

MLE-RBA: A Machine Learning-Empowered Risk-Based Authentication Algorithm

Iurii Matiushin(✉) and Vladimir Korkhov

St Petersburg State University, St Petersburg 199034, Russia
{y.matyushin,v.korkhov}@spbu.ru

Abstract. Risk-Based Authentication (RBA) is a dynamic authentication approach that assesses login attempts based on contextual risk factors. Traditional RBA implementations, such as Freeman et al.'s Naïve Bayes method, provide adaptive security but have limitations in precision and adaptability. In this study, we propose an enhanced RBA method leveraging machine learning to improve risk assessment accuracy.

We design and implement MLE-RBA, an ML-empowered RBA system using a LightGBM classifier trained on a user login dataset, incorporating feature engineering, anomaly detection, and data balancing techniques. Our approach is evaluated against Freeman's method and the SIMPLE heuristic, with performance measured in terms of Equal Error Rate (EER) and other key metrics. Experimental results show that our ML-based approach achieves a lower EER, demonstrating improved authentication accuracy while maintaining usability.

Despite its effectiveness, we emphasize that RBA, even when enhanced with ML, should not replace primary authentication mechanisms but rather serve as a supplementary layer to improve security. Our findings contribute to the ongoing development of adaptive authentication strategies, highlighting ML's potential in optimizing RBA systems.

Keywords: Risk-Based Authentication · Machine Learning · Cybersecurity

1 Introduction

1.1 The Need for Risk-Based Authentication

As cyber threats continue to evolve, traditional password-based authentication methods have become increasingly inadequate. Simple password authentication is vulnerable to attacks such as credential stuffing, phishing, and brute force attacks, leading to widespread security breaches. Two-factor authentication (2FA) and multi-factor authentication (MFA) offer additional security layers, yet they introduce usability challenges, often frustrating users with frequent secondary verifications. To balance security and usability, modern authentication systems must adopt adaptive and context-aware mechanisms [1].

One of these approaches is known as **risk-based authentication**, or **RBA**. The essence of this approach is calculating a risk score associated with a particular login

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15894, pp. 325–339, 2026.
https://doi.org/10.1007/978-3-031-97648-3_22

attempt, based on such factors as the connecting device's geographic location, the device's OS and browser version, IP address, and others.

Based on the risk score calculated by the RBA mechanism, the security system can make a decision on how to proceed: if the perceived risk is low enough, the user can be allowed to connect without requiring any additional steps, but if the risk score exceeds a certain threshold – either static or dynamic – additional verification steps are required, such as one-time passwords, biometric authentication, or other approaches.

This means that RBA possesses the following advantages:

- **Increased usability:** since RBA works in the background from the user's perspective, and only triggers additional security steps when necessary, legitimate users can continue their work uninterrupted in the majority of cases.
- **Learning potential:** based on past sessions, an RBA system can create a more and more comprehensive user profile, becoming better at predicting whether the user is legitimate or not over time.
- **Integration potential:** RBA can – and, indeed, should – be combined with other existing authentication approaches, making the system more secure while not unnecessarily compromising usability [2].

1.2 Historical Background for RBA

The RBA concept was introduced in order to mitigate the issues associated with widely used authentication mechanisms, such as passwords, which often do not offer a high enough degree of security, and 2FA/MFA, which often requires the users to take additional steps in order to access a system, decreasing usability.

In particular, Freeman et al. conducted one of the fundamental studies in the field in 2016, using a Naïve Bayes classifier in order to detect account hijacking [3]. Their approach, based on behaviour patterns associated with a given user, is described in further detail in Part 3 of this work.

Freeman's work was followed by subsequent research by Wiefling, Dürmuth, and Lo Iacono. In particular, by analysing real-world authentication system, they came to the conclusion that several popular online services, such as Google, Facebook, LinkedIn, and GOG.com are using RBA in one form of another, despite frequently obscuring the details of their approach to user authentication [4].

Further studies by the same researchers analysed RBA's benefits and shortcomings in deployed systems; in particular, it was revealed that RBA is often perceived by users to be more user-friendly while maintaining a high level of protection [5,6]. This makes RBA particularly appealing for the situations where balancing security and user experience is crucial, such as large-scale web applications.

