FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 4, February, 2026, pp 331 – 338
DOI: https://doi.org/10.33003/fjs-2026-1004-4870

ADAPTIVE RISK-BASED MULTI-LAYER AUTHENTICATION FRAMEWORK FOR SECURE ONLINE BANKING SYSTEMS

[*1]Jumoke Soyemi, [2]Mudasiru Hammed and [2]Olugbenga Babajide Soyemi

[1]Department of Computer Science, The Federal Polytechnic, Ilaro, Ogun State, Nigeria.
[2]Department of Civil Engineering, The Federal Polytechnic, Ilaro, Ogun State, Nigeria.

[*]Corresponding Auhtor's Email: jumoke.soyemi@federapolyilaro.edu.ng

ABSTRACT

Digital banking services have grown rapidly, increasing exposure to credential theft, phishing, replay attacks, and account takeover fraud. Traditional, single-factor, and static multi-factor authentication systems are still susceptible in the event that attackers breach one or more levels of authentication. This paper presents and experimentally confirms an adaptive risk-based multi-layer authentication system adapted to an online banking context. The model integrates knowledge-based verification (PIN), recognition-based graphical authentication, possession-based one-time password (OTP), and a dynamic risk-scoring engine that adjusts authentication strictness based on contextual indicators such as login location, device profile, and behavioral anomalies. A probabilistic security model is designed to measure the likelihood of attack success, measured by independent authentication layers. The framework was tested in the web-based prototype environment and tested with 120 participants who underwent 500 total authentication attempts, and with simulated adversarial conditions. False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error rate (EER), Area Under the ROC Curve (AUC), Precision, recall, and response time were used to measure the performance. The presented adaptive framework demonstrated a high authentication rate of 98.9, FAR of 0.7, FRR of 2.6, and EER of 1.65, which is considerably higher than single-factor and fixed two-factor baselines. The ROC analysis had an AUC equal to 0.991, which implies that it has a high discrimination ability. These results indicate that risk-adaptive authentication has a higher resilience to fraud and can still be operated effectively.

Keywords: Adaptive authentication, Cybersecurity, Fraud detection, Multi-factor authentication, Online banking security, Risk-based authentication

INTRODUCTION

Digital banking systems have redefined the delivery of financial services through the facilitation of cross-geographic and cross-device transactions remotely. Although this digital transformation has made things more accessible and efficient, it has also widened the cybercrime attack space (Claessens et al., 2002; Ometov et al., 2018; Raghu, 2025). The phishing, session hijacking, credential stuffing, and social engineering attacks have continued to rise in the financial institutions that use the internet banking system (Florencio & Herley, 2007). Authentication schemes that rely on static methods, especially password- and PIN-based authentication, have been found to be ineffective in addressing these threats because they are vulnerable to brute-force attacks, passwords reuse, and phishing attacks (Bonneau et al., 2012; Herley and Van Oorschot, 2012; Oduguwa and Arabo, 2024).

Multi-factor authentication (MFA) offers additional protection by integrating independent authentication properties that are often divided into knowledge-based (what the user knows), possession-based (what the user has), and inherence-based (what the user is) authentication factors (Grassi et al., 2017; Ometov et al., 2018). MFA can greatly lower the risk of unauthorized access by forcing users to undergo numerous types of authentications, in contrast to single-factor authentication methods. MFA implementations, however, are usually based on the premise that the risks are homogeneous in all authentication scenarios. Practically, the risk of authentication can be context-dependent with unfamiliar devices, abnormal login times, unusual geographic locations, or abnormal behavior patterns by the user (Freeman et al., 2016; Traore et al., 2012; Carjuman, 2025; Fereidouni, et al., 2024).

Risk-based adaptive authentication is a solution to this drawback; it dynamically allocates the authentication criteria based on the determined contextual risk. In these systems, verifications with a high-risk condition can be configured to activate an extra verification step, whereas low-risk ones can be provided with simplified authentication processes that do not compromise the system security (Bhargav-Spantzel et al., 2007; Fereidouni et al., 2024; Podapati et al., 2025). This paper incorporates the concept of adaptive risk scoring into a multi-layer authentication system aimed at the online banking systems.

In the previous studies, it has been established that single-factor authentication methods are extremely susceptible to brute-force attacks, phishing, and credential theft (Bonneau et al., 2012; Florencio and Herley, 2007). Two-factor authentication (2FA) and especially a PIN with a one-time password (OTP) leads to a higher level of protection since it adds an extra level of verification and eliminates the possibility of unauthorised access (Aloul et al., 2009; Ometov et al., 2018; Ghiyamipour, 2021). Nevertheless, 2FA systems are vulnerable to new types of threats, including SIM swap attacks, phishing proxies, and social engineering attacks on the OTP delivery channel (Das et al., 2014).

