GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Economics and Management Innovation

Article

Application of Machine Learning in Financial Risk Classification and Account Verification Optimization Strategy

Ziwei Liu [1,*]

[1] Siebel School of Computation & Data Science, University of Illinois Urbana-Champaign, Urbana, IL, 61801, USA

* Correspondence: Ziwei Liu, Siebel School of Computation & Data Science, University of Illinois Urbana-Champaign, Urbana, IL, 61801, USA

Abstract: With the rapid advancement of technology, effective financial risk control and ensuring account security have become key issues of concern in the financial industry. In the face of increasingly complex financial scenarios and constantly updated attack strategies, previous risk assessment and account verification methods are becoming less effective. This study developed an account security authentication mechanism following financial risk classification methodology. More specifically, an account verification architecture that integrates multiple sources of information is created using a comprehensive risk assessment framework that integrates machine learning techniques. This architecture combines biometric technology, user behavior pattern analysis, and device usage data to enhance the account verification process, including accuracy and speed of risk discrimination. In addition, by introducing adaptive optimization mechanisms, the model can self-adjusted and improve in real time. Overall, the strategy proposed in this study has implications for improving the security protection capability and intelligence level of financial systems.

Keywords: financial risk management; account verification; machine learning; multimodal data; risk detection

1. Introduction

Against the backdrop of rapid expansion in the financial sector and rapid penetration of information technology, financial institutions are facing increasingly severe challenges in risk management and account security, which have become major obstacles to achieving healthy growth of the financial system. In recent years, machine learning as an advanced data analysis technology has been increasingly used in financial risk monitoring and account verification. This article reviews the current development status of financial risk classification and account verification, and utilizes machine learning techniques to construct an efficient and intelligent risk detection and warning mechanism. By collecting data, choosing models, and applying optimization, a comprehensive solution featuring multimodal data fusion and dynamic abnormal behavior detection is proposed to improve the risk identification and defense capabilities of financial systems.

2. Background

2.1. Types of Financial Risks and the Need for Account Verification

In the financial field, risk is defined as various unexpected events or situations that may pose challenges to the stability and security of the financial system, covering categories such as market risk, credit risk, and operational execution risk [1]. Common financial risks are shown in Figure 1. Market risk mainly stems from changes in financial market prices, such as interest rates, foreign exchange rates, and fluctuations in stock prices, while credit risk is related to the failure of debtors or trading parties to fulfill contracts. The risk of operational execution is related to internal management processes, system failures, or

Received: 09 March 2025
Revised: 17 March 2025
Accepted: 29 March 2025
Published: 02 April 2025

human errors. Lately, with the rise of online finance, new risks such as cybersecurity and legal compliance have also emerged.

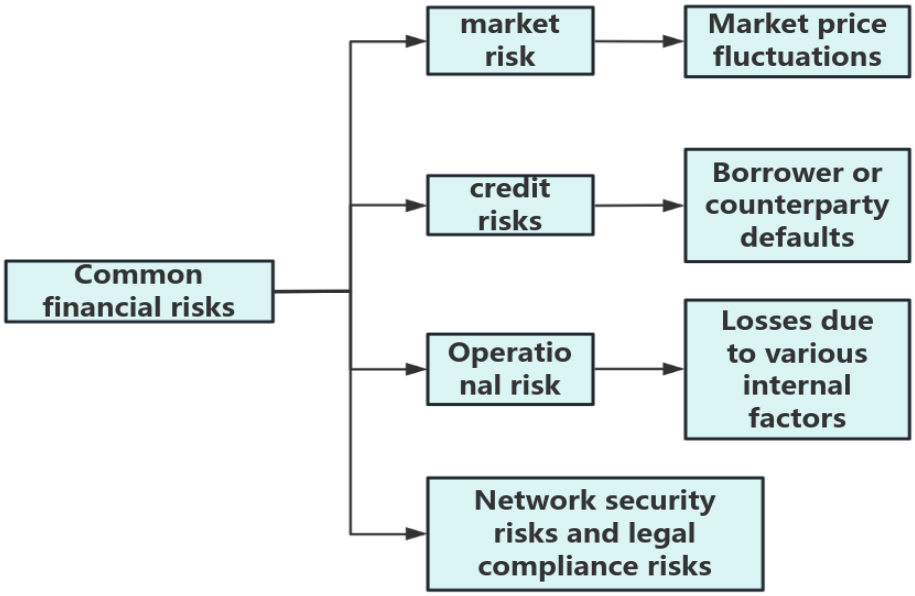

Figure 1. Common types of risks.

