KMAN PUBLISHING INSTITUTE
Journal Website

Article history:
Received 14 December 2025
Revised 06 February 2026
Accepted 15 February 2026
Published online 01 March 2026

Journal of Technology in Entrepreneurship and Strategic Management

Volume 4, Issue 4, pp 1-21

E-ISSN: 3041-8585

Detection of Suspicious Money Laundering and Fraudulent Financial and Banking Transactions Based on Deep Reinforcement Learning

Mehdi. Shakeri Behbahani[1], Mehdi. Sadeghzadeh[2*], Naser. Khani[1], Akbar. Nabiollahi[3]

[1] Department of Management, Na.C., Islamic Azad University, Najafabad, Iran
[2] Department of Computer Engineering, SR.C., Islamic Azad University, Tehran, Iran
[3] Department of Computer Engineering, Na.C., Islamic Azad University, Najafabad, Iran

*** Corresponding author email address**: Mehdi.sadeghzadeh@iau.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Shakeri Behbahani, M., Sadeghzadeh, M., Khani, N., & Nabiollahi, A. (2025). Detection of Suspicious Money Laundering and Fraudulent Financial and Banking Transactions Based on Deep Reinforcement Learning. *Journal of Technology in Entrepreneurship and Strategic Management*, *4*(4), 1-21.

A B S T R A C T

The present study aimed to develop a deep reinforcement learning-based model using neural networks to detect fraudulent and suspicious transactions in banking payment systems, with a focus on POS-based financial transactions. This applied case-study research was conducted using real transaction data from Bank Pasargad and the benchmark CCFD dataset. The research dataset included more than 250,000 real credit card transactions and 284,807 transactions from the benchmark dataset. A hybrid framework consisting of deep reinforcement learning, artificial neural networks, and autoencoder algorithms was employed for fraud detection. After preprocessing, normalization, and dimensionality reduction using the bottleneck method, the data were divided into training and testing subsets. Both supervised and unsupervised learning strategies were simultaneously implemented to improve anomaly detection and fraud classification performance. The proposed algorithms were implemented using R and Python machine learning libraries. The results obtained from the real transaction dataset demonstrated that the proposed model achieved excellent fraud detection performance with an AUC value of 0.999 and a Gini coefficient of 0.999. The final model correctly identified approximately 83% of fraudulent transactions and nearly 100% of legitimate transactions. Furthermore, evaluation on the CCFD benchmark dataset yielded an accuracy rate of 0.95 and a precision score of 0.97, indicating the model's strong capability in handling highly imbalanced datasets and identifying anomalous financial behaviors. The findings indicated that integrating deep reinforcement learning, neural networks, and autoencoder techniques provides an effective approach for detecting fraud in financial and banking transactions. The proposed framework not only improved fraud detection rates but also reduced classification errors and effectively managed imbalanced transaction data. Therefore, the model can serve as a reliable infrastructure for intelligent banking transaction monitoring and real-time fraud detection systems.

Keywords: *Fraud Detection, Deep Reinforcement Learning, Neural Networks, Autoencoder, Banking Transactions, Anomaly Detection*

Extended Abstract

Introduction

The rapid expansion of digital banking systems, electronic payment infrastructures, cryptocurrencies, and cross-border financial transactions has significantly transformed the global financial ecosystem. Alongside these developments, financial crimes—particularly money laundering and fraudulent banking activities—have evolved into increasingly sophisticated and adaptive threats. Traditional anti-money laundering (AML) systems, which primarily rely on rule-based monitoring and manual inspection, are no longer sufficient to detect complex and dynamically changing criminal patterns. The growing volume of financial data, coupled with the high similarity between legitimate and suspicious transactions, has made the identification of illicit activities considerably more challenging. Consequently, researchers and financial institutions have increasingly turned toward artificial intelligence, machine learning, and deep learning approaches to improve fraud detection accuracy and automate AML processes (Goecks et al., 2022). Studies have shown that intelligent systems are capable of identifying hidden patterns, detecting anomalies, and adapting to emerging criminal strategies more efficiently than conventional methods (Tsapa, 2023; Yusoff et al., 2023).

The application of machine learning and deep learning techniques in financial crime detection has attracted significant scholarly attention in recent years. Artificial intelligence-based approaches have demonstrated substantial potential in improving transaction monitoring, anomaly detection, and suspicious activity recognition (Alhajeri & Alhashem, 2023). In addition, explainable artificial intelligence and deep learning frameworks have enhanced the interpretability and operational effectiveness of anti-money laundering systems (Kute et al., 2021). Researchers have also highlighted the importance of integrating machine learning with graph analytics, blockchain technologies, and real-time transaction analysis to address increasingly complex money laundering schemes (Kurshan & Shen, 2020; Oad, Razaque, Tolemyssov, Alotaibi, Alotaibi, & Chenglin, 2021; Oad, Razaque, Tolemyssov, Alotaibi, Alotaibi, & Zhao, 2021). The emergence of cryptocurrency-related financial crimes has further intensified the need for intelligent detection systems capable of processing decentralized and highly interconnected transactional environments (Chitsungo, 2024). Advanced graph-based learning approaches have shown promising results in identifying suspicious cryptocurrency transaction networks and hidden laundering structures (Martins & Brito, 2023; Ouyang et al., 2024; Stefánsson et al., 2022).

Another critical challenge in financial fraud detection involves the highly imbalanced nature of banking transaction datasets. Fraudulent transactions generally represent only a very small proportion of total financial activities, causing many classification models to become biased toward legitimate transactions. To address this issue, recent studies have proposed imbalance mitigation strategies, semi-supervised learning models, active learning frameworks, and anomaly detection techniques (Aldahasi et al., 2024; Karim et al., 2024; Labanca et al., 2022). Machine learning algorithms have also been applied to suspicious transaction prediction and customer risk analytics with encouraging results (Lokanan & Maddhesia, 2023; Zheng, 2025). Furthermore, statistical learning models and intelligent agents have been developed to automate financial crime detection and improve the scalability of AML systems (Jensen & Iosifidis, 2023; Wang, 2022). Despite these advances, significant challenges remain regarding false-positive reduction, model adaptability, data imbalance, computational cost, and the continuous evolution of criminal behaviors (Akhtar et al., 2023; Husnaningtyas et al., 2023).

