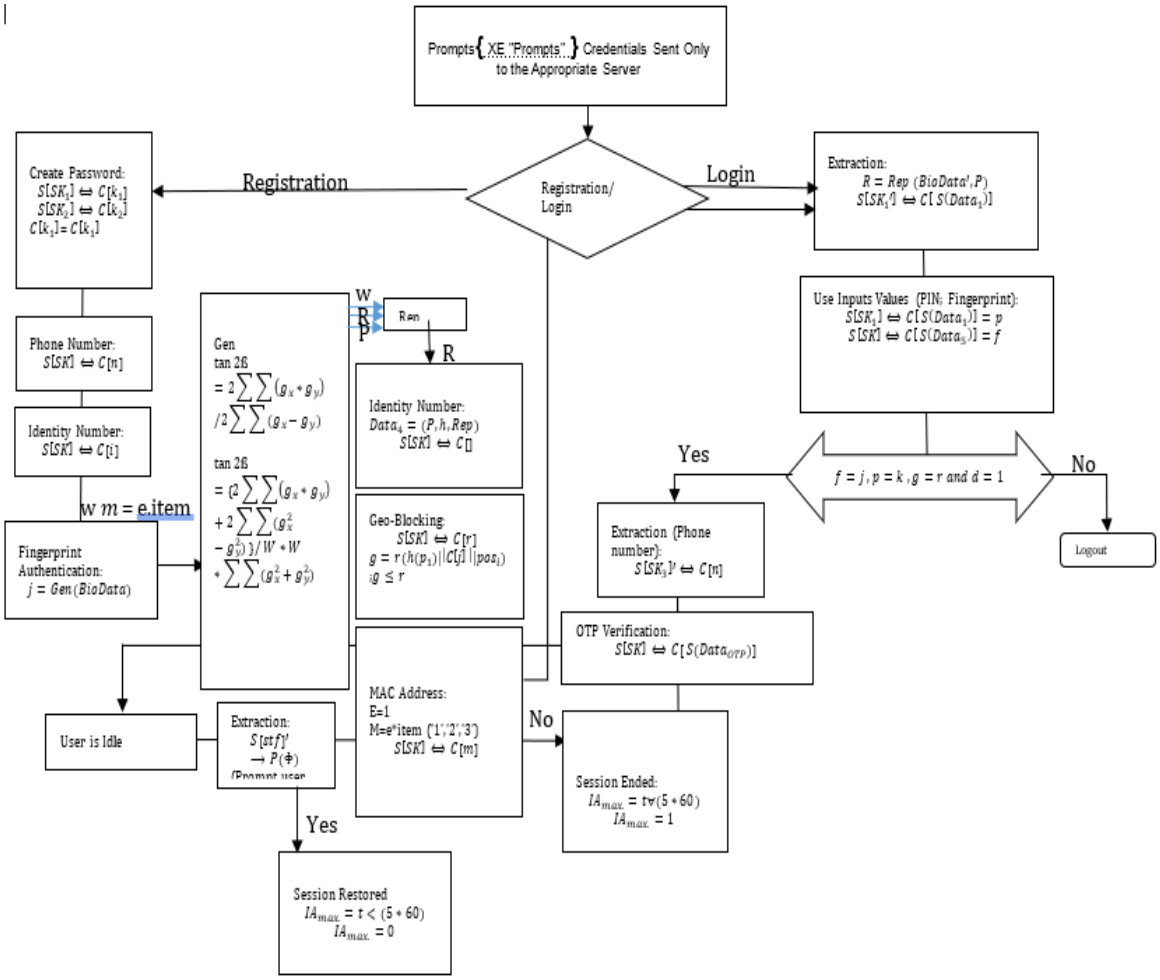

Figure 2. Enhanced 5FA Algorithm Mathematical Flow Model.

Enhancing Security: Image capturing is an advanced security measure beyond traditional measures.

5. Security Constraints

The image capturing mechanism enhances security and user verification in MFA systems. This feature is primarily employed when certain security conditions are not met, such as incorrect login credentials (password/PIN) or when a user attempts to access their account outside of preset geographical boundaries. Here, we will discuss the significance and implementation of image capturing in such scenarios:
Login credentials. It provides an additional layer of verification by capturing an image of the user during specific events, such as failed login attempts or access from unusual locations. This image is valuable for subsequent analysis and verification.

- Failed Login Attempts: When a user repeatedly enters incorrect login credentials (e.g., password or PIN), it may indicate a potential security breach. After a predefined number of failed attempts, the system triggers image capturing. This allows the system to capture the image of the

individual trying to access the account, providing visual evidence that can be used for verification and security analysis.