1.3 The Potential for Machine Learning in RBA

Early implementations of risk-based authentication (RBA), such as Freeman et al.'s algorithm, primarily relied on rule-based heuristics and traditional statistical models. However, the ongoing development of machine learning (ML) offers significant potential to increase the effectiveness of RBA systems. In particular, ML algorithms can analyse

large volumes of authentication data and uncover complex behavioural patterns that earlier methods might find harder to capture. By training on historical login data, ML-based RBA systems can improve over time in several ways, such as dynamically adjusting risk thresholds and re-evaluating the importance of a given risk score factor.

Furthermore, recent advancements such as federated learning have enabled privacy-preserving applications of ML in the context of user authentication, which means that RBA algorithms can utilize user data to improve their accuracy without compromising sensitive user data [7].

Collectively, these developments suggest that ML-driven RBA has the potential to offer several important advantages, such as improved security, usability, and privacy.

1.4 Our Contribution

In this work, we design, implement, and test a machine learning-empowered risk-based authentication method, as well as comparing it to certain existing approaches. More specifically, we:

- Develop an ML-empowered RBA model (MLE-RBA), incorporating advanced feature selection and classification techniques in order to calculate risk scores and determine if a particular user is legitimate or not.
- Evaluate our method using a real-world authentication dataset.
- Benchmark our approach against Freeman's Naïve Bayes-based method, as implemented by the Data & Application Security (DAS) Group [8], and a SIMPLE heuristic-based RBA method, as described by Wiefling, Dürmuth, and Lo Iacono in their 2021 study [5].

The results of our comparative analysis demonstrate that ML-empowered RBA has advantages over other approaches when it comes to accuracy, availability, and adaptability. The findings offer valuable insights into the practical integration of machine learning within risk-based user authentication systems, laying a foundation for future research in this area.

1.5 Article Structure

The article is organized as follows.

In Part 1, we introduce the concept of risk-based authentication and discuss the need for RBA and the potential for using ML in such authentication algorithms, as well as our contribution.

In Part 2, we conduct a literature review on the topic of risk-based user authentication.

In Part 3, we propose and describe MLE-RBA, a machine learning-empowered risk-based authentication algorithm.

In Part 4, we conduct comparative analysis, which includes modifying Freeman's algorithm and implementing a SIMPLE risk-based algorithm for comparison purposes.

In Part 5, we conclude our work, discuss our findings, offer considerations for using ML-empowered RBA as a part of a user authentication system, and list future research directions.

2 Related Work

This section provides a brief review of the current RBA-related research.

"Who Are You? A Statistical Approach to Measuring User Authenticity" (2016) by Freeman et al. is one of the foundational studies in the field of risk-based authentication. It introduces a probabilistic, Bayesian approach to authentication, developing a statistical framework to detect account hijacking and non-legitimate login attempts based on previous user behaviour. The framework is then tested on a sample of real-life login data from LinkedIn as well as simulated attacks, and a systematic study of possible attackers is also provided [3].

Several more recent studies explored RBA and Freeman's algorithm further, focusing on such topics as real-life usage, user perception, and usability of such an approach.

In particular, Wiefling et al. conducted a study on RBA algorithms used in eight popular online services (**"Is this really you? An empirical study on risk-based authentication applied in the wild"**, 2019). In order to achieve that, they have developed an automated browser testing framework capable of simulating human-like user behaviour within each service. They found that an IP address is a particularly relevant piece of information in the risk-based authentication context and discovered three distinct RBA models (single-feature, multi-feature, and VIP). Their work has also led to discovery and fixing of a vulnerability within Facebook's authentication protocol [4].

In **"What's in score for website users: A data-driven long-term study on risk-based authentication characteristics"** (2021), Wiefling et al. provide further analysis of an RBA system's practical deployment. The results of this study demonstrate that RBA should be tailored to each service, and even small configuration adjustments can greatly impact security and usability. They also identify a new, previously unused RBA feature, as well as factors that could potentially affect RBA performance [5].

"F-RBA: A Federated Learning-based Framework for Risk-based Authentication" (2024) by Fereidouni et al. integrates RBA with another emerging technology in the field of ML, particularly, federated learning. The study introduces a distributed architecture that provides local risk assessment on user devices instead of centralizing this functionality. The authors also provide empirical evaluation of their proposed approach using a real-world multi-user dataset [7].