Given the growing importance of intelligent financial security systems, the present study aimed to develop a deep reinforcement learning-based framework integrated with artificial neural networks and autoencoder methods for detecting suspicious money laundering and fraudulent financial transactions within banking systems. The proposed model sought to improve fraud detection accuracy, reduce false classifications, and enhance anomaly detection performance in highly imbalanced financial datasets.

1 Methods and Materials

The present study was conducted using an applied and case-study research design focusing on banking transaction fraud and money laundering detection. The research utilized real financial transaction data obtained from a private banking institution as well as the benchmark CCFD dataset. The real-world dataset initially consisted of approximately 300,000 banking transactions collected from POS-based financial operations. Following data cleaning, preprocessing, and removal of irrelevant attributes, approximately 250,000 validated transactions remained for model development and evaluation. The benchmark CCFD dataset consisted of 284,807 European credit card transactions, including 492 fraudulent transactions, representing a highly imbalanced data distribution.

The proposed framework employed a hybrid architecture integrating deep reinforcement learning, artificial neural networks, and autoencoder-based anomaly detection. Data preprocessing included normalization, feature selection, categorical encoding, timestamp transformation, and dimensionality reduction. Because of the imbalanced nature of the datasets, special attention was given to minimizing false negatives and false positives. The dataset was divided into training and validation subsets using an 80/20 random split strategy. The training data were further separated into supervised and unsupervised learning subsets to support both labeled classification and anomaly discovery processes.

The unsupervised phase of the framework employed deep autoencoder models for anomaly detection and latent feature extraction. A bottleneck learning mechanism was implemented to reduce data dimensionality while preserving critical transaction characteristics. Hidden layers with compressed representations enabled the system to identify unusual behavioral patterns and distinguish anomalous transactions from legitimate ones. The supervised phase utilized neural network classification models initialized with pretrained autoencoder weights to enhance prediction accuracy and learning efficiency.

To implement the proposed framework, the R programming language was used for machine learning modeling and data mining operations, while Python libraries including TensorFlow and Scikit-learn were employed for additional experimental evaluation and benchmark comparisons. Performance evaluation metrics included accuracy, precision, sensitivity, F-measure, Gini coefficient, mean squared error (MSE), root mean squared error (RMSE), and area under the ROC curve (AUC).

Findings

The implementation of the proposed deep reinforcement learning framework on the real banking transaction dataset demonstrated highly promising results. The developed model successfully classified financial transactions into legitimate and fraudulent categories with a high level of precision. The performance evaluation metrics indicated strong predictive capability, with the model achieving an AUC value of 0.9995075 and a Gini coefficient of 0.9990149. The RMSE and MSE values also confirmed the robustness and stability of the proposed architecture.

The anomaly detection mechanism based on autoencoder learning and bottleneck dimensionality reduction significantly improved the identification of suspicious transactions. By reducing hidden feature

E-ISSN: 3041-8585

dimensions and extracting latent behavioral structures, the model enhanced its ability to distinguish abnormal transaction patterns from normal customer activities. The final model correctly identified approximately 83% of fraudulent transactions while accurately classifying nearly 100% of legitimate transactions. Increasing the prediction threshold from 0.5 to 0.6 improved classification reliability and reduced false-positive rates without significantly affecting fraud detection sensitivity.

The proposed framework was further evaluated using the benchmark CCFD dataset. Following normalization and balanced sampling procedures, the model was trained and tested on a reduced yet representative transaction subset. The results demonstrated that the proposed framework achieved an overall accuracy rate of 0.959, precision of 0.979, F-measure of 0.958, and sensitivity of 0.939. These findings indicate that the model maintained strong performance even under highly imbalanced transaction conditions.

The results also showed that integrating supervised and unsupervised learning approaches improved the model's ability to detect both known and previously unseen fraudulent behaviors. The deep reinforcement learning framework effectively adapted to complex transaction environments and demonstrated substantial capability in identifying anomalous financial activities that might remain undetected using traditional rule-based systems.

Discussion and Conclusion

The findings of the present study demonstrate that deep reinforcement learning combined with neural networks and autoencoder-based anomaly detection can provide an effective and intelligent solution for detecting money laundering and fraudulent banking transactions. The proposed framework successfully addressed several critical limitations of traditional anti-money laundering systems, particularly regarding imbalanced data processing, anomaly detection, and adaptive fraud identification. The high accuracy and precision achieved by the model indicate that intelligent learning-based approaches can substantially improve the efficiency of financial transaction monitoring systems.

One of the most important contributions of the present study lies in the integration of supervised and unsupervised learning strategies. While supervised learning enhanced classification precision for previously identified fraudulent behaviors, unsupervised anomaly detection enabled the system to identify emerging and previously unknown transaction patterns. This hybrid architecture increased the adaptability of the model in dynamic financial environments where criminal behaviors evolve continuously over time.

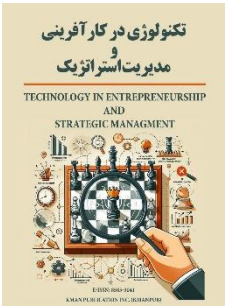
The findings further revealed that dimensionality reduction through bottleneck autoencoder structures significantly improved anomaly detection performance by extracting meaningful latent transaction features. The use of compressed hidden-layer representations enabled the model to identify subtle deviations in customer behavior while minimizing computational complexity. In addition, the proposed framework demonstrated strong capability in reducing false-positive classifications, which remains one of the major operational challenges in anti-money laundering systems.

