Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms

Glen Lehlohonolo Moepi * and Topside Ehleketani Mathonsi

Posted Date: 14 November 2023

doi: 10.20944/preprints202311.0950.v1

Keywords: attacks; biometrics; Multi-Factor Authentication (MFA); online banking services; security; vulnerability

Article

Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms

Glen Lehlohonolo Moepi [1,*,†,‡] and Topside Ehleketani Mathonsi [2,†,‡]

[1] Department, of Information and Communication Technology; Tshwane University of Technology
[2] Department of Information Technology; MathonsiTE@tut.ac.za
* Correspondence: MoepiGL@tut.ac.za; Tel.: +27-86-110-2421
† Current address: Pretoria, South Africa.
‡ These authors contributed equally to this work.

Abstract: One of the fastest growing customer service delivery platforms is online banking. However, the increasing number of attacks on online banking platforms is driving the banks to constantly review their security. This study developed an enhanced Multi-factor authentication scheme with a track and trace capability to reduce these threats. Five modalities of authentication were incorporated in the proposed scheme: The traditional username, password, personal identification number (PIN) and one-time PIN (OTP), augmented with fingerprints or facial scans, registered smart devices, and a time locked user's location. One of the scheme's most impressive accomplishments is its capacity to seamlessly detect undesired activities and send alerts in the form of secretly obtained photographs and location triangulation. Through the design science methodology, this study using different development environments, prototyped three different schemes and compared them against the established schemes. The renowned Datadog and AppDynamics Application Measurement (APM) tools were used to evaluate the effectiveness of the schemes. The best-performing prototype received an 80 percent rating for overall security, slightly behind the 90 percent scores earned by both the First National Bank (FNB) and the Standard Bank (STD) schemes. In terms of resource utilization, the scheme was on par with both of the established schemes. In average response time the proposed scheme outperformed both the FNB and STD Bank with 500 milliseconds as opposed to 700 and 1000 milliseconds, respectively.

Keywords: attacks; biometrics; Multi-Factor Authentication (MFA); online banking services; security; vulnerability

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 of the banks employ Two-Factor Authentication (2FA), such as mobile codes alongside usernames and passwords, these measures are no longer sufficient 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 Multi-Factor Authentication (MFA) system with a built-in track and trace capability as a solution. The proposed MFA adds layers of security, incorporating biometrics, device-specific ID and geolocation alongside the traditional authentication methods [3,4].

This research employed a quantitative approach, utilizing literature reviews and prototyping [5]. The aim was to develop an enhanced MFA scheme for online banking without compromising the user experience [3,6]. Thus, setting the stage for future research in authentication domain [7,8]. The goal of the proposed Enhanced MFA scheme is to improve online banking security while ensuring a seamless user experience, contributing to the field of Information Security and Human-Computer Interface.

 doi:10.20944/preprints202311.0950.v1

Related Work

The IoT unleashed the new wave of online services deliveries. This revolutionized how institutions offered services to their clients. More services migrated to the online platforms. This development of online services increased the probabilities 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 in order 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 evaluation of user authentication techniques. The lack of these authentication studies has a negative impact on both the user's convenience and the purpose of an authentication process. The usability and security of MFA methods were explored in a study by [40]. The study's main focus was on user viewpoints, which are seen as being 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. The majority of banks deployed a range of MFA systems to provide consumers with security. The different MFA designs and features offered a non-homogenous level of security and user experience. The study evaluated the MFA design decisions adopted by the thirty banks operating in different 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 Information Security outlook. At least one authentication factor has been adopted by half of the banks. According to this study, security is an empirical cornerstone of online banking services, hence it is proposed that in order to build a strong protocol for online banking transactions, at least three different criteria be used.

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; any registered device can be chosen by the users to be used for an online authentication process. The user does not need to create or remember any credentials thus mitigating the risks associated with username and passwords combinations. However, the scheme focused mostly on user flexibility rather than stronger security for online transactions. Using multiple registered devices increased the attack surface for online transactions. In the event that 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 [13,14] highlighted the essence of authentication using human behaviour. The study centered on the necessity for implementing strong authentication schemes. Through the expedition on the authentication challenges on security and efficiency, they noted that most of the 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 it's 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 was able to predict the impostor's actions and offer a solution based on those actions. Increased security was provided by the system. The majority of current authentication methods ignore the value of user-centric controls. This study incorporates biometrics

 doi:10.20944/preprints202311.0950.v1

and user behaviour as important authentication variables because it recognizes the significance of innate and inherent user features.