"RLAuth: A Risk-Based Authentication System Using Reinforcement Learning" (2023) by C. Picard and S. Pierre provides an example of using binary anomaly detection in a risk-based authentication system. The authors propose a system consisting of an anomaly detector, a risk engine, and an authentication manager, and conducted empirical testing to prove its effectiveness. It should be noted that this study focuses specifically on mobile application security [9].

The study **"Evaluation of Real-World Risk-Based Authentication at Online Services Revisited: Complexity Wins"** by Jan-Phillip Makowski, Daniela Pöhn (2023) re-evaluates the RBA systems of major online services such as Google, Amazon, and Facebook. The authors' research partly verifies the earlier findings of Wiefling et al. They note that the risk-based authentication systems employed by certain popular services, Amazon in particular, seem insufficiently strong, failing to provide alternative ways to safely verify a user's identity and seemingly not reacting to several suspicious user behaviour patterns [10].

Overall, the evolution of RBA reflects a concerted effort to develop authentication systems that are both secure and user-friendly. By using contextual information and adaptive mechanisms, RBA offers a promising alternative to traditional authentication methods, providing high level of security while not compromising usability.

3 The Proposed ML-Based Algorithm

We propose **MLE-RBA (Machine Learning–Empowered Risk-Based Authentication)**, a novel risk-based algorithm inspired by Freeman's work but leveraging the capabilities of machine learning in order to provide more accurate user identity verification based on contextual factors and behavioural data.

MLE-RBA is designed to dynamically assess the risk of authentication attempts by combining classical risk-based heuristics with modern machine learning techniques. The algorithm leverages both anomaly detection and supervised classification to estimate a numerical risk score for each login attempt, which is then used to determine whether additional verification is warranted.

In this work, the algorithm is implemented using a multi-stage pipeline that includes target encoding, class imbalance handling, anomaly detection, and classifier calibration.

3.1 The Rationale for Our Algorithm

As stated above, our algorithm was originally inspired by Freeman's Naïve Bayes-based method.

The method estimates the risk of a login attempt based on statistical rarity. It assigns a risk score to login attempts based on how unusual certain attributes (e.g., IP address, User-Agent, ASN) are compared to past logins from the same user and the global distribution of all users. The risk score is then compared to a predefined threshold. If the risk score is below the threshold, the login succeeds; if it is above the threshold, additional authentication (e.g., MFA) is required. The underlying principle is to flag anomalous activities while minimizing friction for regular users.

While effective, this approach has limitations:

1. **Feature weighting is fixed:** each feature contributes equally or is manually weighted, regardless of actual importance.
2. **Static thresholds:** the risk threshold is predefined and does not adapt to different attack patterns or user behaviours.
3. **Lack of advanced behavioural analysis:** the model does not fully utilize time-based or frequency-based behavioural features.

Our algorithm enhances Freeman's approach while preserving its core idea:

1. **Machine learning-based feature weighting:** instead of manually assigning feature importance, we train a model to learn the impact of each feature on login success. This ensures that important features (such as IP changes) influence the risk score more than less relevant ones.

2. **Adaptive threshold selection:** instead of using a fixed threshold, we dynamically adjust it based on Precision-Recall curves, minimizing both false positives and false negatives.
3. **Enhanced feature engineering:** we introduce behavioural metrics like time since last login, improving risk assessment.

The source code is available at our GitHub repository [11].
The following sections explain the algorithm's work in more detail.

3.2 MLE-RBA Algorithm Pipeline

Feature Engineering and Data Preprocessing
Initially, the input dataset (e.g., collected login records) is pre-processed to handle missing values and standardize feature formats. Categorical features such as "country", "region", "city", "ASN", "user agent string", "browser name and version", "OS name and version", and "device type" are first imputed for missing values and then encoded using a target encoding method with smoothing. A time-based feature, "time_since_last_login," is derived by calculating the time difference between successive login attempts for each user.
Handling Class Imbalance
Authentication datasets typically suffer from class imbalance, with genuine logins vastly outnumbering attack attempts. To address this, the algorithm employs SMOTETomek – a hybrid resampling method that both oversamples the minority class and cleans the majority class by removing ambiguous samples [12, 13]. This balancing step is applied exclusively on the training data to avoid data leakage.
Anomaly Detection
To capture irregularities in user behaviour, the MLE-RBA algorithm incorporates two complementary anomaly detection methods:

- **Local Outlier Factor (LOF):** configured with a tuned number of neighbours and a specified contamination rate, LOF identifies local deviations in the data using a cosine similarity metric.
- **Isolation Forest:** this global anomaly detector isolates observations by recursively partitioning the data.