The results obtained from both real banking transaction data and the benchmark CCFD dataset indicate that deep reinforcement learning models can maintain stable performance under highly imbalanced financial conditions. This is particularly important because fraudulent transactions typically constitute only a very small percentage of overall banking activities. The proposed system showed strong sensitivity in detecting suspicious activities while preserving high accuracy for legitimate transactions, thereby improving overall system reliability.

The increasing complexity of financial crimes, cryptocurrency-related laundering activities, and digital transaction networks highlights the necessity of deploying intelligent and adaptive financial security systems. The findings of the present study suggest that artificial intelligence-driven anti-money laundering frameworks can enhance banking security, strengthen customer trust, and reduce financial losses associated with fraud and illicit transactions. Furthermore, the scalability and flexibility of the proposed framework make it suitable for integration into real-time banking transaction monitoring infrastructures.

Overall, the present study confirms that deep reinforcement learning and intelligent anomaly detection models represent a promising direction for future anti-money laundering and fraud detection systems. As financial technologies continue to evolve, the implementation of adaptive machine learning frameworks capable of processing large-scale transaction data will become increasingly essential for maintaining financial integrity and combating sophisticated economic crimes.

E-ISSN: 3041-8585



شاپای الکترونیکی: ۳۰۴۱-۸۵۸۵

تکنولوژی در کارآفرینی و مدیریت استراتژیک

دوره ۴، شماره ۴، صفحه ۲۱-۱

MAN PUBLISHING INSTITUTE

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۲۳ آذر ۱۴۰۴
اصلاح شده در تاریخ ۱۷ بهمن ۱۴۰۴
پذیرفته شده در تاریخ ۲۶ بهمن ۱۴۰۴
منتشر شده در تاریخ ۱۰ اسفند ۱۴۰۴

کشف تراکنش‌های مشکوک به پولشویی و تقلب در تراکنش‌های مالی و بانکی بر مبنای یادگیری تقویتی عمیق

مهدی شاکری بهبهانی [۱]، مهدی صادق زاده [۲*]، ناصر خانی [۱]، اکبر نبی الهی [۳]

۱. گروه مدیریت، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران
۲. گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
۳. گروه مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

[*] **ایمیل نویسنده مسئول:** Mehdi.sadeghzadeh@iau.ac.ir

اطلاعات مقاله

نوع مقاله

پژوهشی اصیل

نحوه استناد به این مقاله:

شاکری بهبهانی، مهدی.، صادق زاده، مهدی.، خانی، ناصر.، و نبی الهی، اکبر. (۱۴۰۴). کشف تراکنش‌های مشکوک به پولشویی و تقلب در تراکنش‌های مالی و بانکی بر مبنای یادگیری تقویتی عمیق. *تکنولوژی در کارآفرینی و مدیریت استراتژیک*، ۴ (۴)، ۲۱-۱.

چکیده

هدف پژوهش حاضر ارائه یک مدل مبتنی بر یادگیری تقویتی عمیق و شبکه‌های عصبی برای شناسایی تراکنش‌های متقلبانه و مشکوک در سامانه‌های پرداخت بانکی با تأکید بر تراکنش‌های مبتنی بر دستگاه‌های POS بود. این پژوهش از نوع کاربردی و مطالعه موردی بود که بر روی داده‌های واقعی بانک پاسارگاد و مجموعه داده معیار CCFD انجام شد. داده‌های پژوهش شامل بیش از ۲۵۰ هزار تراکنش واقعی کارت‌های اعتباری و ۲۸۴۸۰۷ تراکنش در مجموعه داده معیار بود. برای طراحی مدل، از ترکیب یادگیری تقویتی عمیق، شبکه عصبی مصنوعی و الگوریتم خودرمزنگار استفاده شد. داده‌ها پس از پاکسازی، نرمال‌سازی و کاهش ابعاد با روش گلوگاه، به دو بخش آموزش و آزمون تقسیم شدند. در مرحله آموزش، مدل‌های با ناظر و بدون ناظر به صورت هم‌زمان به‌کار گرفته شدند تا توانایی کشف ناهنجاری و تشخیص تقلب افزایش یابد. پیاده‌سازی الگوریتم‌ها با استفاده از زبان‌های R و Python و کتابخانه‌های یادگیری ماشین انجام شد. نتایج اجرای الگوریتم بر روی داده‌های واقعی نشان داد که مدل پیشنهادی توانست با مقدار AUC برابر با ۰.۹۹۹ و مقدار Gini معادل ۰.۹۹۹ عملکرد بسیار مطلوبی در تشخیص تقلب ارائه دهد. همچنین مدل نهایی حدود ۸۳ درصد از تراکنش‌های متقلبانه و نزدیک به ۱۰۰ درصد از تراکنش‌های مجاز را به درستی شناسایی کرد. در مجموعه داده معیار CCFD نیز صحت الگوریتم برابر با ۰.۹۵ و دقت آن ۰.۹۷ به دست آمد که نشان‌دهنده توانایی بالای مدل در مدیریت داده‌های نامتوازن و شناسایی رفتارهای غیرعادی در تراکنش‌های بانکی بود. یافته‌های پژوهش نشان داد که ترکیب یادگیری تقویتی عمیق، شبکه‌های عصبی و خودرمزنگارها می‌تواند رویکردی کارآمد برای کشف تقلب در تراکنش‌های مالی و بانکی فراهم سازد. مدل پیشنهادی علاوه بر افزایش نرخ کشف تقلب، توانایی مناسبی در کاهش خطاهای تشخیص و مدیریت داده‌های نامتوازن دارد و می‌تواند به عنوان زیرساختی مؤثر برای سامانه‌های هوشمند نظارت بر تراکنش‌های بانکی مورد استفاده قرار گیرد.