According to [15], the systems are easily prone to attacks when services are accessed by the users. 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, in comparison to the other existing schemes, the authentication technique performed better in terms of defense against attacks, effectiveness, computing cost, and security characteristics. However, the program provided a way to cancel a user smart card that had been lost or stolen. The purpose of this study is to replace the use of physical tokens, which are vulnerable to theft and can be lost by the user. The amount of security vulnerabilities is increased since tangible tokens like smart cards are not password secured. In order to give a strong multimodal authentication without using tokens, this study will use registered security-protected devices enforced with biometric user recognition features. The authors [16] researched popular authentication strategies for online banking services. The objective of the study was to identify and comprehend the widely used authentication methods in order to propose a more sensible mix of authentication methods. The authors [16], concluded that the fingerprint authentication method is the most secure and user-friendly method. However, the study gave the user the option to use any one of the three available authentication factors. The main goal of 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. With the exception of a card reader system or user option, the study is identical to this proposed scientific design study in many ways. The proposed innate and inherent five factors are interconnected to provide impenetrable security.

The goal of this research is to provide an improved MFA with integrated track and trace functionality that can be utilized 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. In comparison to the proposed MFA, several of these established schemes use fewer modalities. 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 login, PIN, OTP, facial and fingerprint biometrics, registered device, and time-based location were among the five factors.

Proposed Solution

This study proposed an enhanced Five Factor MFA scheme for online banking platforms with a track and trace capability. The authentication flow procedure starts in stage one. The registration process for users begins with this step. At this important 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.

If the User ID and the correct password or PIN are matched, the MFA moves on to Stage two. The user only has three chances to type in the correct PIN or password. If all three attempts are incorrectly matched, the system will block the user and stop the future authentication steps. The customer must alert the bank and reactivate their profiles in order 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 level of verification; it is produced at random by an online system and sent to the client's registered mobile number. The consumer will then confirm their account information by entering their OTP on the online banking platforms. These entries will be compared and the additional authentication will be approved.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

The third stage of authentication 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 on 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 a maximum of 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 on to stage five after the device has been 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 successfully completed to ensure that the transactions are being 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 by the use of GPS, the geo-fencing technology, and time limits. Verified users will only be allowed to perform transactions under this enhanced Five-factor authentication scheme on registered devices, in their desired locations, and during their chosen time frames, as shown in the flowchart in Figure 2 below.

The 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 a variety of techniques, including cryptographic hashing, compare usernames, validate Personal Identification Numbers (PINs), and create One-Time Pins (OTPs). Additionally, complex mathematical modeling 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