Biometric authentication provides greater identity checks through physiological or behavioral attributes such as fingerprints, facial, and voice patterns (Jain et al., 2006). Nevertheless, widespread implementation of biometric authentication is usually accompanied by other issues, such as the cost of infrastructure, privacy issues, and hardware dependencies that can restrict the mass application in all digital banking settings (Jain et al., 2006; Anwar et al., 2025). Graphical password Systems have also been considered as an alternative authentication system. It has been revealed that graphical authentication may prove to be more resistant to dictionary and brute-force attacks than traditional text-based passwords (Saadi et al., 2024; Biddle et al., 2012;

Wiedenbeck et al., 2005). In spite of these benefits, the use of graphical password systems can present usability problems because of the cognitive load during authentication (Ghiyamipour, 2021).

Recent studies on adaptive authentication have also paid more attention to contextual risk modeling in order to enhance access control mechanisms (Freeman et al., 2016; Traore et al., 2012). Nevertheless, most of the current methods do not have detailed empirical verification or formal mathematical modeling to measure the decrease in attack probability under the influence of layered authentication mechanisms (Chennuri, 2024; Podapati et al., 2025). Moreover, only a limited number of studies combine graphical authentication, PIN validation, one-time password validation, and contextual risk analysis into one authentication architecture that is backed up by quantitative performance assessment.

This study fills this gap by coming up with a mathematically modelled multi-layered authentication system that incorporates adaptive risk-based authentication logic that can dynamically change security requirements based on contextual conditions. The paper also presents a probabilistic model, which measures the resistance to layers of attack and shows that by combining several authentication schemes, the probability of getting unauthorized access is significantly lowered. The given framework is empirically tested by the means of extensive experimental assessment based on the Receiver Operating Characteristic (ROC) analysis and Equal Error Rate (EER) calculation. Besides this, a performance comparison is also done with single factor and two factor baseline authentication systems to determine the efficiency and better performance of the proposed adaptive authentication.

System Architecture and Modelling

Overview of the Adaptive Framework

The suggested framework will be based on four key pieces, including the registration module that will capture and store user credentials and profile during the account creation process, the multi-layer authentication engine that will be used to verify user identity by using the sequential authentication steps that may include PIN, graphical password and one-time password, the risk scoring engine that will be used to assess contextual indicators such as device, location of the account log-in and account access time to determine the level of authentication needs and the fraud detection and notification, which will alert or notify the user and the system administrator upon the detection of any potential security Figure 1. Adaptive Risk-Based Multi-Layer Authentication Framework Architecture.

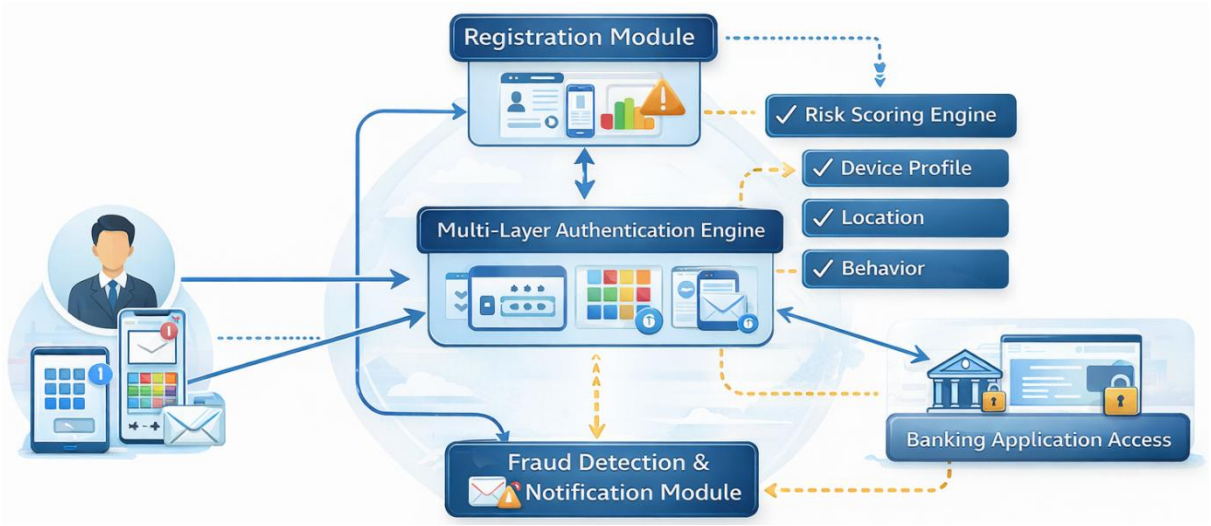

Figure 1: Architecture of the Adaptive Risk-Based Multi-Layer Authentication Framework

