ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Research on artificial intelligence-driven internet payment risk control system

Jiaxin Zheng

Beihang University (BUAA) Al Quds Dist. Riyadh 13214 - 7470, 13214, Kingdom of Saudi Arabia

Abstract: With the popularization of digital payment, the importance of Internet payment risk management has become more and more significant. This paper begins with the principles and challenges of traditional Internet payment risk control systems and analyzes the limitations of existing systems in dealing with new payment frauds. Traditional methods rely on rules and pattern recognition, while emerging fraud technologies and complex financial environments have made these methods much less effective. The article further explores the application of AI technologies in risk control systems, especially how machine learning and deep learning can effectively improve the accuracy and efficiency of risk control. Through case studies, it demonstrates the process of AI wind control system in actual deployment and its significant advantages in detecting fraud and reducing the misjudgment rate. Finally, the article discusses the future development direction and potential application areas of AI risk control systems, pointing out their significant value in improving risk management capabilities and shortening response time.

Keywords: Internet payment; Risk control; Artificial intelligence

1. Introductory

With the rapid development of the Internet economy and the increasing frequency of e-commerce and online financial transactions, Internet payments have become an indispensable part of modern business activities. However, the popularity of Internet payments has also brought new challenges, especially in terms of payment security and risk management. With the diversification of Internet payment means and the continuous expansion of payment scenarios, the payment system faces increasingly complex security threats, including but not limited to identity theft, account fraud and transaction fraud and other forms of risk. In this environment, the traditional rule-based risk control system has been difficult to meet the needs of modern payment security[1].

2. Traditional internet payment risk control system and its challenges

Traditional Internet payment risk control systems are mainly based on rule engines and heuristics to identify and manage risks. The rule engine judges and screens transaction behavior by setting a series of predetermined conditions or criteria. For example, the risk control system may monitor the time frequency of transactions, such as the number of transactions for the same account shall not exceed 10 times in 24 hours, or more than 5 login attempts from the same IP address in a short period of time (e.g., within 15 minutes) will be regarded as abnormal behavior. These time periods are set based on historical data analysis of normal user behavior and potential fraud. Geographic location analysis is also a key risk control measure, where the system monitors and compares changes in the geographic location of the transaction location. If the system detects that a user's transaction activity occurs in two locations that are geographically very far apart within a short period of time (e.g., within one hour), this uncharacteristic rate of geographic movement will trigger a security alert. In addition, device fingerprinting

technology adds a layer of security by recognizing a user's device information[2].

While traditional risk control systems played a role in the early days of the Internet payment environment, the limitations of these systems are becoming increasingly apparent in the face of increasingly sophisticated and intelligent fraud tactics. Settings like fixed rules may not be able to cover all potential fraud scenarios, especially in the face of new or mutated fraud tactics, fixed rules often do not react flexibly enough. Excessive reliance on rules may lead to a high false alarm rate, i.e., normal transactions are misjudged as fraud, which not only affects the user experience, but also increases operational costs. And the efficiency and accuracy of traditional systems in processing big data also lags far behind AI-based methods, especially in real-time data processing and real-time risk assessment.

3. Artificial intelligence in risk control systems

3.1. Advantages of artificial intelligence technology in risk control

Artificial intelligence (AI) technology has been increasingly widely used in the Internet payment risk control system, especially machine learning (ML) and deep learning (DL) technologies have begun to play an important role in the field of risk management. The introduction of these technologies has greatly improved the efficiency and accuracy of the risk control system in the following aspects:

Pattern Recognition and Behavioral Analysis: machine learning and deep learning technologies excel at learning and recognizing complex patterns from large amounts of data. In a risk control system, these technologies can be used to identify subtle differences between normal transactions and fraudulent behavior[3].

Real-time data processing and decision making: AI systems can process real-time data streams and make decisions on the fly. Using streaming data processing and online learning algorithms, AI risk control systems can assess risk as soon as a transaction occurs, rather than relying on batch processing and after-the-fact analysis.

Adaptive learning capability: in contrast to traditional models, AI models are able to continuously learn and adapt themselves to new data. This means that AI risk control systems are able to adapt to new fraud tactics and strategies over time.

Deep feature engineering: deep learning models, especially convolutional neural networks (CNN) and recurrent neural networks (RNN), excel at feature extraction. These models automatically extract useful features from raw data, which is especially valuable when working with complex and high-dimensional transactional data.

Multimodal data fusion: In modern payment systems, transaction data may come from multiple sources and formats, including text, images, time-series data, etc. AI techniques, especially multimodal learning approaches, can integrate information from different data sources to provide a comprehensive risk assessment.