$$S[SK_1] \Leftrightarrow C[k_1] \quad (1)$$

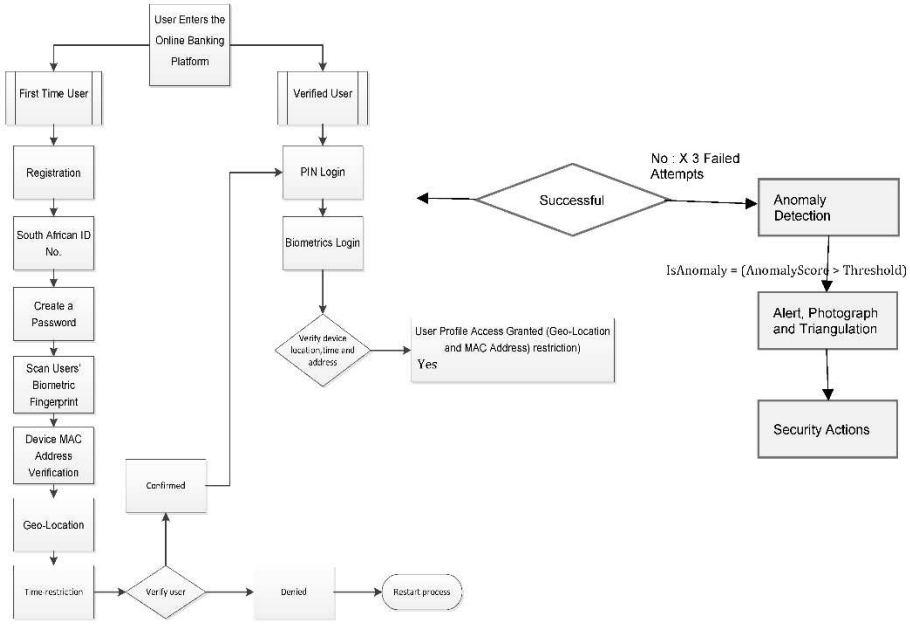

Figure 1. The Adaptive MFA Flow Chart.

 doi:10.20944/preprints202311.0950.v1

Equation 1 explains how to save the Application PIN securely. The bidirectional arrow (⇔) signifies the mutual interaction, where the client (C) offers their PIN $[k_1]$ for authentication, and the server (S) safely retains the user's secret parameter string.

Moving to biometric authentication, the core of this method is feature extraction and facial data classification. Fisher's Linear Discriminant (FLD) method is employed to extract pertinent facial data, with the objective of optimizing 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

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

Fisher's Linear Discriminant Function J is represented by Equation 2, it optimizes the contrast between within- and between-class variations. Better class separability, which is essential for classification and pattern recognition tasks, is correlated with a higher J value.

3. Fingerprint Extraction- Genetic Bio data

$$j = Gen(BioData) \rightarrow (R, P) \tag{3}$$

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

$$S[SK_6] \Leftrightarrow C[r]\text{ , therefore} S[SK_6] \rightarrow Data_6, \tag{4}$$

These calculations highlight the complex procedures that strengthen digital security, permitting various forms of authentication while protecting the integrity and privacy of user data. All the steps involved in implementing the enhanced Five-factor authentication scheme are mathematically represented in Figure 2. Each stage encapsulates the functions each factor in the proposed scheme has to play.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