کلیدواژگان: *تشخیص تقلب، یادگیری تقویتی عمیق، شبکه عصبی، خودرمزنگار، تراکنش بانکی، کشف ناهنجاری*

مقدمه

پیشرفت فناوری‌های مالی، توسعه بانکداری دیجیتال، گسترش تجارت الکترونیک و افزایش حجم تراکنش‌های برخط در دهه‌های اخیر، ساختار نظام‌های مالی و بانکی را به‌صورت بنیادین متحول کرده است. در کنار این تحولات، جرایم مالی نیز پیچیده‌تر، هوشمندتر و فراملی شده‌اند و پولشویی به‌عنوان یکی از مهم‌ترین تهدیدهای نظام مالی جهانی، به یکی از دغدغه‌های اصلی بانک‌ها، مؤسسات مالی، نهادهای نظارتی و دولت‌ها تبدیل شده است. پولشویی نه‌تنها موجب اخلال در شفافیت اقتصادی و افزایش فساد مالی می‌شود، بلکه می‌تواند بستر مناسبی برای تأمین مالی جرایم سازمان‌یافته، قاچاق، جرایم سایبری و فعالیت‌های غیرقانونی فراهم سازد. ازاین‌رو، توسعه سامانه‌های هوشمند برای شناسایی تراکنش‌های مشکوک و مقابله با پولشویی، به یکی از اولویت‌های اساسی حوزه بانکداری دیجیتال و امنیت مالی تبدیل شده است. (Goecks et al., 2022) بیان می‌کند که رشد فناوری‌های مالی و افزایش وابستگی نظام‌های بانکی به زیرساخت‌های دیجیتال، سبب شده است که روش‌های سنتی مقابله با جرایم مالی دیگر کارایی لازم را نداشته باشند. همچنین (Yusoff et al., 2023) تأکید می‌کند که فناوری‌های نوین داده‌محور و سامانه‌های هوشمند نقش کلیدی در ارتقای توان بانک‌ها برای مقابله با پولشویی و تقلب مالی ایفا می‌کنند. در همین راستا، (Akhtar et al., 2023) نیز اشاره می‌کند که افزایش پیچیدگی جرایم مالی در عصر دیجیتال، چالش‌های حقوقی و فناورانه گسترده‌ای را برای نظام‌های نظارتی ایجاد کرده است.

در گذشته، اغلب سامانه‌های ضدپولشویی بر مبنای قوانین ثابت، سناریوهای از پیش تعریف‌شده و نظارت انسانی فعالیت می‌کردند؛ اما با پیچیده‌تر شدن الگوهای مجرمانه، افزایش حجم تراکنش‌ها و تغییر مداوم رفتار مجرمان، این روش‌ها با محدودیت‌های جدی مواجه شدند. روش‌های مبتنی بر قواعد ثابت، توانایی محدودی در شناسایی الگوهای جدید و ناهنجاری‌های پیچیده دارند و اغلب منجر به افزایش نرخ هشدارهای کاذب می‌شوند. (Ahmed et al., 2021) نشان داد که سامانه‌های مبتنی بر قواعد معنایی اگرچه در شناسایی برخی الگوهای شناخته‌شده مؤثر هستند، اما در برابر الگوهای نوظهور و پویا با محدودیت مواجه می‌شوند. همچنین (Ketenci et al., 2021) بیان می‌کند که تغییرات زمانی و رفتاری در تراکنش‌های مالی سبب می‌شود الگوهای پولشویی به‌سرعت دگرگون شوند و سامانه‌های سنتی نتوانند به‌طور مؤثر با این تغییرات سازگار شوند. از سوی دیگر، (Lokanan, 2022) معتقد است که استفاده از ابزارهای بصری‌سازی و تحلیل الگوهای تراکنشی می‌تواند درک بهتری از شبکه‌های پولشویی ایجاد کند، اما همچنان نیاز به الگوریتم‌های هوشمند برای تحلیل داده‌های پیچیده احساس می‌شود. (Kurshan & Shen, 2020) نیز با تمرکز بر محاسبات گرافی در جرایم مالی، تأکید می‌کند که ساختار شبکه‌ای جرایم مالی و ارتباطات پنهان میان حساب‌ها و تراکنش‌ها، شناسایی دستی یا مبتنی بر قواعد سنتی را بسیار دشوار کرده است.

در چنین شرایطی، هوش مصنوعی، یادگیری ماشین و یادگیری عمیق به‌عنوان راهکارهایی نوین برای تحلیل داده‌های عظیم مالی و شناسایی الگوهای پنهان مورد توجه قرار گرفته‌اند. الگوریتم‌های یادگیری ماشین می‌توانند بدون نیاز به تعریف صریح قواعد، الگوهای مشکوک را از داده‌ها استخراج کنند و توانایی بالایی در تحلیل رفتارهای غیرعادی داشته باشند. (Alhajeri & Alhashem, 2023) بیان می‌کند که استفاده از هوش مصنوعی در سامانه‌های ضدپولشویی، موجب افزایش دقت شناسایی تراکنش‌های مشکوک و کاهش وابستگی به نظارت انسانی شده است. (Tsapa, 2023) نیز کاربردهای مختلف هوش مصنوعی در بانکداری ضدپولشویی را بررسی کرده و نشان داده است که الگوریتم‌های هوشمند قادرند رفتارهای پیچیده مالی را در زمان واقعی تحلیل کنند. افزون بر این، (Rouhollahi, 2021) اشاره می‌کند که هوش مصنوعی می‌تواند با تحلیل رفتار مشتریان و کشف روابط پنهان میان تراکنش‌ها، سامانه‌های کشف جرایم مالی را متحول سازد. (Kute et al., 2021)

E-ISSN: 3041-8585

نیز در مرور انتقادی خود بر کاربرد یادگیری عمیق و هوش مصنوعی توضیح‌پذیر در کشف پولشویی، بر اهمیت استفاده از مدل‌های قابل‌تفسیر برای افزایش اعتماد نهادهای مالی و نظارتی تأکید کرده است.