The development of digital financial services has made account verification a cornerstone of financial security. Account verification refers to the process of confirming and validating the identity of users accessing financial services, and is typically achieved through knowledge-based authentication (KBA), biometrics-based authentication (BBA), or multi-factor authentication (MFA) methods [2]. This process serves as a crucial first line of defense against unauthorized access and fraudulent activities in financial systems, as it directly addresses several critical financial risks. For credit risk, it helps ensure that financial institutions are dealing with legitimate entities, reducing the likelihood of deliberate defaults. From an operational risk perspective, robust verification systems minimize the chance of unauthorized transactions and identity theft. In the context of market risk, verified accounts help maintain market integrity by preventing market manipulation through fake accounts or coordinated fraudulent activities. The connection between financial risk and digital technology has become even more pronounced with the recent emergence of cryptocurrency and decentralized finance (DeFi), where distributed transactions pose novel challenges to traditional risk management frameworks [3].

2.2. Machine Learning in Financial Risk Classification

2.2.1. Definition of Classification for Financial Risk

Financial risk classification is generally a binary probabilistic determination process, where the outcome is based on the subject of interest (e.g., fraudulent or normal transaction, authentic or inauthentic login to bank accounts, etc.) [4]. Establishing a financial risk classification system is of great significance for financial institutions to implement risk management, as an accurate risk classification helps identify the risks and provides a solid basis for risk evaluation, control, and prevention work. Given the complexity and interconnectivity of financial markets, the types and manifestations of adversarial activities continue to evolve [5]. Traditional risk classification methods are no longer sufficient to adapt to these changes, and the use of cutting-edge technologies such as machine learning to dynamically monitor and classify financial risks can enhance the accuracy and effectiveness of financial risk classification [6].

2.2.2. Data Collection and Preprocessing

In the process of building a financial risk classification model based on machine learning, data collection and preprocessing are fundamental steps [7]. The effectiveness of financial risk classification relies on a massive amount of dimensional and factual data, which includes user account details, transaction history, login activities, device information, and many other aspects. The collection of data generally involves various channels such as bank transaction systems, payment interfaces, financial institutions, etc. The collected data is typical and can comprehensively map the behavioral patterns of various customer groups, providing sufficient information support for model training.

The initially collected data often contains impurities, incompleteness, or omissions, and must be preprocessed. Data purification is the first step, and the core is to remove useless or duplicate data, fill in missing data, and eliminate abnormal data. In the process of filling in missing values, methods such as average filling, interpolation, or completing based on the distribution characteristics of the data can be used. The handling of outliers is usually reliant on industry standards or based on the statistical distribution of historical data to filter out data records that are too extreme and illogical. Subsequently, the data needs to be standardized or normalized to eliminate interference between different units of measurement. The commonly used standardization methods include Z-score normalization and minimum-maximum value normalization, which help unify the values of different attributes into the same range and prevent some values from dominating the model training due to their large range. In the data preprocessing stage, feature selection and feature engineering explore the interrelationships and information gains between features, select features that are crucial for risk identification, reduce information redundancy, and improve the computational efficiency and prediction accuracy of the model [8].

During the development of a risk classification model, banks or financial institutions typically conduct preliminary data organization on customer account transaction information, removing erroneous data caused by operational errors and supplementing missing information. Through the process of data standardization, they are able to analyze user behavior more accurately and efficiently assign them to appropriate groups.

2.2.3. Model Selection, Training and Evaluation

For classification problems, selecting appropriate models and adjusting their parameters is particularly crucial, and financial risk classification has no exception [9]. Many machine learning techniques such as decision trees, SVM (Support Vector Machines), Random Forests, and Gradient Boosting Trees (GBT) are widely used, each with its unique advantages and applicable scenarios, as shown in Figure 2 below.