Both methods are trained on the balanced, encoded training data. Their output scores are normalized and then combined with equal weighting to produce an aggregate anomaly score, which is appended as an additional feature to the original feature matrix. This hybrid approach enhances the algorithm's sensitivity to both local and global anomalies.
Classifier Training and Calibration
The final feature matrix, which includes both the encoded features and the combined anomaly score, is used to train a LightGBM classifier. The classifier is configured with optimized hyperparameters, including an increased maximum depth (to capture more complex interactions), regularization terms, and class weights that favour the minority (attack) class.

LightGBM was chosen because of its efficiency and scalability when handling large datasets, which are important advantages in a real-world authentication scenario. It also offers excellent speed and accuracy, as well as superior performance over such classifiers

as Random Forest and traditional gradient boosting methods, especially when working with large amounts of data and high-dimensional feature spaces.

Due to the imbalanced nature of the problem, the classifier's raw output probabilities are further calibrated using sigmoid calibration (via CalibratedClassifierCV) to ensure that the risk scores are well-calibrated and reflect true likelihoods.

Threshold Selection and Evaluation Metrics

To translate continuous risk scores into a binary decision (e.g., whether to trigger additional authentication), a decision threshold must be determined.

The algorithm computes the Receiver Operating Characteristic (ROC) curve, from which it calculates both the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The optimal threshold is selected discretely by identifying the threshold at which the absolute difference between FAR and FRR is minimized. This threshold is then used to classify login attempts.

Evaluation metrics such as the Area Under the ROC Curve (AUC-ROC), confusion matrix, classification report, and Equal Error Rate (EER) are computed to assess the model's performance.

3.3 Visual Representation

Visual representation of the MLE-RBA algorithm is shown in Fig. 1.

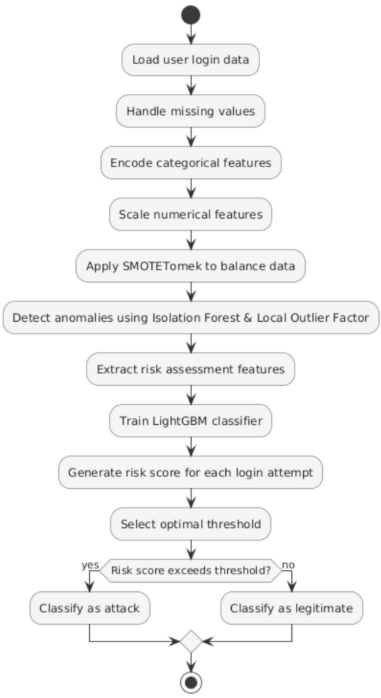

Fig. 1. ML-empowered RBA algorithm pipeline.

4 Algorithm Testing and Evaluation

4.1 Dataset

In order to train and test our algorithm, as well as to perform comparative testing, we use the login data set for risk-based authentication provided by the Data & Application Security Group (DAS) [14]. The dataset is available at the DAS Group's GitHub page [15].

The authors describe the dataset as follows: "Synthesized login feature data of >33 M login attempts and >3.3 M users on a large-scale online service in Norway. Original data collected between February 2020 and February 2021."

Each record in the dataset represents a single login attempt and includes a variety of features such as:

- **User identifiers and timestamps:** a unique user ID and the corresponding login timestamp allow for the reconstruction of user-specific login histories and the analysis of temporal patterns.
- **Network information:** attributes like the IP address, Autonomous System Number (ASN), and geographical indicators (country, region, and city) provide context regarding the network origin of the login attempt.
- **Device and client data:** the dataset captures details from the user agent, including the browser name and version, operating system name and version, and the device type. These features are critical for establishing a behavioural profile for each user.
- **Authentication outcome:** it includes a binary label indicating whether the login was successful.