یکی از مهم‌ترین چالش‌های حوزه کشف پولشویی، عدم توازن شدید داده‌ها است؛ زیرا تعداد تراکنش‌های مشکوک در مقایسه با تراکنش‌های سالم بسیار اندک است. این موضوع سبب می‌شود بسیاری از الگوریتم‌های طبقه‌بندی، به سمت کلاس غالب متمایل شوند و توانایی مناسبی در شناسایی تراکنش‌های غیرقانونی نداشته باشند. (Ruchay et al., 2023) نشان داد که طبقه‌بندی نامتوازن تراکنش‌های بانکی، یکی از چالش‌های اساسی در طراحی سامانه‌های کشف تقلب است و استفاده از تکنیک‌های یادگیری ماشین پیشرفته می‌تواند این مشکل را کاهش دهد. همچنین (Aldahasi et al., 2024) با بررسی روش‌های کاهش عدم توازن داده‌ها در تشخیص تقلب مالی، نشان داد که استفاده هم‌زمان از الگوریتم‌های یادگیری ماشین و تکنیک‌های متعادل‌سازی داده‌ها، دقت سامانه‌های کشف تقلب را به‌طور معناداری افزایش می‌دهد. (Labanca et al., 2022) نیز چارچوبی مبتنی بر یادگیری فعال ارائه داد که در آن سامانه به‌صورت پویا داده‌های مهم‌تر را برای آموزش انتخاب می‌کند و این موضوع موجب افزایش کارایی در محیط‌های دارای داده نامتوازن می‌شود. در همین زمینه، (Lokanan & Maddhesia, 2023) با استفاده از الگوریتم‌های یادگیری ماشین برای پیش‌بینی تراکنش‌های مشکوک به پولشویی، نشان داد که مدل‌های هوشمند در شناسایی الگوهای غیرمعمول عملکرد مطلوبی دارند.

با ظهور رمزارزها و گسترش تراکنش‌های مبتنی بر بلاکچین، ابعاد جدیدی از پولشویی دیجیتال شکل گرفته است. ناشناس بودن نسبی تراکنش‌های رمزارزی، سرعت انتقال وجوه و ماهیت فرامرزی شبکه‌های بلاکچین، فرصت‌های جدیدی را برای مجرمان مالی ایجاد کرده است. (Chitsungo, 2024) بیان می‌کند که جرایم مبتنی بر رمزارزها، شامل پولشویی، تجارت غیرقانونی و جرایم سایبری، در سال‌های اخیر رشد چشمگیری داشته‌اند و مقابله با آن‌ها نیازمند راهکارهای فناورانه پیشرفته است. (Ouyang et al., 2024) با استفاده از یادگیری کنتراستی زیرگراف‌ها در شبکه بیت‌کوین، نشان داد که روش‌های یادگیری گراف می‌توانند الگوهای پیچیده پولشویی را با دقت بالایی شناسایی کنند. همچنین (Stefánsson et al., 2022) از یادگیری ماشین بدون ناظر برای شناسایی آدرس‌های مشکوک در بلاکچین بیت‌کوین استفاده کرد و نتایج موفقیت‌آمیزی به دست آورد. (Turner et al., 2020) نیز با تحلیل تراکنش‌های غیرقانونی بیت‌کوین، نشان داد که تحلیل شبکه‌ای و داده‌کاوی نقش مهمی در کشف فعالیت‌های مجرمانه در فضای رمزارزها دارند. افزون بر این، (Martins & Brito, 2023) تأکید می‌کند که تحلیل گراف تراکنش‌های رمزارزی با استفاده از الگوریتم‌های یادگیری ماشین، امکان کشف ساختارهای پیچیده پولشویی را فراهم می‌کند.

تحلیل شبکه‌ای و یادگیری گراف در سال‌های اخیر به یکی از مهم‌ترین رویکردهای پژوهشی در حوزه ضدپولشویی تبدیل شده است. برخلاف روش‌های سنتی که هر تراکنش را به‌صورت مستقل بررسی می‌کنند، روش‌های مبتنی بر گراف قادرند ارتباطات میان کاربران، حساب‌ها و تراکنش‌ها را تحلیل کنند و الگوهای پنهان شبکه‌ای را استخراج نمایند. (Karim et al., 2024) با ارائه روش‌های نیمه‌نظارتی مقیاس‌پذیر مبتنی بر یادگیری گراف، نشان داد که این تکنیک‌ها در کشف شبکه‌های پیچیده پولشویی عملکرد بسیار مناسبی دارند. همچنین (Dumitrescu et al., 2022) از تشخیص ناهنجاری در گراف تراکنش‌های بانکی برای کاربردهای ضدپولشویی استفاده کرد و به نتایج مطلوبی دست یافت. (Zheng, 2025) نیز با معرفی یادگیری تطبیقی گراف برای تحلیل ریسک مشتریان، نشان داد که داده‌های شبکه‌ای و پراکنده می‌توانند از طریق مدل‌های گرافی پیشرفته به‌صورت هوشمند تحلیل شوند. علاوه بر این، (Kurshan & Shen, 2020) معتقد است که محاسبات گرافی، آینده سامانه‌های کشف جرایم مالی را شکل خواهند داد؛ زیرا بسیاری از عملیات پولشویی در قالب شبکه‌های پیچیده و چندلایه انجام می‌شوند.