The architecture provides a demonstration of how the user interacts with key security elements of the system. Account creation is the first interaction the user has with the registration module. In the authentication process, the multi-layer authentication engine handles the processing of login requests and orchestrates verification of the request by multiple security layers. The risk scoring engine considers the contextual factors, including the device identity, location, and the behavior of logging in, among others, to identify what level of authentication should be applied. The fraud detection and notification module tracks suspicious transactions and alerts when abnormal transactions are detected. A successful verification is a secure access to the banking application.

Dynamic Risk Scoring Model for Adaptive Authentication

The proposed framework includes a dynamic risk scoring mechanism to facilitate context-sensitive decision making at the time of login to assess the probability of fraudulent access basing on various indicators of the context. The system does not use a standard authentication process on all the authentication attempts, but instead changes the authentication requirements based on the level of risk that is estimated to be posed by the request.\

The risk score R is calculated as a weighted average of contextual security indicators on the time of login,

$$R = w_1L + w_2D + w_3T + w_4B \quad (1)$$

where:

L = is the location anomaly rating, and it is the difference between the present location and the locations that have been trusted by the user in the past. Login with a different geographic area or IP address leads to an increase in the value of the location anomaly.

D = represents the device unfamiliarity score, which measures whether the request to log in is made by a formerly registered or trusted device. When the system identifies a new or unfamiliar device fingerprint, the score is boosted.

T = represents an abnormal time-of-access score, which includes the abnormalities in the time of access relative to the historical user pattern of use. Out-of-band access also makes the value of anomalies increase.

B = denotes the behavioral deviation score, which is calculated based on user interaction behavior, including typing dynamics, navigation behavior, or response time during the authentication.

The coefficients w_1, w_2, w_3,and $w_4$are normalized weight parameters that determine the relative importance of each risk factor. These weights satisfy the condition.

$\sum_{i=1}^{4} wi = 1$ (2)

and can be tuned during system training or experimental calibration to reflect the most predictive indicators of fraudulent activity within the operational environment.

Risk-Based Authentication Decision Policy

Once the aggregated risk score R is computed, the system determines the appropriate authentication level based on predefined risk thresholds. This adaptive decision process ensures that legitimate users experience minimal friction while suspicious attempts undergo a stricter verification procedure.

The policy of decision is as follows:

i. Low-Risk Authentication
   If $R < \theta_1$

The attempted login is categorized as low risk, which means that the contextual parameters are very similar to the history of the user. In this instance, the system will need PIN-based authentication, which will allow quick and convenient access to the system.

ii. Moderate-Risk Authentication
   If $\theta_1 \leq R \leq \theta_1$

The attempted login is classified as moderate risk. Such a case can occur when the user enters the system with a new device or a strange location, but there is no high level of suspicious activity. The system thus implements the use of two-factor authentication, where both Personal Identification Number (PIN) and Graphical password verification are used.

iii. High-Risk Authentication
   If $R \geq \theta_2$

The login attempt is rated as high risk, which means that there is a substantial deviation from the usual access pattern of the user. In this case, the system will enable the three-layered authentication, which consists of: PIN validation, Graphical password authentication and One-Time Password (OTP) delivered to the registered mobile phone or email. This multiple-level verification system greatly minimizes the chances of unauthorized access despite having an attacker who has partial credentials.

The dynamic risk scoring method has a variety of benefits over the traditional static authentication systems. To begin with, it reduces the number of authentication processes by the legitimate users under normal circumstances. Second, it enhances protection in the background of suspicion by adding up more checks. Lastly, mathematical formulation enables the system to be customized and complemented with the analysis of the empirical data to detect phishing, steal credential, and hijack the session better. The proposed framework is appropriate to be deployed in online banking systems and secure messaging services because it offers a balanced trade-off among the security robustness and the user usability by integrating contextual anomaly detection with adaptive authentication policies.

Algorithm 1: Adaptive Risk-Based Authentication Decision

An adaptive authentication system dynamically decides the degree of verification to be done against every attempted login, depending on the calculated contextual risk score. The decision process, based on the proposed framework, is the following algorithm.