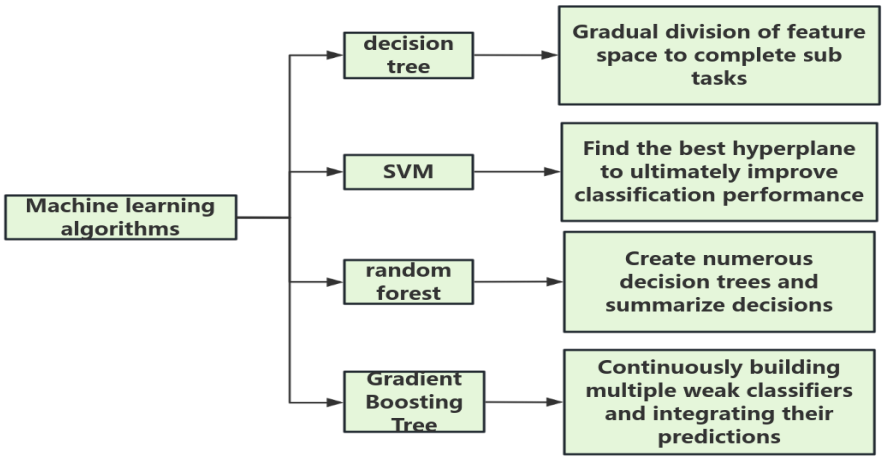

Figure 2. Machine Learning Algorithm.

Decision tree, as a classification algorithm based on a tree structure, completes classification tasks by dividing the feature space step by step. Nonetheless, this process is prone to overfitting, and usually requires pruning or ensemble learning strategies (such as in the random forest algorithm) to reduce the possibility of overfitting. The random forest algorithm enhances the robustness and accuracy of the model by creating numerous decision trees and summarizing their prediction results. Support Vector Machines (SVM) perform well on high-dimensional datasets, with the core of finding the optimal hyperplane to amplify the distance between different categories and improve classification performance. When facing nonlinear classification problems, SVM can use kernel functions (such as radial basis functions) to transform data into high-dimensional space for processing. Gradient Boosting Tree (GBT) gradually improves the accuracy of the model by continuously constructing multiple weak classifiers and integrating their predictions. This algorithm demonstrates strong fitting performance when dealing with complex nonlinear correlations in financial data.

After selecting the model, evaluation can be conducted by comparing the results against known truth labels and calculating the evaluation metrics. The most commonly used evaluation criteria involve accuracy, recall, precision, and F1 score. Monitoring the F1 score is particularly crucial when performing classification tasks such as credit risk assessment, as it can ensure a balance between false positives and false negatives during prediction, prevent missed judgments of high-risk customers, and avoid losses caused by financial risks. Having evaluation criteria is also instrumental to comparing model performances [10].

Next, adjusting the model's parameters based on the evaluation results is core to achieving optimal model performance. Commonly used optimization methods include grid search and random search. In the process of grid search, numerous parameter combinations are tested one by one to determine the optimal parameters, while random search randomly selects parameter combinations for experimentation. To avoid overfitting, cross validation is often used to evaluate the performance of each hyperparameter combination, which is aggregating the classification results on various validation data that are random subsets of training data held out from each training iteration.

2.2.4. Model Deployment

The optimized model may then be applied to specific business scenarios. As an example, in the loan review process banks use their model to predict delinquency likelihoods by analyzing factors such as the applicant's credit history and income status. Once the model identifies an applicant as a high-risk individual, the applicant may receive rejection of their loan application or be required to pay a higher interest rate [11]. Since the models are typically trained using certain cohorts of loan data, they need to be periodically updated and re-trained in order to capture the latest behavior patterns.

In summary, with high-quality training data and appropriate algorithms, financial risk classification models can provide powerful decision-making assistance for financial institutions, helping them make more accurate decisions in risk control.

3. Implementation of a Multimodal Machine Learning-Based Account Verification Strategy

In the field of financial risk management, with the continuous improvement of standards, account verification that used to rely solely on a single method (such as passwords or SMS verification codes) is no longer sufficient to meet the dual requirements of security and accuracy in the current financial system. Using multimodal data fusion technology to enhance account authentication has become an efficient response strategy [12]. This work hereby proposes a strategy that consolidates multidimensional information to achieve a more robust confirmation of user identity that can enhance the system's protection capabilities and trustworthiness. Similar to most financial risk classification systems, building

an account verification system with multimodal data fusion mainly involves data collection, feature extraction, and deployment, which is discussed below. Practical features such as alerting and self-adaptation are also explained in details.