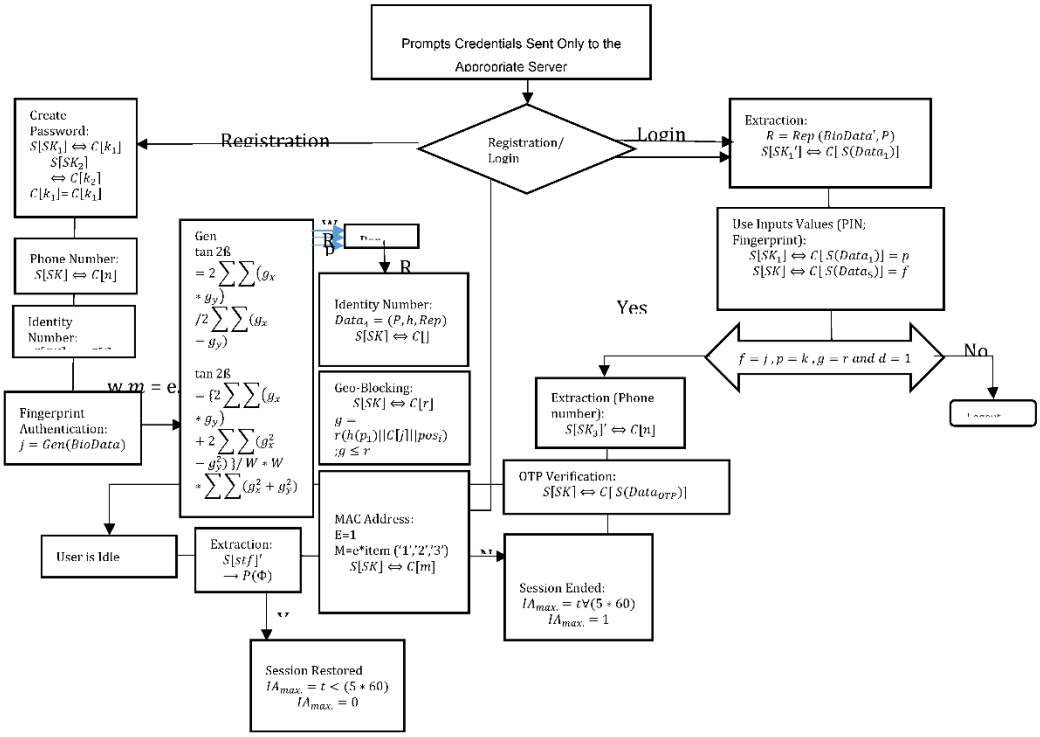

Figure 2. Enhanced Five-Factor Authentication Algorithm Mathematical Flow Model.

5. Security Constraints

The image capturing mechanism plays a crucial role in enhancing security and user verification in multifactor authentication (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 from outside of preset geographical boundaries. Here, we will discuss the significance and implementation of image capturing in such scenarios:

- Enhancing Security: Image capturing is an advanced security measure that goes beyond traditional 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. Image capturing is triggered after a predefined number of failed attempts. 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: Geo-fencing is a common technique used to restrict 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 serve as valuable forensic evidence in case of 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 cameras. It also necessitates image storage, retrieval, and secure transmission, which can pose technical challenges.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

- Implementation Challenges: The effective implementation of 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: Using image capturing technology for security purposes 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 serves as a valuable tool to document security incidents, monitor failed login attempts, and enforce geo-fencing restrictions. However, its implementation should be accompanied by clear communication with users and adherence to privacy and legal regulations to ensure that it is used ethically and responsibly.

Moving on to the session timeout. Session timeout is a critical aspect of 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 gain access to 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 contribute to the efficient use of 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, 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 Figure 3, 4 and 5 below.

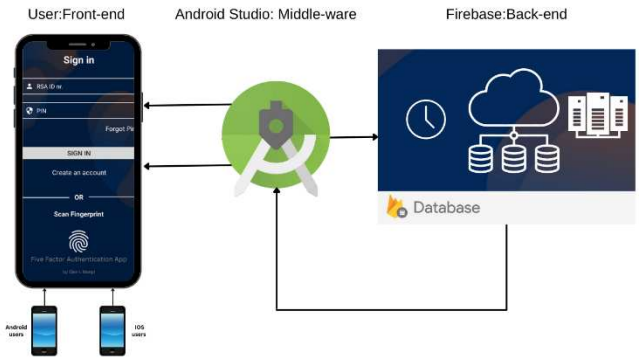

Figure 3. MFA Prototype A.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

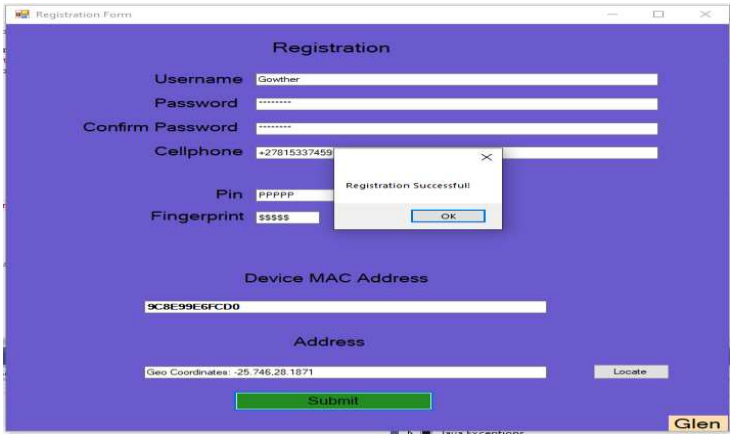

Figure 4. MFA Prototype B.

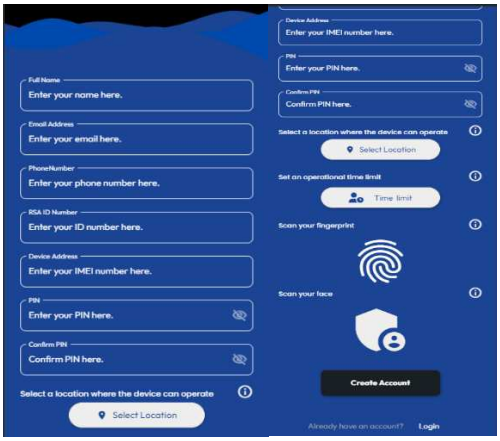

Figure 5. Enhanced Five-Factor Authentication Scheme Prototype A.