4.2 Freeman's Algorithm

The first algorithm we compare MLE-RBA to is Freeman's RBA algorithm.

For comparative testing purposes, we used the implementation of Freeman's algorithm by Data & Application Security Group, which is freely accessible on GitHub [8].

To provide a comprehensive evaluation and direct comparison with our approach, we enhanced the above implementation with additional evaluation code. Specifically, after obtaining risk scores for each login attempt, our evaluation module computes the AUC-ROC score using standard libraries and visualizes the ROC curve. The confusion matrix is generated to provide an error breakdown, and a custom function calculates the EER by finding the intersection point of the false acceptance and false rejection rates.

Our variation of the DAS Group's implementation can be found in our GitHub repository [11].

4.3 SIMPLE Algorithm

We also implement another risk-based algorithm as a benchmark – a simple feature-based model, described by Wiefling et al. as follows [5]:

"The simple model (SIMPLE) extends the single-feature model used in the open source single sign-on solution OpenAM [31] and is assumed to be used at GOG.com [46]. It also partly reflects models given in literature [42,24,16]. We based our implementation on OpenAM, since it is freely available and probably widely used. The SIMPLE algorithm checks a number of features for an exact match in the user's login history. The risk score is the number of inspected features with at least one match in the login history divided by the total number of considered features. Thus, the risk score granularity increases with the number of observed features."

Our implementation uses the same dataset as for Freeman's algorithm and our MLE-RBA approach. The data is indexed by login timestamps and is grouped by user to ensure that the authentication history for each individual is processed in chronological order. The algorithm focuses on a fixed set of features:

For each user, the algorithm maintains a history of observed values for these features. When processing each login attempt, the algorithm compares the current feature values with those previously recorded. The risk score is determined by the ratio of familiar values (the ones already seen in a given user's login history) to the total number of features.

To facilitate a robust comparison with other RBA methods, we enhanced our implementation of SIMPLE by integrating evaluation metrics, including the AUC-ROC score, confusion matrix, and Equal Error Rate (EER). This evaluation framework provides a comprehensive view of the algorithm's performance, allowing us to contrast its behaviour with both Freeman's probabilistic method and our ML-empowered RBA approach.

Our implementation of the SIMPLE algorithm is also accessible at our GitHub repository [11].

4.4 Evaluation Metrics

We use several different metrics in order to evaluate the authentication algorithms' accuracy.

- **AUC-ROC score** shows how well a model can produce relative scores to discriminate between positive and negative results – in our case, between legitimate and fraudulent authentication attempts – across all classification thresholds.
- **Confusion matrix** demonstrates the number of true positives (legitimate login attempts flagged as such), false positives (attacks successfully passing as legitimate login attempts), true negatives (accurately detected attack attempts), and false negatives (legitimate login attempts flagged as attacks).
- **EER (equal error rate)** shows the point at which the false acceptance rate (FAR) and false rejection rate (FRR) are equal – in our case, we can change FAR and FRR values by adjusting the risk score threshold.

Overall, these metrics offer complementary perspectives: AUC-ROC for overall discrimination performance, the confusion matrix for detailed error analysis, and EER for understanding the balance between security and user experience.

4.5 Evaluation Results

In this section, we demonstrate the results of the comparative analysis via two types of graphs.

FAR, FRR, and EER graph for the SIMPLE algorithm can be seen in Fig. 2.

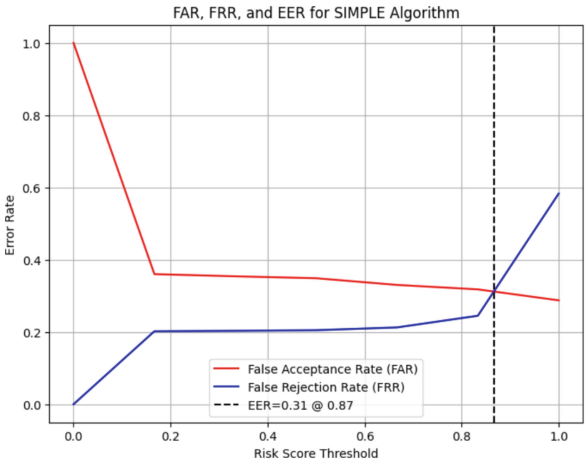

Fig. 2. FAR, FRR, and EER graph for the SIMPLE algorithm.