Input:

User login request U, contextual parameters L, D, T, B

Output:

Authentication decision and required verification level

Table 1: Adaptive Risk-Based Authentication Decision Procedure

Algorithm 1:	
Steps:	Begin
1	Capture contextual login parameters: location, device ID, access time, and behavioral metrics
2	Compute anomaly scores: i. $L \leftarrow$ Location anomaly score ii. $D \leftarrow$ Device unfamiliarity score iii. $T \leftarrow$ Time-of-access anomaly score iv. $B \leftarrow$ Behavioral deviation score
3	Compute the overall risk score $R = w_1L + w_2D + w_3T + w_4B$
4	$R < \theta_2$ then Request PIN authentication only
5	*Else if* $\theta_1 \leq R \leq \theta_2$ then *Request PIN + Graphical Password*
6	*Else if* $\theta_1 \leq R \leq \theta_2$ then *Request PIN + Graphical Password*
7	Else if $R \geq \theta_2$ then *Request PIN + Graphical Password + One-Time Password (OTP)*
8	*Verify submitted credentials*
9	If verification is successful then *Grant secure access to the application*
10	Else *Trigger fraud detection alert and deny access*
11	End

Algorithm 1 starts with gathering contextual parameters linked to the login attempt. Algorithm 1 begins by collecting contextual parameters associated with the login attempt. These parameters are transformed into normalized deviation

scores of the user behavior of the past. The weighted risk score Ris was then calculated as wi. Depending on the score, the system will adaptively decide on the necessary level of authentication based on two threshold values θ_1 and θ_2. This is a multitiered approach to decision making where a low-risk access request is made user-friendly, whilst potentially malicious actions face increased authentication measures.

Implementation, Development, and Testing Platform

The proposed adaptive risk-based multi-layer authentication system was implemented, developed, and tested through a software-based experimental platform, which was developed and tested based on a client-server architecture. The system was created with high-level programming languages, namely Python in the back end to handle logic and authentication processing, and JavaScript, HTML, and CSS to handle the user interface and interactions between the client and the system.

The backend services were installed on a web application platform that is integrated with Flask, and a MySQL database was used to store user authentication profiles containing PINs, graphics password patterns, device identifiers, and behavioral logs.

The system was experimented in a controlled simulation environment with standard computing hardware (personal computers and laptops) connected to a network to simulate real-world conditions of logins. Different authentication scenarios, such as legitimate access, and simulated attack scenarios, such as brute-force access, OTP replay, and device spoofing, were tested in this environment.

To compute performance metrics, built-in Python libraries and data analysis packages like NumPy and scikit-learn were used, which made it easy to compute FAR, FRR, precision, recall, F1-score, EER, and ROC-AUC.

Experimental Design and Evaluation

Participants and Dataset

The suggested adaptive risk-based multi-layer authentication system was experimentally tested with the help of the controlled dataset created with the participation of the users and simulated attack conditions. The test was conducted on 120 registered subjects who voluntarily entered into the experimental authentication setting. In the registration step, every participant generated a distinct authentication profile that comprised a personal identification number (PIN), graphical password pattern, and contextual attributes like device identity and customary login behavior.

To assess the effectiveness of the authentication framework under realistic conditions, a dataset of 500 authentication attempts was collected and analyzed. This dataset consisted of 350 legitimate authentication attempts performed by registered users during normal login activities. These legitimate attempts were recorded across varying contextual conditions, including different devices, login times, and network locations, in order to capture natural behavioral variations among users. Besides the valid access attempts, 150 simulated attack attempts were created to test the resilience of the system against unauthorized access. These were simulated attacks to reflect the common credential compromise and impersonation situations as witnessed in contemporary digital systems. In the attack simulations, random attempts at brute-forcing PINs were performed, where an unauthorized user made repeated attempts of trying to guess valid PIN combinations without information regarding the correct ones. The other attack scenario was graphical password permutation attacks, where the attackers tried various combinations of different graphical patterns in an attempt to compromise the graphical authentication layer.

Additional attack tests included OTP replay attacks, and, in this case, previously recorded one-time passwords were reused to attempt unauthorized access. As OTP mechanisms are configured to be valid within a window of time, this test measured the capability of the system to identify and block reused authentication tokens. Moreover, there were also device spoofing simulations to evaluate the possibility of attackers cheating the device recognition with the simulation of the digital fingerprint of a trusted device. The fact that both legitimate and malicious attempts at logging in were introduced yielded the possibility to evaluate the authentication framework in detail in terms of its capacity to differentiate between a genuine user and a possible attacker when placed in different contextual settings.