از سوی دیگر، کلان‌داده و تحلیل داده‌های عظیم مالی، بستر مناسبی برای توسعه سامانه‌های هوشمند ضدپولشویی فراهم کرده‌اند. بانک‌ها و مؤسسات مالی روزانه میلیون‌ها تراکنش را پردازش می‌کنند و استخراج دانش از این داده‌ها بدون استفاده از فناوری‌های هوشمند عملاً امکان‌پذیر نیست. (Jiao, 2023) بیان می‌کند که تحلیل کلان‌داده‌ها می‌تواند انطباق سامانه‌های بانکی با الزامات ضدپولشویی را بهبود بخشد و فرآیند نظارت مالی را کارآمدتر سازد. همچنین (Jensen & Iosifidis, 2023) نقش آمار و یادگیری ماشین را در مبارزه با پولشویی برجسته دانسته و تأکید می‌کند که مدل‌های داده‌محور نسبت به روش‌های سنتی، قدرت بیشتری در کشف رفتارهای مشکوک دارند. (Wang, 2022) نیز رویکردی مبتنی بر عامل‌های هوشمند ارائه کرده که می‌تواند به‌صورت خودکار الگوهای پولشویی را شناسایی و از وقوع جرایم مالی جلوگیری کند. افزون بر این، (Tan et al., 2024) با بررسی طرح‌های پولشویی چندکشوری، سامانه‌ای خودکار برای تشخیص فعالیت‌های غیرقانونی پیشنهاد کرده که قادر است تعاملات پیچیده بین‌المللی را تحلیل کند.

در کنار پیشرفت‌های فناورانه، پژوهشگران به اهمیت ترکیب فناوری‌های نوظهور مانند بلاکچین، تحلیل زمانی، یادگیری عمیق و یادگیری نیمه‌نظارتی نیز توجه کرده‌اند. (Oad, Razaque, Tolemyssov, Alotaibi, Alotaibi, & Zhao, 2021) و (Oad, Razaque, Tolemyssov, Alotaibi, Alotaibi, & Chenglin, 2021) روشی مبتنی بر بلاکچین برای اسکن تراکنش‌ها و کشف پولشویی ارائه کردند که امکان رهگیری بهتر تراکنش‌های مالی را فراهم می‌سازد. (Ketenci et al., 2021) از تحلیل زمان-فرکانس برای شناسایی فعالیت‌های مشکوک استفاده کرد و نشان داد که ویژگی‌های زمانی تراکنش‌ها می‌توانند اطلاعات ارزشمندی درباره رفتارهای غیرقانونی ارائه دهند. (Hampo et al., 2023) نیز سامانه‌ای مبتنی بر الگوریتم kNN برای کشف پولشویی طراحی کرد که عملکرد مطلوبی در طبقه‌بندی تراکنش‌ها داشت. علاوه بر این، (Japinye, 2024) در مرور عملکردی جامع خود نشان داد که ادغام یادگیری ماشین با سامانه‌های ضدپولشویی مبتنی بر رمزارز، موجب بهبود چشمگیر دقت شناسایی و کاهش هشدارهای کاذب می‌شود. (Nicholls et al., 2021) نیز در بررسی جامع خود درباره جرایم سایبری مالی، بر نقش یادگیری عمیق در مقابله با چشم‌انداز در حال تحول جرایم مالی تأکید کرده است.

اگرچه مطالعات متعددی در زمینه کاربرد هوش مصنوعی، یادگیری ماشین، یادگیری عمیق و تحلیل گراف در حوزه ضدپولشویی انجام شده است، اما همچنان چالش‌هایی نظیر تغییر مداوم الگوهای مجرمانه، پیچیدگی شبکه‌های مالی، عدم توازن داده‌ها، نرخ بالای هشدارهای کاذب، کمبود داده‌های برچسب‌گذاری‌شده و محدودیت تفسیرپذیری مدل‌ها پابرجاست. (Husnaningtyas et al., 2023) در مرور نظام‌مند خود بر سامانه‌های ضدپولشویی، تأکید می‌کند که ادغام یادگیری ماشین و یادگیری عمیق هنوز با چالش‌های اجرایی و عملیاتی فراوانی مواجه است. همچنین (Goecks et al., 2022) بیان می‌کند که بسیاری از مطالعات موجود هنوز در سطح آزمایشگاهی باقی مانده‌اند و انتقال آن‌ها به محیط‌های واقعی بانکی نیازمند پژوهش‌های کاربردی بیشتری است. افزون بر این، (Alkhalili et al., 2021) با تمرکز بر فیلترسازی فهرست‌های نظارتی نشان داد که استفاده از یادگیری ماشین در سامانه‌های ضدپولشویی می‌تواند نرخ خطا را کاهش دهد، اما همچنان نیاز به مدل‌های تطبیقی و هوشمند وجود دارد.

بنابراین، با توجه به رشد روزافزون تراکنش‌های مالی دیجیتال، پیچیده‌تر شدن روش‌های پولشویی، ناکارآمدی نسبی سامانه‌های سنتی، افزایش جرایم مبتنی بر رمزارزها و ضرورت استفاده از فناوری‌های هوشمند، طراحی و توسعه مدل‌های نوین مبتنی بر یادگیری ماشین و یادگیری عمیق برای کشف تراکنش‌های مشکوک و مقابله با پولشویی، از اهمیت ویژه‌ای برخوردار است؛ ازاین‌رو هدف پژوهش حاضر، ارائه مدلی هوشمند مبتنی بر یادگیری تقویتی عمیق و شبکه‌های عصبی برای کشف تراکنش‌های مشکوک به پولشویی و تقلب در تراکنش‌های مالی و بانکی است.

E-ISSN: 3041-8585

روش پژوهش

روش این پژوهش، روش مطالعه موردی است زیرا به طور ویژه بر روی تراکنش‌های بانک پاسارگاد تمرکز دارد. به دلیل ارتباط دانشگاه با بانک پاسارگاد و با توجه به نیازسنجی و جلساتی که از سمت شرکت صورت گرفت. این پژوهش کاملا با رویکرد عملیاتی برای بانک پاسارگاد انجام شد. پژوهش از نظر هدف از نوع کاربردی است زیرا نتایج آن برای آگاهی مدیران بانک از عوامل مؤثر بر میزان پذیرش خدمات بانکداری الکترونیکی توسط مشتریان کاربرد دارد و باعث رضایتمند مشتریان استفاده کننده از کارت و دستگاه POS می‌شود. پژوهش از نظر مکانی، بانک پاسارگاد که یکی از بانک‌های خصوصی جمهوری اسلامی ایران می‌باشد است. پژوهش از نظر روش در زمره پژوهشهای توصیفی پیمایشی است. زیرا به بررسی توزیع ویژگی‌های رفتاری مشتریان بانک مورد پژوهش پرداخته و نحوه ارتباط میان آنان را در چارچوب مشخص توصیف می‌کند. تا جامعه آماری پژوهشی شامل تمام تراکنش‌های کارت اعتباری مشتریان مرتبط با بانک خصوصی مورد پژوهش است که از درگاه POS استفاده می‌کنند.