Confusion matrix for the SIMPLE algorithm can be seen in Fig. 3.

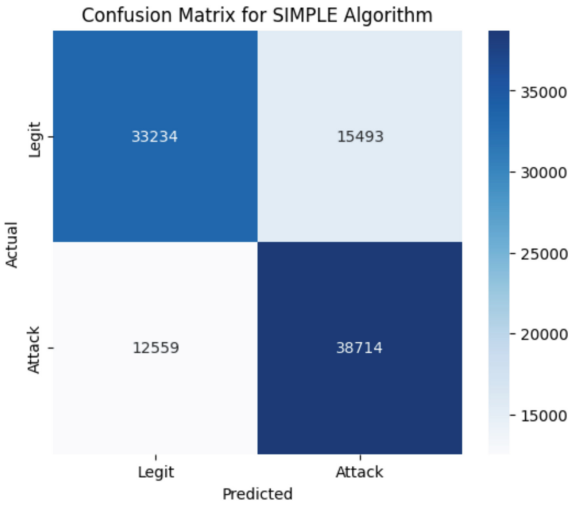

Fig. 3. Confusion matrix for the SIMPLE algorithm.

FAR, FRR, and EER graph for Freeman's algorithm can be seen in Fig. 4.

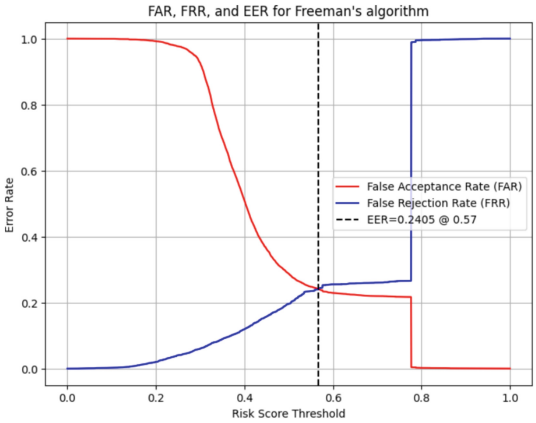

Fig. 4. FAR, FRR, and EER graph for Freeman's algorithm.

Confusion matrix for Freeman's algorithm can be seen in Fig. 5.

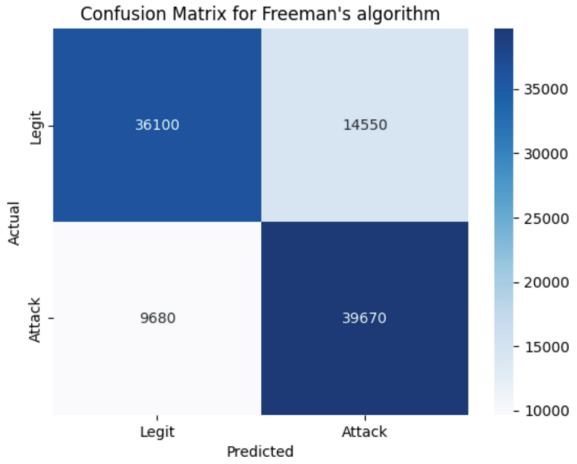

Fig. 5. Confusion matrix for Freeman's algorithm.

FAR, FRR, and EER graph for the MLE-RBA algorithm can be seen in Fig. 6.

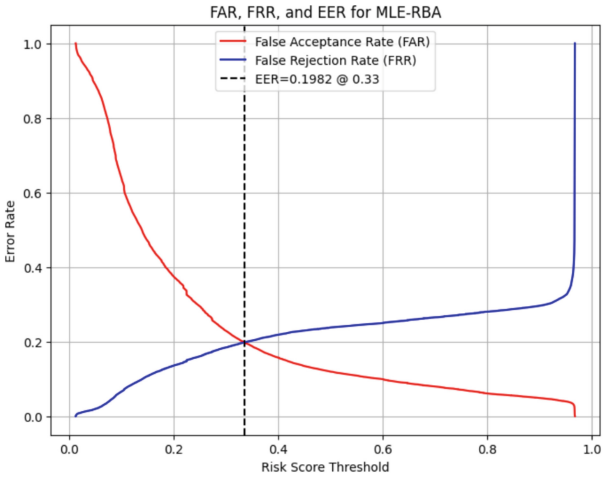

Fig. 6. FAR, FRR, and EER graph for MLE-RBA.