- Geo-fencing: a common technique for restricting user access based on geographical location. If a user tries to access their account from outside the preset boundaries, image capturing is initiated. This ensures that unauthorized access attempts are documented with visual evidence.
- Forensic Analysis: The captured images are valuable forensic evidence in a security incident. If a security breach occurs or a user disputes unauthorized access, these images can be reviewed to verify the identity of the person attempting to access the account.
- Mobile Device Camera: Necessitates image storage, retrieval, and secure transmission, which can pose technical challenges.
- Implementation Challenges: Effective image capturing requires advanced technology, including cameras or mobile device cameras. It also necessitates image storage, retrieval, and secure transmission, which can pose technical challenges.
- Legal and Ethical Considerations: Image-capturing technology used for security must comply with legal and ethical standards. This includes adhering to privacy laws, ensuring data protection, and securing the stored images from unauthorized access.

In summary, image capturing is a powerful security feature in MFA systems that can strengthen user verification and enhance security. It is a valuable tool for documenting security incidents, monitoring failed login attempts, and enforcing geo-fencing restrictions. However, its implementation should be accompanied by clear communication with users and adherence to privacy and legal regulations to ensure it is used ethically and responsibly.

Moving on to the session timeout. Session timeout is critical to web and application security and user management. It refers to the automatic termination of a user's session within a web or mobile application after a specified period of inactivity. This feature is essential for several reasons:

Security Enhancement: Session timeout is a fundamental security measure that helps protect user accounts from unauthorized access, especially when users forget to log out after their session. By automatically logging users out after a period of inactivity, it reduces the risk of unauthorized access if a user leaves their device unattended.

Protection against Unauthorized Use: If a user forgets to log out or closes the application without logging out, their session may remain active. In such cases, an unauthorized user could access the user's account, leading to security breaches. Session timeout mitigates this risk by ending the session and requiring re-authentication.

Application Performance: Session timeout can also help efficiently use server resources. It prevents idle sessions from consuming server resources, which is especially important for applications with a large user base.

Experimentation

Three prototypes were developed: Prototype A, a mobile App built on the Android Studio platform; Prototype B, a web-based application built on the Visual Studio platform; and Prototype C, a mobile App built on the FlutterFlow platform, as shown in Figures 3, 4, and 5.