Evaluation Metrics

In order to measure the effectiveness and dependability of the suggested authentication system quantitatively, a number of accepted biometric and cybersecurity assessment indicators were used. The metrics give objective measure of the strength of security as well as the usability nature of the system. The False Acceptance Rate (FAR) is one of the key indicators in the assessment and provides an idea of the percentage of unauthorized access by users to the system. The value of FAR closer to zero shows that the system is resistant to impersonation and credential compromise attacks. The False Rejection Rate (FRR) is another significant metric, and it is the percentage of legitimate users that are denied access when they are being authenticated. The FRR needs to be minimized when it comes to ensuring usability and making sure that the actual users are not shown undue failures when attempting to log in. Precision and Recall were also used to determine the correctness of the system in classifying legitimate and malicious authentication processes. Precision indicates the accuracy of the detected intrusion, which is really malicious, and recall is the capability of the system to identify true intrusion attempts. In order to have a balanced score that takes into consideration both precision and recall at the same time, F1-score was computed. The F1-score is the harmonic mean of the two performance indicators, precision and recall, providing one performance measurement on the accuracy and completeness of detection.

The other important parameter in the analysis is the Equal Error Rate (EER), which is the operating point where the false rejection rate and the false acceptance rate will be identical. The EER is found to be very popular in the authentication study area due to the fact that it gives one number that represents the overall trade-off between security and usability in the system. A reduction in the EER values demonstrates an improvement in the authentication performance.

Lastly, the effectiveness of the suggested framework was further examined in terms of the ROC curve, which also represents the correlation between the true positive rate and the false positive rate, but at various levels of decision threshold. The AUC was calculated to measure the total discriminative ability of the authentication model. A higher AUC value is a sign that the system is very effective in separating the legitimate users and the attackers. Collectively, these metrics of evaluation offer a holistic evaluation of the proposed adaptive authentication framework, which allows a thorough evaluation of its capability to ensure robust security without compromising the convenience of users.

RESULTS AND DISCUSSION

Performance Comparison

The effectiveness of the proposed adaptive risk-based authentication framework was tested and compared with the existing authentication models to find out its efficiency to enhance security without compromising acceptable usability. The system in question was specifically compared to two baseline approaches, namely a single-factor authentication model and a two-factor authentication model. These models reflect the typical authentication systems that are generally applied in numerous digital banking systems.

The outcome of the evaluation shows that there is a great improvement in authentication security when the adaptive multi-layer authentication framework is implemented. The False Acceptance Rate (FAR) of the single-factor model was 12.1%, which implies a very high chance of unauthorized access when the single credential factor is applied. The two-factor authentication model was more resistant to attacks, with the FAR as low as 4.4%. The proposed adaptive authentication model, however, had a significantly lower FAR of 0.7%, which means that the chances of an attacker passing through the authentication layers were very low.

Regarding usability as presented in Table 2, the False Rejection Rate (FRR) was also considered. The single-factor model registered an FRR of 1.9, and the two-factor model registered a slightly higher value of 2.2 because of the extra authentication process. The proposed adaptive model achieved an FRR of 2.6%, which is only slightly greater than the baseline approaches and is well within the usability limits. This minor change is anticipated due to the fact that the system automatically implements more stringent authentication measures whenever greater risk scores are identified. When the system effectiveness is considered in the broadest sense, the proposed model was found to have an authentication accuracy of 98.9 in comparison with the single-factor model (86.4) and the two-factor model (93.5). This enhancement shows that the combination of layered authentication and contextual risk assessment would greatly increase the accuracy of the authentication process.

The EER further confirms the superior performance of the proposed system. While the single-factor model produced an EER of 7.0% and the two-factor model produced 3.3%, the adaptive framework achieved a much lower EER of 1.65%, reflecting a stronger balance between security and usability. Similarly, the Area Under the ROC Curve values demonstrate the improved classification capability of the adaptive authentication system. The proposed model achieved an AUC value of 0.991, which is significantly higher than the values recorded for the single-factor (0.842) and two-factor (0.931) authentication systems.

Table 2: Authentication Performance Comparison

Model	FAR	FRR	Accuracy	EER	AUC
Single-Factor Authentication	12.1%	1.9%	86.4%	7.0%	0.842
Two-Factor Authentication	4.4%	2.2%	93.5%	3.3%	0.931
Proposed Adaptive Model	0.7%	2.6%	98.9%	1.65%	0.991

The results clearly indicate that integrating contextual risk evaluation with multi-layer authentication substantially improves both detection capability and resistance to unauthorized access.