Confusion matrix for the MLE-RBA algorithm can be seen in Fig. 7.

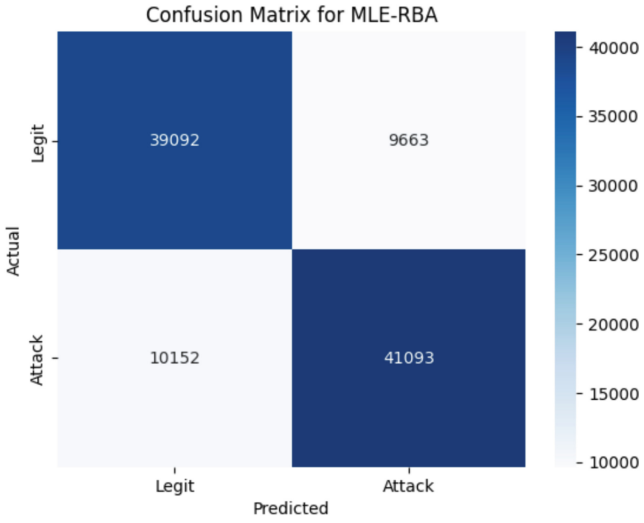

Fig. 7. Confusion matrix for MLE-RBA.

4.6 Results Summary

A summary of evaluation metrics for SIMPLE, Freeman's, and MLE-RBA algorithms is presented in Table 1.

Table 1. Evaluation metrics summary.

Metric	SIMPLE	Freeman	MLE-RBA
EER	0.3100	0.2405	0.1982
AUC-ROC	0.6862	0.7600	0.8721

5 Conclusions and Future Work

5.1 Results Discussion

Our experimental evaluation indicates that the MLE-RBA approach demonstrates improved performance compared to both Freeman's algorithm and the SIMPLE heuristic. The metrics show that MLE-RBA achieves a better balance between false acceptances and false rejections, and it has a higher ability to distinguish between legitimate and fraudulent login attempts.

In practical terms, these improvements suggest that the ML-based model is more effective at adapting to dynamic behavioural patterns, which is crucial for maintaining security without compromising usability. The enhanced discrimination performance implies that the system can more reliably detect anomalous behaviour, which reduces the risk of unauthorized access while minimizing unnecessary authentication challenges.

5.2 Considerations for the Algorithm's Usage

However, it should be noted that the MLE-RBA algorithm, even while outperforming other RBA approaches, still shows a relatively high EER, especially compared to the more classical authentication methods.

This shows that RBA should not be relied upon as the sole way to confirm a user's identity; instead, it should be implemented as a part of a hybrid authentication system incorporating multiple authentication factors. As discussed at the beginning of the article, if the RBA method outputs a risk score exceeding the chosen threshold, approaches such as OTP (one-time passwords) can be used to make the final decision on whether to allow continued access to the system or deny it.

Moreover, MLE-RBA can coexist with a wide range of commonly used authentication methods, from classic password protection to biometrics. It can be used as one of the levels of a multi-factor authentication (MFA) system triggering additional defence layers if the risk threshold is reached, or as a part of a hybrid method calculating login risk scores based on a variety of factors – for instance, by combining it with a keystroke or mouse movement recognition algorithm.

That said, an important point of consideration is ensuring that MLE-RBA integrates smoothly with other systems to avoid conflicts, such as triggering redundant MFA requests or producing conflicting risk evaluation outputs. For example, if MLE-RBA flags a login as high-risk, but biometric or password-based systems do not, this could lead to inconsistent results.

By carefully calibrating risk thresholds and establishing clear protocols for prioritizing or reconciling conflicting assessments, MLE-RBA can ensure a coherent, unified decision-making process and enhance security without sacrificing usability and overburdening the user with unnecessary checks.

5.3 Future Work Directions

As shown above, MLE-RBA shows promise, providing better results in terms of accuracy compared to other approaches, but there is still room for further improvement.