ISSN: 2424-8460(O)
2251-2608(P)

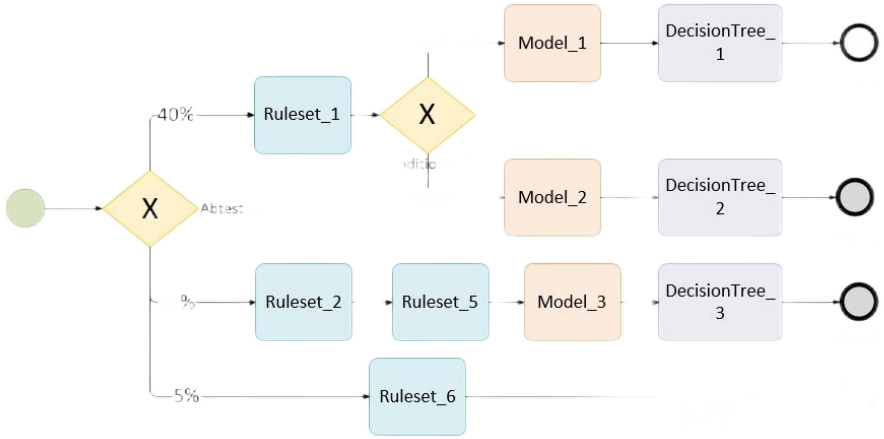

Figure 1. Artificial intelligence risk control decision engine system flow diagram

3.2. Mechanism and characteristics of the realization of artificial intelligence risk control system

The implementation mechanism of the AI risk control system is mainly based on advanced algorithms and big data technology, and it conducts in-depth analysis of user behavior, transaction patterns and their background environments through the comprehensive application of machine learning, deep learning, natural language processing and data analysis. On this basis, the AI risk control system makes use of its self-learning and self-adaptive capabilities to continuously optimize the risk identification model and improve the system's prediction accuracy and response speed. In practical application, the AI wind control system will first clean and standardize the input data through data preprocessing, which includes eliminating noisy data, processing missing values and normalizing the input format. Thereafter, the system will utilize various machine learning algorithms such as Decision Trees, Support Vector Machines (SVMs), and Integration Learning to perform the initial risk assessment. Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are then used to process more complex data structures, such as time-series data, in order to identify potential patterns of fraudulent behavior.

For example, by training a deep neural network model to analyze a customer's historical transaction data, the model is able to learn what kind of transaction behavior might indicate risk. Important technical parameters during model training include learning rate, batch size, and number of iterations, which directly affect the learning effect and predictive performance of the model. After the models are trained, the risk control system applies them in real-time trade monitoring, using real-time data streams to score each trade, and the scoring automatically decides whether to trigger an alert based on the risk level of the trade.Another notable feature of the AI risk control system is its adaptive adjustment mechanism, which means that the model is able to self-adjust and optimize itsel.

4. Optimizing SEO strategies to boost retail sales

4.1. The process of deploying an AI wind control system

Each step in the process of deploying an AI risk control system relies on strict technical parameters and standards to ensure the effectiveness and reliability of the system.

a) Data preparation and preprocessing: In this phase, data must be cleaned and standardized to fit the needs of the machine learning model. Specific operations include handling missing values, standardizing value ranges,

and coding categorical variables. For example, transaction amounts may need to be log-transformed to handle extreme values, while geolocation information needs to be converted to latitude/longitude format. In addition, splitting the dataset into a training set (typically 70%) and a test set (typically 30%) is also an important task in this phase.

b) Model development and training: Select appropriate machine learning algorithms (e.g., random forests, neural networks, or support vector machines) to construct the wind control model. During model training, key technical parameters include learning rate, batch size, and number of iterations. For example, a deep learning model might have a learning rate of 0.01, a batch size of 64, and 1000 iteration cycles performed during training. These parameters will be adjusted based on the model's performance on the validation dataset to optimize the model's accuracy and prevent overfitting.

c) Model validation and testing: After the model has been developed, its performance must be evaluated on an independent test set, and commonly used evaluation metrics include precision, recall, and AUC-ROC curves. These metrics quantify the model's ability to identify risky trades[4].

d) System Integration and Deployment: Integrate the trained model into an existing payment system, which usually involves API development to ensure that the model can receive transaction data and return risk assessment results in real time. System deployment also needs to take into account load balancing and data security to ensure system stability and transaction data security under high concurrency.

e) Monitoring and Maintenance: After deployment, the system needs to be constantly monitored to ensure its stable performance. Monitoring metrics include the response time of the model (millisecond response is usually required), changes in the accuracy rate, and so on. In addition, with the accumulation of new data and changes in fraud tactics, it is necessary to retrain and optimize the model on a regular basis.