3.1. Multimodal Data Collection and Feature Extraction

In the data collection process, various types of data need to be collected for verification through diverse channels, such as biometric information (such as fingerprints, vocal or facial features), user behavior records (such as the frequency of transaction occurrence, amount sizes), and device related information (including IP addresses, device unique identifiers). These data resources can provide a more comprehensive basis for account verification, improving the accuracy of the process.

In the feature extraction stage, deep learning (such as convolutional neural networks) shall be used to extract core attributes of biometric information. For user behavior information, statistical analysis techniques may be applied to obtain behavioral pattern features such as an empirical distribution. The acquisition of device information relies on network analysis tools to obtain attributes such as IP address and device type. The main purpose of this step is to translate unstructured data into features, eliminate irrelevant or redundant(correlated) attributes, and leave only the information that can add orthogonal value to establishing the user's true identity.

3.2. Abnormal Behavior Detection and Risk Warning

Monitoring abnormal user behavior and issuing early risk alerts constitute key points for preventing fraud and mitigating risks. Due to the rapid development of fraudulent methods, traditional rule-based alerting mechanisms cannot keep up with the speed of their changes. Machine learning based abnormal transaction monitoring technology, on the other hand, can extract abnormal signals more flexibly with the diverse user data collected, and issue risk alerts in a timely manner, therefore enhancing the security protection capability of the financial system [13].

In the process of monitoring abnormal behavior, the primary task is to find problems proactively: the model will first construct a "norm" of user behavior through in-depth analysis of these data, then classify abnormal behaviors that differ from the normal behavior pattern, and report with high confidence. The norm can be either some well established positive cases, or an empirical baseline. In the former case, common machine learning methods including clustering algorithms, Isolation Forests, and Support Vector Machines (SVM) can be used, and the reporting threshold can be determined by the desired F1 score/AUC, etc. When there are no viable examples, it is possible to use measures such as Euclidean distance between the observed data and known patterns, and the reporting threshold could be determined based on percentiles of the empirical distribution. For the behavior data points $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ and $x_j = (x_{j1}, x_{j2}, \ldots, x_{jn})$ of two users, the Euclidean distance formula is shown in formula (1).

$$d(x_i, x_j) = \sqrt{\sum_{k=1}^{n}(x_{ik} - x_{jk})^2} \quad (1)$$

Once abnormal activities are detected, the system will activate an alarm through the risk warning system and notify the relevant responsible persons to take necessary measures. As an example, if a user's trading behavior exhibits high and frequent characteristics, and these behaviors are highly comparable to that of known scams, or falling within the top 5% of the most extreme use cases, the system will classify them as abnormal activity and issue an alert to prompt financial institutions or users to perform identity verification or account locking operations.

3.3. Real-Time Model Update and Adaptive Adjustment Mechanism

In the deployment of machine learning systems for risk classification and account verification, real-time model adaptation is crucial for maintaining robust protection. Given the dynamic nature of financial transactions and the evolutionary characteristics of attack vectors, models must incorporate flexible adjustment mechanisms to adapt to these temporal changes. Through incremental learning and adaptive algorithms, the system can continuously update its classification boundaries and underlying probability distributions based on new transaction patterns and account behaviors across the user base. One effective approach is the stochastic gradient descent (SGD) for online learning, where model parameters are adjusted in real-time as new data points arrive. The objective is to minimize a loss function $L(\theta)$, where θ represents the d-dimensional parameters of the model. Perform real-time updates using formula (2).

$$\theta_{t+1} = \theta_t - \eta \nabla L(\theta_t) \quad (2)$$

where θ_t and θ_{t+1} respectively denote the parameter vectors at times t and $t+1$, $\eta > 0$ is the learning rate, and $\nabla L(\theta_t)$ represents the gradient of the loss function with respect to the parameters.