همچنین هر چند شناسایی تقلب آسان نیست، روشهای گوناگونی برای شناسایی تقلب کارت‌های بانکی به کار گرفته میشود. اغلب روشهای استفاده شده در ادبیات موضوع مبتنی بر داده کاوی است. روش‌های داده کاوی به عنوان یکی از اصلی ترین ابزارهای شناسایی تقلب در کارتهای بانکی استفاده می‌شود هرچه حجم داده‌ها بیشتر و روابط میان آنها پیچیده نمی‌باشد دسترسی به اطلاعات نهفته در باندها مشکل تر می‌شود. لذا نقش داده کاوی یکی از روشهای کشف دانش، روشن تر می‌شود.

در این پژوهش از مجموعه داده‌های واقعی و مجموعه داده معیار CCFD استفاده شد. مجموعه‌ای داده‌های واقعی حدود ۳۰۰,۰۰۰ تراکنش بود که با توجه به موضوع پژوهشی داده‌ها پاکسازی شدند و از این مجموعه حدود ۲۵۰۰۰۰ مورد از تراکنش‌های کارتهای اعتباری باقیماند که برای هر تراکنش می‌توان مشخصی نمود که آیا تراکنش جعلی است یا نه مجموعه داده‌های نهایی اعتبار سنجی شده با توجه به مشورت با اهل فن برچسب گذاری شدند و به دو مجموعه سالم و متقلبانه تقسیم شدند. داده‌های مجموعه‌ای مانند این هنگام انجام یادگیری ماشین دارای رفتار خاصی هستند، زیرا آنها به شدت ناسازگار و نامتقارن میباشد. در این مورد مطالعه ۰.۱۰۱٪ از همه معاملات جعلی بوده و برچسب گذاری شدند، یعنی حجم بالایی از تراکنش‌ها سالم بودند و درصد پایینی متقلبانه بودند که این عدم تقارن باعث گمراهی مدل می‌شود.

مجموعه داده معیار CCFD شامل ۲۸۴۸۰۷ تراکنش میشود که در طی دو روز در سپتامبر ۲۰۱۳ توسط مشتریان اروپایی به ثبت رسیده اند. در این بین تعداد ۴۹۲ تراکنش وجود دارند که برچسب غیرقانونی داشته و در مجموع ۱۷۲/۰ درصد از کل تراکنش‌ها در مجموعه داده معیار را تشکیل میدهند که حاکی از عدم توازن شدید در این داده هاست. برای حفظ محرمانگی اطلاعات ویژگی‌های اصلی و اطلاعات پیش زمینه درباره آنها در اختیار قرار داده نشده اند. فقط ویژگی‌های عددی این مجموعه داده و آنهم بعد از ناشناس سازی در دسترس هستند.

هنگام برخورد با چنین عدم تعادل شدید در پایگاه داده در زمان اندازه گیری عملکرد مدل، باید مراقب بود ما اشتباه نشود یعنی مورد متقلبانه به اشتباه سالم تشخیص داده نشود و بالعکس مدل سالم به عنوان متقلبانه تشخیص داده شود که مورد دوم در نزد مشتریان بانک نمای بندتری دارد و رضایتمندی آن‌ها از کاهش خواهد دارد. از آنجا که فقط تعداد بسیار اندکی از موارد متقلبانه هستند مدلی که با دقت بالایی ۹۹٪ تراکنش‌های مجاز را شناسایی کند. با وجود دقت بالای آن چنین مدلی لزوما به ما کمک نمی‌کنند که موارد جعلی را با دقت بالا پیدا کنیم.

در چنین داده‌هایی ممکن است ما دچار پدیده پیش سرازش شوید وقتی در ینگ مدل، داده‌های آموزشی شامل ویژگی‌هایی با نویز با داده‌هایی با واریانس بالا باشد، باعث به وجود آمدن پدیده پیش سوارش می‌شود که این مین کلیه ساعت می‌گیرند شما مبدل بیش از چه

سینه داده‌های آموزشی وابسته شود و نتواند توزیعی را که داده‌های واقعی از آن تولید شده بودند را هندل کند. این مسئله سبب می‌گردد تا درستی مدل در پیش بینی داده‌هایی که در نمونه گیری وجود ندارند به شدت کاهش یابد و مدل را دچار گمراهی کنند.

برای حصول نتیجه روندی در ادامه توضیح داده میشود در پیش گرفته شد. ابتدا با مطالعه منابع کتابخانه‌ای به بررسی روند کلی کلیه کارهای انجام شده، نورسی چارچوب‌ها و الگور شیرهای موجود در زمینه کشف طلب پرداخته شد. کارهای گذشتگان مطالعه شد و الگوریتمها و روشهای استفاده شده توسط آنها بررسی شده و این روشها در مقالات خارجی و داخلی مقایسه شدند و از سوی دیگر انگور شیرهای روز گلشف ناهنجاری‌ها در داده‌های بزرگ مورد وارسی و مطالعه قرار گرفت تا با استفاده از تازه‌های علیم داده کاوی به انجام پژوهش پرداخته شود.