Figure 3. 5FA Scheme Prototype A

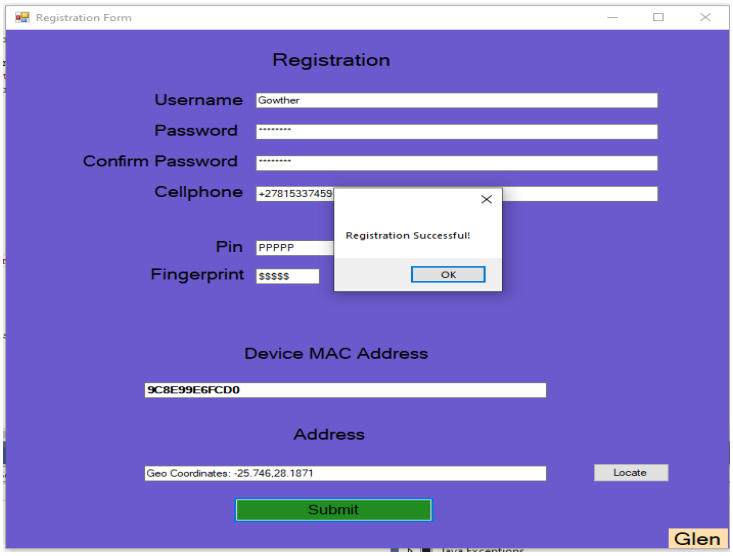

Figure 4. 5FA Scheme Prototype B

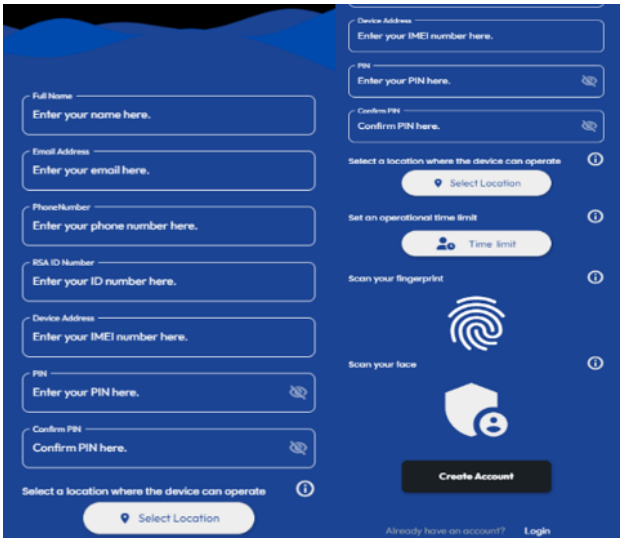

Figure 5. 5FA Scheme Prototype C

The study aimed to uncover the strengths and weaknesses of each MFA prototype by simulating a hypothetical scenario with a thousand concurrent users for each app. The comprehensive evaluation of Prototypes A, B, and C, alongside their respective features and functionalities, offers insights into their performance, security, and usability. These evaluations shed light on the strengths and areas that require improvement in each prototype.

Prototype A, as shown in Figure 3, incorporated robust security features that included Geo-restriction, PIN, fingerprint extraction, MAC-address restriction, and OTP for enhanced user authentication and access control. While it successfully integrated multi-factor authentication and access restrictions, further refinement is possible to optimize its performance and user experience.

Prototype B, shown in Figure 4, introduced web-based functionality. It inherited security features from Prototype A, improving overall security. However, it was resource-intensive, and performance issues were identified, needing minor improvements. Nonetheless, it demonstrated adequate security.

Prototype C, shown in Figure 5, represents an amalgamation of features from Prototypes A and B. It introduced novel features like session time-out and intruder image capturing capability.

In summary, these evaluations served as a foundation for iterative improvements and optimization, emphasizing a dedication to safeguarding user data and enhancing user experience. These prototypes exhibited a commendable security rating, offering distinct advantages and areas for enhancement. Furthermore, adherence to ISO/IEC 29119 standards underscores the importance of universally recognized software testing principles, ensuring software quality and user confidence. This provides a comprehensive understanding of the prototype's strengths and areas requiring future refinement. Thus, contributing to the ongoing commitment to deliver robust and secure MFA Applications.

Experimental Evaluations

The three App prototypes were subjected to rigorous testing alongside the well-established FNB and STDB Apps. The goal was to gauge their performance in a simulated scenario where 1000 users concurrently engaged with each App. This study used Datadog and AppDynamics Application Performance Monitoring (APM), renowned cutting-edge tools for measuring online application platforms, to evaluate performance metrics.

The in-depth evaluation was conducted using AppDynamics and Datadog. These APM tools afforded a unique perspective on the applications' performance. AppDynamics is a prominent member of the Cisco suite. It seamlessly integrated extensive Application APM capabilities, allowing for an in-depth analysis of applications at the code execution level. The platform facilitated the measurement of end-to-end business transaction performance and monitored the health of individual application and infrastructure nodes. It also automatically discovered application topology, providing insights into dependencies and interactions.

The Datadog tool emerged as a powerful ally in our quest for performance insights. This Software-as-a-Service (SaaS) observability platform offered a comprehensive suite of APM capabilities. Its advanced features included distributed tracing, providing an end-to-end view of the application ecosystem. By correlating distributed traces with front-end and back-end data, Datadog APM enabled us to monitor the health metrics, identify service dependencies, and reduce latency, thereby eliminating errors and enhancing overall application performance.

The Key Performance Indicators (KPIs) included average throughput, response time, resource utilization, and security. Other metrics included load time, crash reports, and device information (such as screen resolution and Operating Systems. These measurements were critical for controlling the applications' technical performance and expediting the testing procedure. The goal was to provide a secure and seamless user experience while following industry benchmarks and best practices, eventually prioritising MFA performance and quality of service.

C. Result and Discussion

Throughput and Response Time

Throughput is the quantity of information units a system can handle in a specific period. It is the total period for the central processing unit (CPU), memory, encryption, and decryption to complete requests. Throughput is used in Information System Ecosystems to measure the performance of different computer components and network systems. It assists with the APM metrics and how customers relate to websites and applications. The overall Throughput performance graph is presented in Figure 6.

The overall throughput of the FNB and STDB Apps was higher than that of the App prototypes. FNB had a higher throughput of 1850 TPM, followed by STDB with 1750 TPM. However, Prototype C continued to perform well, showing considerable throughput gains above Prototypes A and B; it measured a throughput of 1000 TPM. Through this comparison, we determined the relative effectiveness of each App in handling user transactions. This gave the study useful information for further investigation and decision-making to improve their overall performance.