The time interval t can be defined based on specific system requirements, such as per-transaction or per-batch updates. To address the challenge of catastrophic forgetting and maintain model stability, the loss function can be augmented with regularization terms $\lambda R(\theta_t)$, where (θ_t) is a regularization function (commonly L1 or L2 norm), and λ controls the strength of regularization. This formulation helps prevent overfitting and ensures the model maintains good generalization performance even when processing high-velocity streaming data. The learning rate η can be adaptively adjusted using techniques such as AdaGrad or Adam to optimize the convergence properties of the online learning process. This adaptive mechanism ensures robust performance across varying data distributions and helps maintain model stability during sudden drift scenarios common in financial transaction patterns.

4. Conclusion

This article uses financial risks and machine learning concepts to conceptualize a strategy for account verification. This strategy relies on the fusion of heterogeneous data from multiple sources and parameter tuning of risk classification models. Combined with abnormal transaction monitoring and risk warning capabilities, it can greatly enhance the security of accounts. However, the model still needs to overcome challenges such as uneven data distribution and practical challenges in feature selection. Future research directions will focus on improving integration quality and algorithm robustness. Last but not least, given the rapid development of the financial field, the continuous updating and adaptive capabilities of the models will also become a focus of future iteration.

References

1. M. Murdock, N. Thanh, and R. Nivine, "The effect of state-level corruption on performance and risk of financial institutions," *J. Financial Crime*, vol. 30, no. 6, pp. 1784-1807, 2023, doi: 10.1108/JFC-09-2022-0237.
2. N. A. Karim et al., "Online Banking User Authentication Methods: A Systematic Literature Review," *IEEE Access*, vol. 12, pp. 741-757, 2024, doi: 10.1109/ACCESS.2023.3346045.
3. J. R. Jensen and O. Ross, "Managing Risk in DeFi," in *CEUR Workshop Proc.*, Aachen, 2020, doi: 10.2139/ssrn.3745568.
4. Y. Peng, G. Wang, G. Kou, and Y. Shi, "An empirical study of classification algorithm evaluation for financial risk prediction," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 2906-2915, 2011, doi: 10.1016/j.asoc.2010.11.028.
5. A. Adogame, "The 419 code as business unusual: youth and the unfolding of the advance fee fraud online discourse," *Asian J. Social Sci.*, vol. 37, no. 4, pp. 551-573, 2009, doi: 10.1163/156853109X460192.
6. A. Mashrur, W. Luo, N. A. Zaidi, and A. Robles-Kelly, "Machine Learning for Financial Risk Management: A Survey," *IEEE Access*, vol. 8, pp. 203203-203223, 2020, doi: 10.1109/ACCESS.2020.3036322.
7. C. Souza, "AI model risk: What the current model risk management framework can teach us about managing the risks of AI models," *J. Financial Compliance*, vol. 6, no. 2, pp. 103-112, 2023, doi: 10.69554/SOKX4074.

8. J. Fan and R. Li, "Statistical challenges with high dimensionality: Feature selection in knowledge discovery," *arXiv* preprint math, 2006, no. 0602133, doi: 10.4171/022-3.
9. M. A. Mezher, "Forecasting financial markets and credit risk classification using genetic folding algorithm," *Int. J. Electron. Banking*, vol. 3, no. 4, pp. 283-300, 2022, doi: 10.1504/IJEBANK.2022.128566.
10. A. Levy and R. Baha, "Credit risk assessment: A comparison of the performances of the linear discriminant analysis and the logistic regression," *Int. J. Entrepreneurship and Small Business*, vol. 42, no. 1-2, pp. 169-186, 2021, doi: 10.1504/IJESB.2021.112265
11. S. Shi et al., "Machine learning-driven credit risk: A systemic review," *Neural Comput. Appl.*, vol. 34, no. 17, pp. 14327-14339, 2022, doi: 10.1007/s00521-022-07472-2.
12. J. Yang et al., "Auto insurance fraud detection with multimodal learning," *Data Intell.*, vol. 5, no. 2, pp. 388-412, 2023, doi: 10.1162/dint_a_00191.
13. S. Boosa, "AI-powered risk management in fintech: Leveraging big data for fraud detection," *Int. J. Sci. Eng.*, vol. 10, no. 3, pp. 77-88, 2024, doi: 10.53555/ephijse.v10i3.262.