ROC Curve Analysis

In an attempt to further test the discriminative capacity of the authentication framework, Receiver Operating Characteristic (ROC) was analyzed. The ROC curve shows the correlation between the True Positive Rate (TPR) and False Positive Rate (FPR) with the change in the threshold of authentication decision. The trial conducted during the experiment changed different risk threshold values and OTP expiration to see the impact of authentication stringency on the detection performance. The higher the decision threshold, the more conservative the system and therefore the fewer false acceptance but the possibilities of false rejection are higher.

The generated ROC curve of the proposed adaptive authentication framework in Figure 2 gave a better performance in comparison to the baseline models. The curve was always more aligned to the upper-left side of the ROC space, which means that it is highly sensitive and has low false positive probabilities at different thresholds. The calculated Area Under the Curve of the adaptive authentication model is 0.991, which compares to the theoretical maximum of 1.0. The result in Figure 2 is an indication that the proposed system can differentiate legitimate login from malicious login attempts.

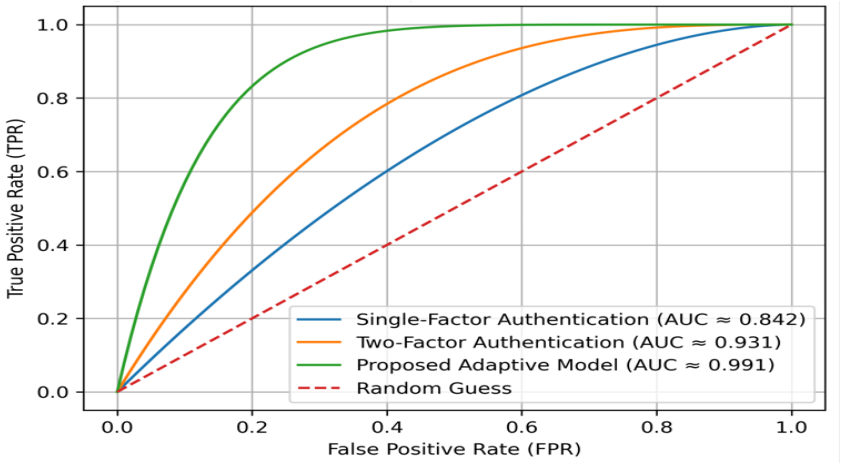

Figure 2: ROC Curve Comparison of Authentication Models

The outcome of this analysis also proves that combining risk features (location anomaly, device familiarity, access time irregularity, and behavioral deviation) can greatly advance categorization accuracy in authentication systems.

Equal Error Rate Analysis

The Equal Error Rate (EER) is also another significant evaluation criterion of the authentication system, as it indicates the operating point at which the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal. This value gives one figure that captures the total balance between the security of the system and its user-friendliness. In the assessment procedure, FAR and FRR values were plotted against authentication thresholds so as to determine the point of intersection. This analysis revealed that the proposed system attained an EER of 1.65% lower than the baseline system.

The single-factor authentication model achieved an EER of 7.0%, indicating low resistance to unauthorized access attempts. This value increased to 3.3% with the two-factor authentication system, showing the advantages of an extra authentication factor. Nonetheless, the adaptive multi-layer authentication system considerably decreased the EER to 1.65%, which underscores the efficiency of integrating contextual risk scoring and dynamic authentication requirements.

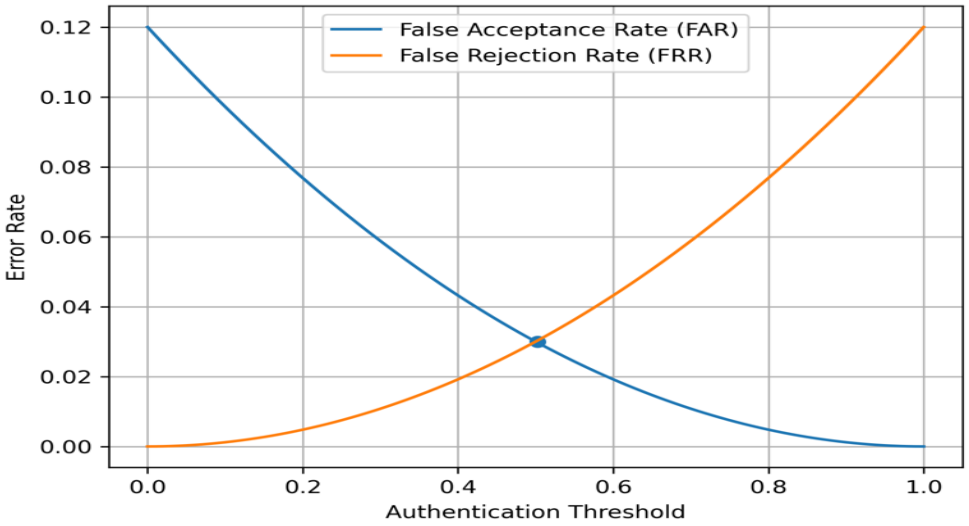

Figure 3: FAR–FRR Intersection Showing Equal Error Rate

The fact that the EER value is lower implies that the system has a superior trade-off between security and usability by ensuring that false acceptance and false rejection rates are minimized.