4.2. Analysis of the current status and effect of the current application of AI risk control systems

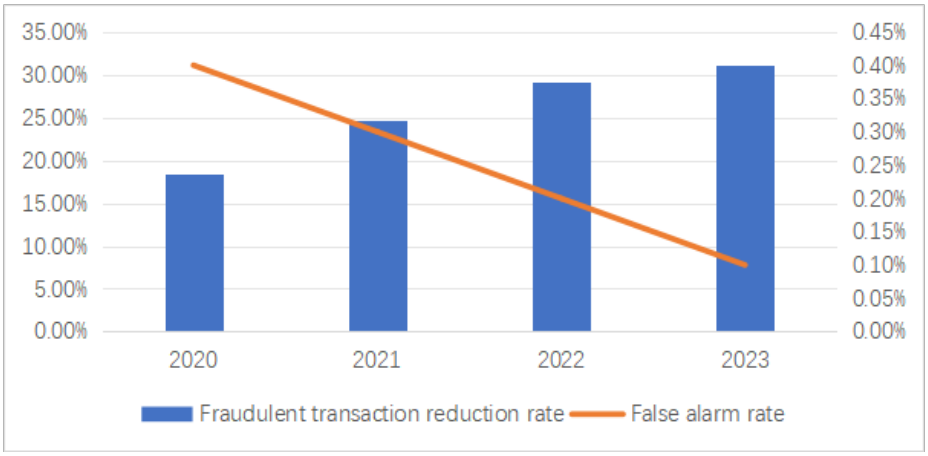

Figure 2. PayPal AI risk control system performance improvement effect.

(Source:PayPal internal risk control system annual report 2020-2023)

Over the past few years, with the popularization and optimization of AI risk control systems, some major financial service providers and payment platforms have received significant performance improvements. For example, PayPal managed to increase its fraudulent transaction detection rate to 97.5% in 2021 while reducing the false alarm rate to 0.3%, thanks to its adoption of deep learning algorithms, which are capable of learning

and recognizing complex consumer behavior patterns. The system has helped the company reduce fraudulent transactions by 30.2 percent globally since its launch in 2020, and has boosted the overall approval rate of transactions, which has increased to 94.8 percent from the previous 91.7 percent. The platform effectively identifies and stops potential fraud by analyzing hundreds of signals per transaction in real time, while maintaining an extremely low false block rate for legitimate transactions[5].

These figures not only show the effectiveness of AI risk control systems in improving detection accuracy and reducing operational costs, but also demonstrate how these technologies can help companies optimize the user experience and improve operational efficiency while safeguarding consumer security. Through these concrete examples, we can see that AI technology is gradually becoming a key driver in the field of financial risk control.

5. Concluding remarks

Through an in-depth discussion of the application of artificial intelligence technology in the Internet payment risk control system, and analyzes the deployment process, current application status, and actual effects of the AI risk control system.The AI risk control system has achieved significant results in improving the fraud detection rate, reducing the false alarm rate, and improving the efficiency of the operation, and in the future, with the advancement of the technology and the innovation of the data analysis methodology, it is expected that the AI risk control system will be even more intelligent and automated. At the same time, strengthening the interpretability and compliance of the AI decision-making process will also be a key development direction to ensure the fairness of the risk control system and customer trust.

References

[1] Simons K, Freeman K .USING ARTIFICIAL INTELLIGENCE to Support Harm Reduction Goals[J]. Professional Safety, 2024, 69(10): 47.

[2] Wang X, Huang " R, Sommer M , et al.The Efficacy of Artificial Intelligence-Enabled Adaptive Learning Systems From 2010 to 2022 on Learner Outcomes: A Meta-Analysis [J]. Journal of Educational Computing Research, 2024, 62(6): 1568-1603.

[3] Sebők M, Ring O, Kis G M, et al.The geopolitics of vaccine media representation in Orbán's Hungary—an AI-supported sentiment analysis [J].Journal of Computational Social Science, 2024, (prepublish): 1-24.

[4] Akutay S, Kaçmaz Y H ,Kahraman H .The effect of artificial intelligence supported case analysis on nursing students' case management performance and satisfaction: A randomized controlled trial[J].Nurse Education in Practice, 2024, 80104142-104142.

[5] Kara K ,Ergin A E , Yalçın C G , et al. Sustainable brand logo selection using an AI-Supported PF-WENSLO-ARLON hybrid method [J].Expert Systems With Applications, 2025, 260125382-125382.