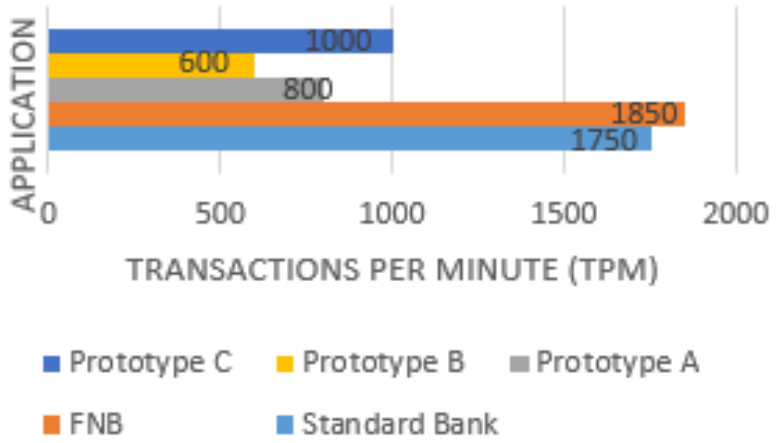

Figure 6. Average Throughput Data Bar Graph.

Prototype C (300 milliseconds) stood out as the best App with the lowest average response time, indicating its excellent efficiency in handling user interactions. Prototype A (500 milliseconds) and Prototype B (800 milliseconds) fell within a mid-range response time, while the STDB App (1000 milliseconds) disappointed with the longest average response time, as shown in Figure 7. It's important to note that the response time is a critical performance metric, as it directly impacts user experience and satisfaction.

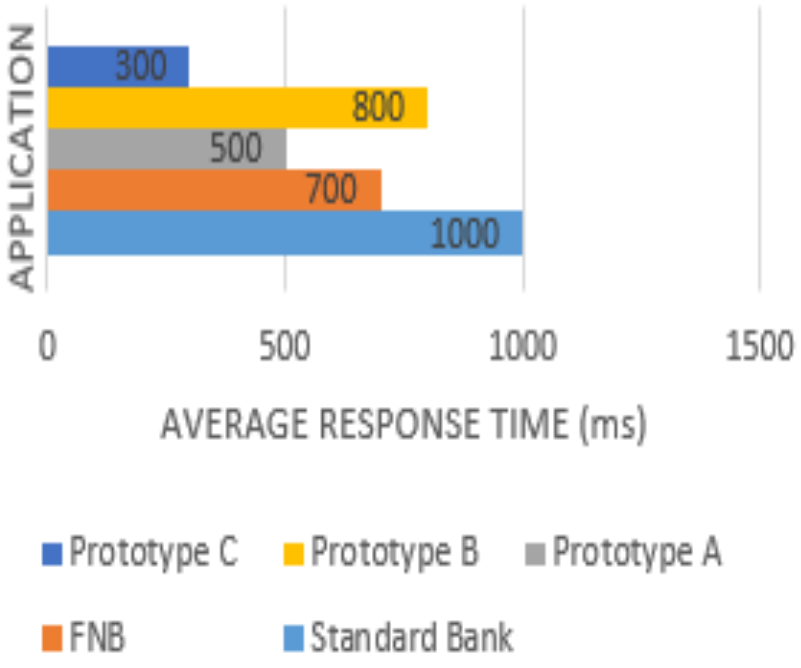

Figure 7. Average Response Time Data Bar Graph.

B. Security and Resource Utilization

Security is essential in safeguarding sensitive data, maintaining user trust, complying with legal requirements, preventing fraud and cyber-attacks, minimizing financial loss, protecting the institution's reputation, and staying resilient against evolving threats. The FNB (9) and the STDB (9) Apps boasted the strictest security posture. They were shortly followed by Prototype C, which had a strong security rating of 8. Prototypes A (7) and B (6) proved adequate security.

Prototype C demonstrated the most efficient resource utilization, earning a rating of 8. This exceptional performance could be attributed to its effective resource optimization strategies, ensuring smooth operation and minimal resource wastage. It stood out as a top performer among the App prototypes. The STDB and the FNB Apps followed closely behind, both of which achieved resource utilisation ratings of 9. These banking Apps excelled in managing system resources, emphasising high performance and responsiveness to user interactions. Their superior resource optimization contributed significantly to their overall efficiency. Table 1 summarizes the overall result.

Table 1. Summary of Experimental Apps Evaluation.

Metric	Prototype A	Prototype B	Prototype C	STD Bank App	FNB BankApp
Throughput (TPM)	800	100	1000	1750	1850
Response Time (ms)	500	800	300	1000	700
Security Rating	7	6	8	9	9
Resource Utilization Rating	7	6	8	9	9
Speed Rating	5	4	7	8	9

Despite the innovative strides made by prototypes in MFA applications, it is crucial to recognize that these solutions are not devoid of limitations, as seen in Table 2. These limitations shed light on areas that warrant further investigation and refinement to ensure the effectiveness of the MFA applications.