Discussion

The results of the experimental assessment show that the suggested adaptive authentication system significantly improves the security status of online systems and ensures the adequate usability of the system by genuine users. The overall power of the framework is that it can dynamically change the requirements of authentication according to the contextual evaluation of risks. Also, unlike traditional authentication methods that are static and depend on a similar verification process to all the login attempts, the proposed model uses contextual signals like user behavior, device properties, the location where the individual is logging in and time of access to identify the right level of authentication that should be used.

In low-caution cases when the way the user logs in matches the already set model, the system will only allow authentication with the main credential, such as. the PIN. This reduces redundant authentication processes and minimizes the level of user inconvenience, hence improving the general user experience. Nevertheless, in case anomalies or suspicious activity are detected, e.g., the detection of unknown devices, unusual geographic routes, anomalous times of login, or odd behavior, the system automatically increases the authentication process by enabling extra authentication, e.g., by turning on graphical password validation and one-time password (OTP) validation. Layered authentication architecture can be used to enhance cyberattack resistance to a large extent. Probabilistically, the probability that an intruder manages to go past several independent authentication levels reduces exponentially with the number of verification levels added to the system. As an example, although a malicious actor can manage to compromise or guess the PIN, he or she will still have to reproduce the graphical password sequence properly and deliver a valid OTP in a short time. It is a multi-layer defense system, and accordingly, complicates and computes intrusion attempts more to achieve success.

The analysis conducted experimentally indicated that despite the extra security checks in case of high-risk circumstances, the system still achieved an average authentication response time of 2.3 seconds. Response time is within the acceptable range of a modern digital financial platform, which suggests that additional security controls do not impact its responsiveness and user experience in a significant way.

The performance evaluation of the system demonstrates that the contextual risk analysis combined with multi-factor authentication is efficient. The ROC analysis provided a high classification accuracy, and the EER is low, which means that the framework can be trusted with distinguishing legitimate users and potential attackers. Generally, the findings indicate that the proposed model offers a sound and viable defense against most cybersecurity vulnerabilities, including credential theft, brute-force attacks, replay attacks, and impersonation of a device.

CONCLUSION

This study deployed an Adaptive Risk-Based Multi-Layer Authentication Framework for Secure Online Banking Systems. The system combines various authentication

methods and risk assessment to validate specific login requests according to statistics of user location, access time, behavior pattern, and device knowledge. The deployed system improves unauthorized access and ensures the dynamic application of credentials according to the perceived level of risk. The Architecture proposed in this study is a combination of PIN, OTP, layered architecture, and graphical password. The mathematical models that were developed show that the likelihood of successful unauthorized access is exponential in the number of independent authentication layers. The challenges raised in this theoretical review clearly support the suitability of the proposed security architecture and continue to emphasize the usefulness of multi-factor authentication mechanisms in enhancing the security of a system. Also, the performance, robustness, and reliability of the system were proven using an experimental evaluation under normal and adversarial conditions. Both legitimate authentication attempts and simulation of attack conditions, including brute-force PIN attacks, graphical permutation attacks, OTP replay attacks, as well as simulation of device spoofing, were also stressed on the framework. The FAR, FRR, accuracy, precision, recall, and F1-score were calculated as performance metrics to determine the effectiveness of the system. The findings show that the adaptive authentication model performs better compared to traditional single-factor and two-factor authentication models.

The Receiver Operating Characteristic analysis revealed that the system had an Area Under the Curve of 0.991, meaning that it had an almost 100 percent capacity to discriminate against valid users and attackers. Also, Equal Error Rate analysis showed that the intersection point was low, indicating that the authentication model was stable and reliable in different decision thresholds. One of the most important contributions of this study is the creation of an adaptive decision mechanism that eliminates the unnecessary complexity of the authentication process when the risk is low and implements more stringent security checks in case the suspicious activity is identified. This is an advantageous method of both improving security and ease of use because invalid users are not forced to go through unnecessary authentication procedures when making regular access attempts. Overall, the results point to adaptive risk-based authentication as an effective, scalable, and feasible way of improving cybersecurity in modern digital financial environments. The security threats that are common, such as compromise of credentials, impersonation attacks, and session hijacking, can be countered, and the system can still perform efficiently using the framework. Altogether, contextual risk assessment combined with multi-layer authentication solutions would provide a powerful and implementable security framework to financial organizations that aim to secure sensitive online services against a growing range of more complex cyber threats without interfering with a smooth user experience.