We plan to continue improving our approach by conducting experiments with a wide variety of ML models and classifiers, such as ensemble methods, deep learning architectures, hybrid models combining several algorithms, etc. The end goal is to determine the optimal combination of steps to accurately calculate login risk scores, separating the attackers from the legitimate users.

In addition, it should be noted that we are currently working with a single, albeit extensive and high-quality dataset. Should we gain access to a wider range of user login data, we also plan to incorporate it into our work, making sure the system we are developing can be effectively implemented in a variety of real-world scenarios.

One possible direction of further improvement is the interpretability of MLE-RBA's decisions. Machine learning models can often appear as "black box" systems, which can make it hard for human users to understand how exactly the authentication system decides whether a given login attempt is "risky" or not. A way of addressing this is to integrate explainable AI (XAI) techniques, such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations), which provide clearer insights into the model's decision-making process [16]. This will make it easier for administrators to identify why MLE-RBA flags certain login attempts as risky and adjust the model as necessary – for instance, if a legitimate user is wrongly identified as a possible threat.

Another promising direction is the integration of the ML-RBA system into a continuous authentication framework. By incorporating a CA method like dynamic keystroke recognition, which demonstrates superior accuracy relative to other similar methods [17], the system could continuously validate user identity rather than relying solely on point-of-entry checks. This hybrid approach has the potential to significantly enhance both security and usability by providing ongoing assurance of user authenticity while remaining relatively unobtrusive to the end user.

Acknowledgement. Supported by Saint Petersburg State University, project ID: 95438429.

References

1. Rashidi, B., Garg, V.: Open sesame: lessons in password-based user authentication. Cyber Secur. A Peer-Reviewed J. **4**(4), 317–329 (2021)
2. Security vs. usability: Pros and cons of risk-based authentication. https://www.infosecinstitute.com/resources/management-compliance-auditing/security-vs-usability-pros-cons-of-risk-based-authentication. Accessed 01 Mar 2025

3. Freeman, D., et al.: Who are you? a statistical approach to measuring user authenticity. NDSS, vol. 16 (2016)
4. Wiefling, S., Iacono, L.L., Dürmuth, M.: "Is this really you? An empirical study on risk-based authentication applied in the wild. In: ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25–27, 2019, Proceedings 34. Springer (2019)
5. Wiefling, S., Dürmuth, M., Iacono, L.L.: What's in score for website users: a data-driven long-term study on risk-based authentication characteristics. In: Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25. Springer, Heidelberg (2021)
6. Wiefling, S., Dürmuth, M., Iacono, L.L.: "More than just good passwords? a study on usability and security perceptions of risk-based authentication. In: Proceedings of the 36th Annual Computer Security Applications Conference (2020)
7. Fereidouni, H., et al.: F-RBA: A Federated Learning-based Framework for Risk-based Authentication. arXiv preprint arXiv:2412.12324 (2024)
8. rba-algorithm. https://github.com/das-group/rba-algorithm. Accessed 20 Mar 2025
9. Picard, C., Pierre, S.: RLAuth: A risk-based authentication system using reinforcement learning. IEEE Access **11**, 61129–61143 (2023)
10. Makowski, J.-P., Pöhn, D.: Evaluation of real-world risk-based authentication at online services revisited: complexity wins. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (2023)
11. MLE-RBA. https://github.com/YuriyM-SPB/MLE-RBA. Accessed 23 Mar 2025
12. Chawla, N.V., et al.: SMOTE: synthetic minority over-sampling technique. J. Artif. Intell. Res. **16**, 321–357 (2002)
13. SMOTETomek. https://imbalanced-learn.org/stable/references/generated/imblearn.combine.SMOTETomek.html. Accessed 23 Mar 2025
14. Wiefling, S., et al.: Pump up password security! Evaluating and enhancing risk-based authentication on a real-world large-scale online service. ACM Trans. Privacy Secur. **26**(1), 1–36 (2022)
15. rba-dataset. https://github.com/das-group/rba-dataset. Accessed 21 Mar 2025
16. Angelov, P.P., et al.: Explainable artificial intelligence: an analytical review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery **11**(5), e1424 (2021)
17. Matiushin, I., Korkhov, V.: Continuous authentication methods for zero-trust cybersecurity architecture. In: International Conference on Computational Science and Its Applications. Springer, Cham (2023)