Through simulating a hypothetical scenario with a thousand concurrent users for each App, the study aimed to uncover the strengths and weaknesses of each MFA prototype. The comprehensive evaluation of Prototype 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, there are opportunities for further refinement to optimize its performance and user experience.

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

Prototype C as shown in Figure 5, represents an amalgamation of features from both prototype 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, with each 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 prototypes strengths and areas requiring future refinement. Thus, contributing to the ongoing commitment to deliver robust and secure MFA Applications.

 doi:10.20944/preprints202311.0950.v1

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. To evaluate performance metrics this study used Datadog and AppDynamics Application Performance Monitoring (APM). These are renowned cutting-edge tools, used to measure online application platforms.

In-depth evaluation was conducted using AppDynamics and Datadog. These APM tools afforded a unique perspective on the performances of the applications. 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 aspects. 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 giving MFA performance and QoS priority.

A. Result and Discussion

A. Throughput and Response Time

The throughput is the quantity of information units a system can handle in a specific period. It is the total period it takes for the Central Processing Unit (CPU), memory, encryption and decryption to complete requests. It is used in Information System Ecosystems to measure the performance of different computer components and network systems. Throughput assist with the APM metrics; how customers relate to the websites and applications. The overall Throughput performances graph is presented in the below Figure 6.

The overall throughputs of the FNB and STDB Apps were 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 Prototype A and B, it measured a throughput of 1000 TPM. Through this comparison, we were able to determine 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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

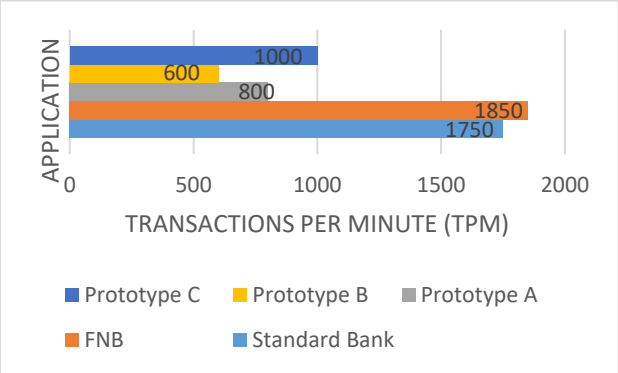

Figure 6. Average Throughput Data Bar Graph.

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.

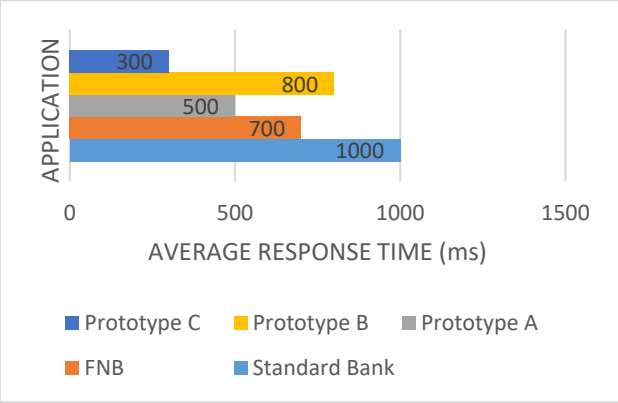

Figure 7. Average Response Time Data Bar Graph.

B. Security and Resource Utilization

Security is an essential in maintaining safeguard sensitive data, maintain user trust, comply with legal requirements, prevent fraud and cyberattacks, minimize financial loss, protect the institution's reputation, and stay resilient against evolving threats. The FNB (9) and the STDB (9) Apps, boasted strictest security posture. They were shortly followed by Prototype C, which had a strong security rating of 8. Prototype A (7) and B (6) likewise 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. Following closely behind were the STDB and the FNB Apps, both achieved resource utilization ratings of 9. These banking Apps excelled in managing system resources, emphasizing high performance and responsiveness to user interactions. Their superior resource optimization contributed significantly to their overall efficiency. The summary of the overall result is represented in Table 1.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 November 2023 doi:10.20944/preprints202311.0950.v1

Table 1. Summary of the key metrics evaluated in all of the Apps.