Limitations

This research was done in an experimental setting that is not fully real-world operational conditions, which is likely to be complex and less predictable. Also, the analysis did not represent a diverse geographic area, i.e., differences in user behaviour of different areas and structures were not heavily reflected. Moreover, the suggested authentication system has not been implemented in a large-scale actual banking system yet, and hence, its performance with high-volume and real-time financial transactions is still to be empirically tested.

Future Work

The future research must be based on the extension of the framework with the use of machine learning, which provides behavioral profiling techniques in order to enhance the user behavior modeling and authentication accuracy. Real-time detection of anomaly models would enhance the capacity of the system to detect suspicious activities as they take place even more. Moreover, the use of blockchain-based mechanisms of identity verification can also increase the integrity and traceability of digital identities in the authentication procedure.

REFERENCES

Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In *2009 IEEE/ACS international conference on computer systems and applications* (pp. 641-644). IEEE.

Anwar, N. M., Ahmad, S. S. S., Kausar, N., Stević, Ž., & Gaba, Y. U. (2025). Multiple biometric authentication for online banking system based on multiple fuzzy approach. *Scientific Reports*, *15*(1), 32824.

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2007). Establishing and protecting digital identity in federation systems. *Journal of Computer Security*, 14(3), 269–300.

Biddle, R., Chiasson, S., & Van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4), 1–41.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE symposium on security and privacy* (pp. 553-567). IEEE.

Carjuman, N., Fook, L. C., & Hlaing, Z. C. (2025, November). Enhanced MFA Framework Against Modern Security Threats. In *Proceedings of the 2025 10th International Conference on Cloud Computing and Internet of Things* (pp. 148-155).

Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, 21(3), 253–265.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In *Network and Distributed System Security Symposium (NDSS)* (Vol. 14, No. 2014, pp. 23-26).

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the World Wide Web Conference*, 657–666.

Freeman, D., Jain, S., Dürmuth, M., Biggio, B., & Giacinto, G. (2016, February). Who Are You? A Statistical Approach to Measuring User Authenticity. In *Network and Distributed System Security Symposium (NDSS)* (Vol. 16, pp. 21-24).

Ghiyamipour, F. (2021). Secure graphical password based on cued click points using fuzzy logic. *Security and Privacy*, *4*(2), e140.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63B)*. National Institute of Standards and Technology.*NIST special publication*, *800*, 63-3.

Herley, C., & Van Oorschot, P. (2012). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, 10(1), 28–36.

Jain, A., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security*, 1(2), 125–143.

Kandula, S. R., Kassetty, N., ALANG, K. S., & Pandey, P. (2024). Context-aware multi-factor authentication in zero trust architecture: Enhancing security through adaptive authentication. *International Journal of Global Innovations and Solutions (IJGIS)*.

Oduguwa, T., & Arabo, A. (2024). Passwordless authentication using cryptography, steganography, and biometrics. *Journal of Cybersecurity and Privacy*. *4*(2), 278-297.

Ometov, A., Bezzateev, S., Mäkitalo, N., et al. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1–37.

Podapati, V. H., Nigam, D., & Das, S. (2025, July). SoK: a systematic review of context-and behavior-aware adaptive authentication in mobile environments. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 406-419). Cham: Springer Nature Switzerland.

Raghu, N., Bhat, R., Nambiar, P. R., Shetty, G. S., & DB, A. K. (2025). Blockchain-enhanced GAN image encryption scheme for cloud computing. In *Intelligent Systems and IoT Applications in Clinical Health* (pp. 367-392). IGI Global.

Saadi, Z. M., Sadiq, A. T., Akif, O. Z., & Farhan, A. K. (2024). Security vulnerabilities and protective strategies for graphical passwords. *Electronics*, 13(15), 3042

Traore, I., Woungang, I., Nakkabi, Y., Obaidat, M. S., Ahmed, A. A. E., & Khalilian, B. (2012). Dynamic sample size detection in learning command line sequence for continuous authentication. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *42*(5), 1343-1356.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1–2), 102–127.