Table 2. Limitations of Prototypes in MFA App Development.

Prototype A	Prototype B	Prototype C
1. False Positives and Negatives	1. Scalability Challenges	1. Sophisticated Attacks
2. Network Latency and Performance Impact	2. Web-Based Vulnerabilities	2. False Positives and Negatives
3. Device Co-Compatibility and	3. Browser Compatibility	3. Continual Monitoring and Enhancement

System Requirements		
4. Privacy Concerns	4. Network Latency and Performance Impact	4. Ongoing Refinement and Fine-Tuning
5. Evolving Cyber Threats	5. Biometric Authentication Challenges	
6. Administrative Overhead	6. User Acceptance and Training	
	7. Overhead on Server Resources	

To address these limitations, continuous research, collaboration with cybersecurity experts, regular updates, and leveraging advanced technologies, including AI and ML, will be employed to enhance the effectiveness of the MFA schemes

D. Conclusion

An improved 5FA scheme for online banking security was created by this study. To enhance online banking platforms, the study integrated five distinct modalities. This security solution was a strong, resilient, and easy-to-use MFA strategy that showed notable performance improvements in Average Throughput, Average Latency, and Resource Usage.

As a result, the objectives of this study were accomplished. The security of the internet banking systems was greatly improved by the 5FA system. As the digital ecosystem changes, this MFA research is a step towards developing user-friendly and solid schemes for a safer authentication experience.

E. References

[1] M. K. Sharma and M. J. Nene, "Two-Factor Authentication Using Biometric-Based Quantum Operations," Security and Privacy, vol. 3, no. 3, p. e102, 2020.

[2] G. Ali, A. M. Dida, and S. A. Elikana, "Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures," Future Internet, vol. 12, no. 10, p. 160, 2020.

[3] G. L. Moepi and T. E. Mathonsi, "Multi-Factor Authentication Method for Online Banking Services in South Africa," in Proc. 2021 Int. Conf. Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2021, pp. 1–5, doi: 10.1109/ICECET52533.2021.9698724.

[4] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," Indiana University Bloomington, 2019.

[5] G. L. Moepi and T. E. Mathonsi, "Implementation of an Adaptive Five-Factor Authentication Scheme for Online Banking Services in South Africa," in Proc. 2023 IEEE AFRICON, Nairobi, Kenya, 2023, pp. 1–6, doi: 10.1109/AFRICON55910.2023.10293332.

[6] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," IEEE Network, vol. 33, no. 2, pp. 82–88, 2019.
[7] B. Tardif, "Identification and Authentication (IA)," Division of Information Technology, vol. 1, no. 1, pp. 1–2, 2022.
[8] A. Kempen, "E-mails can cause… Cybersecurity Vulnerability in your Organisation," Serva-Mus Community-Based Safety and Security Magazine, vol. 115, no. 10, pp. 20–21, 2022.
[9] F. Blauw and S. Von Solms, "Streamlined Approach to Online Banking Authentication in South Africa and Europe," in Proc. IST-Africa Conf., IEEE, 2014, pp. 1–10.
[10] A. Rahulani and K. Mothibi, "Digital Banking Trends in South Africa," Financial Sector Conduct Authorities, vol. 1, no. 1, 2021.
[11] S. Bezzateev and S. Fomicheva, "Soft Multi-Factor Authentication," Saint Petersburg, Russia: Saint-Petersburg State University of Aerospace, 2020.
[12] A. Alhothaily, A. Alrawais, C. Hu, and W. Li, "One-Time-Username: A Threshold-Based Authentication System," Procedia Computer Science, vol. 129, pp. 426–432, 2018.
[13] N. A. M. Ariffin, F. A. Rahim, A. Asmawi, and Z.-A. Ibrahim, "Vulnerabilities Detection Using Attack Recognition Technique In Multi-Factor Authentication," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 18, no. 4, pp. 1998–2003, 2020.
[14] I. Khan, Z. Alkhalil, C. Hewage, and L. Nawaf, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Computer Science, vol. 3, no. 1, 2021.
[15] P. K. Dhillon and S. Kalra, "A Secure Multifactor Remote User Authentication Scheme for Internet of Multimedia Things Environment," Int. J. Commun. Syst., vol. 32, no. 15, p. e4077, 2019.
[16] Z. A. Zukarnain, A. Muneer, and M. K. A. Aziz, "Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges," Centre for Research in Data Science (CERDAS), vol. 1, no. 1, pp. 12–17, 2022.