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
Performance Percentage (2010s to 2100s)	50%	40%	70%	80%	90%

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 Prototype Versions 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 Compatibility and System Requirements	3. Browser Compatibility	3. Continual Monitoring and Enhancement
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.

Conclusion

This study developed an enhanced Five-factor authentication scheme for online banking security. The scheme incorporated a set of five distinct modalities with the goal of improving online banking services. The security solution was a robust, resilient and user-friendly MFA scheme. The scheme demonstrated notable performance improvements in terms of the Average Throughput, Average Time, Resource Utilization, and Security.

As a result, the goals of this research were successfully accomplished. The security of the online banking platforms was enhanced with the developed Five-factor authentication Scheme. This MFA research offers a step toward creating solid schemes for a safer authentication experience as the digital landscape changes.

References

1. Sharma, M.K. & Nene, M.J. Two-Factor Authentication Using Biometric Based Quantum Operations. Security and Privacy, 3(3):e102. , 2020.
2. Ali, G., Dida, A.M. & Elikana S. A. Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. Future Internet, 12(10):160. , 2020.
3. Das, S., Wang, B., Kim, A. & Camp, L.J. MFA Is A Necessary Chore: Exploring User Mental Models of Multi-Factor Authentication TZZechnologies, 2020.
4. Das, S., Wang, B., Tingle, Z. & Jean Camp, L. Evaluating User Perception of Multi-Factor Authentication a Systematic Review. Indiana University Bloomington, 2019.
5. Marasco, E. & Albanese, M., Biometric Multi-Factor Authentication: On the Usability of the FingerPIN Scheme. National Science Foundation.1 (1): 1-5 and 7-13, 2021.
6. Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y. & Gerla, M. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. IEEE Network, 33(2):82-88, 2019.
7. Tardif, B. Identification and Authentication (IA). Division of Information Technology, 1(1):1-2., 2022.
8. Kempen, A. E-mails can cause… Cybersecurity Vulnerability in your Organisation Serva-Mus Community-Based Safety and Security Magazine, 115(10):20-21, 2022.
9. Blauw, F. & Von Solms, S. Streamlined Approach to Online Banking Authentication in South Africa and Europe. 2014 IST-Africa Conference Proceedings. IEEE: 1-10. , 2014.
10. Rahulani, A. & Mothibi, K. Digital Banking Trends in South Africa. Financial Sector Conduct Authorities, 1(1). , 2021.
11. Bezzateev, S. & Fomicheva, S. Soft Multi-Factor Authentication. Saint Petersburg, Russia, Saint-Petersburg State University of Aerospace. .2020.
12. Alhothaily, A., Alrawais, A., Hu, C. & Li, W. One-Time-Username: A Threshold-Based Authentication System. Procedia Computer Science, 129:426-432, 2018.
13. Ariffin, N.A.M., Rahim, F.A., Asmawi, A. & Ibrahim, Z.-A. Vulnerabilities Detection Using Attack Recognition Technique In Multi-Factor Authentication. TELKOMNIKA (Telecommu-nication Computing Electronics and Control), 18(4):1998-2003. , 2020.
14. Khan, I., Alkhalil, Z., Hewage, C. & Nawaf, L., Phishing Attacks: A Recent Comprehen-sive Study and a New Anatomy. 2021 Editor's Pick: Computer Science, 3(1), 2021.

 doi:10.20944/preprints202311.0950.v1

15. Dhillon, P.K. & Kalra, S. A Secure Multifactor Remote User Authentication Scheme for Internet of Multimedia Things Environment. International Journal of Communication Systems, 32(15): e4077, 2019.
16. Zukarnain, Z. A., Muneer, A. & Aziz, M. K. A. Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. Centre for Research in Data Science (CERDAS), 1(1): 12-17, 2022.