از انجایی که بانکداری در ایران و جهان کاملا متفاوت میباشد. مطالعات صورت گرفته در این زمینه به دو حوزه تقسیم شده و مورد بررسی قرار گرفت در مجموعه کارهای صورت گرفته در حوزه جهانی برای کشف تقلب کارهای زیادی صورت گرفته ولی مطالعه‌ای که با دقت بالا به این موضوع پرداخته باشد اندک است و در ایران هم با استفاده از علم یادگیری تقویتی عمیق به این موضوع پرداخته نشده بود. در نتیجه بر آن شدیم تا با استفاده از یادگیری تقویتی عمیق وارد این حوزه شویم

داده‌های اصلی پژوهش شامل تراکنش‌های ثبت شده کارتهای بانکی در پایگاه داده‌ای یکی از بانک‌های خصوصی داخلی کشور و با رعایت ملاحظات اخلاقی و با اخذ مجوز از آن بانک به دست آمد و از آن برای طراحی مدل شناسایی تقلب در کارتهای بانکی بهره جویی شد. لذا تراکنش‌های حدود ۸۶ هزار کارت در بازه زمانی تقریبی یک ماده با حدود بیش از ۲۵۰ هزار تراکنش استخراج شده است. همچنین جهت اعتبارسنجی و مقایسه نتایج پژوهش با مقالات دیگر، از مجموعه داده معیار CCFD استفاده شد.

با توجه به تعدد فیلدهای اطلاعاتی و کاربردی نبودن برخی از آن‌ها برای این پژوهش، پس از تحلیل آنها به کمک خبرگان و در نظر گرفتن تقلب‌های صورت گرفته و شناسایی فیلدهای تحت تأثیر تقلب‌های مختلف پارامترهای مؤثر در طراحی مدل پژوهش استخراج شد و فیلدهای ناکارا از پایگاه اطلاعاتی کنار گذاشته شد.

از طرف دیگر هم باید داده‌ها به فرمت قابل فهم الگوریتم التخابی تبدیل می‌شد. بنابر این فیلدهای تاریخی تبدیل و فیلدهای ملتی کدگذاری شد تا در زمان پردازش کار با داده‌ها آسان تر باشد. برای این منظور به دلیل حجم بالای داده از ابزارهای کار با داده‌های حجیم بهره برده شد.

در مرحله بعد به طرح ریزی و شناسایی سیستم مورد نظر و بررسی نیازهای سیستم و مشتری پرداخته و با ارزیابی زیر ساخت‌ها و امکانات موجود با طرح ریزی‌های ممکن پژوهش را انجام داده و با شناسایی اهداف و مقامت پروژه و محدودیت‌های پروژه و فرضیات و سیستم طراحی شده و مشخص گردید. که با استفاده الگوریتمهای حوزه یادگیری تقویتی عمیق به انجام کشف نقلب پرداخته خواهد شد و زبان برنامه نویسی برای پیاده سازی انگور شهرها انتخاب گردید.

در مرحله نیاز سنجی به تعریف نیازمندیهای پروژه و تحلیل داده‌ها پرداخته که به چه نوع اطلاعاتی نیاز داریم و چه گزارشانی لازم به طراحی است و نیاز به چه نوع گزارشانی داریم و داده‌ها را کاملا شناسایی کرده و داده‌ها تمیز شد و داده‌های غیر ضروری حذف گردید تا باعث گمراهی در روند کار نشود. در این مرحله ابتدا باید منابع داده خارجی تحلیل شوند که شامل تعیین موجودیتها و ارتباطات از هر داده خارجی و اضافه نمودن موجودیت‌ها میباشد. مدل داده منطقی که در مراحل قبل بدست آمده اند را تحلیل کرده و بهبود داده شد.

E-ISSN: 3041-8585

در نهایت هم با توجه به یافته‌های پژوهش به نتیجه گیری درباره موضوع پرداخته شد. مرحله کشف الگوهای مهم با در نظر گرفتن یک حد آستانه میباشد نتایج این مرحله به پروفایلهای تجمعی کاربر تبدیل می‌شوند که برای استفاده در بخش توصیه مناسب میباشد. در این مرحله به تجزیه و تحلیل الگوهای بدست آمده و استفاده از الگوهای کشف شده برای شناسایی رفتار مشکوک می‌پردازند.

برای ایجاد مدل شناسایی تقلب در تراکنش‌های کارتهای اعتباری بانکی یک متغیر افراز ایجاد شد تا بتوان داده‌ها را به دو بخش آموزش و اعتبار سنجی تقسیم بندی کرد به واسطه تعریف متغیر افراز و انتخاب داده‌هایی که برای آموزش و آزمون استفاده خواهند شد از مجموع ۲۵۶,۵۵۹، داده، ۲۰۵,۲۴۶ داده (۸۰ درصد) برای آموزش و ایجاد مدل اختصاص یافت و ۵۱,۳۱۳ داده ۲۰ درصد برای اعتبار سنجی مدل به صورت تصادفی تخصیص داده شد. از مجموع ۲۰۵,۲۴۶ داده‌های آموزشی که به دو قسمت مساوی (۱۰۲,۶۲۳) تقسیم شد ۴۰ درصد از کل داده برای داده آموزشی با ناظر (سرپرست) و ۴۰ درصد باقی مانده از کل داده داده آموزشی بدون ناظر تعیین شد.

برای مدل سازی از یادگیری تقویتی عمیق از شبکه عصبی استفاده و مجموعه داده‌ها به مجموعه‌های آموزش و تست تقسیم شد. از آنجا که قرار شد یک مدل پیش آموزش دیده با ناظر بررسی شود، داده‌ها به دو مجموعه آموزش جداگانه و یک مجموعه آزمون مستقل برای مقایسه مدل نهایی تقسیم شد.

در مرحله اول مدل شبکه عصبی بدون ناظر با استفاده از آموزش عمیق خود رمزگذارها آموزش داده شد و در ادامه، یک تکنیک به نام متد آموزش گلوگاه اجرا شد، گلوگاه به جایی در شبکه میگویند که لایه مخفی در میانه شبکه عصبی بسیار کوچک است. این به این معنی است که مدل مورد بحث اندازه داده‌های ورودی را کاهش دهد در این مورد مطالعه تا ۲ گره یا بعد کاهش یافته است.

مدل خودرمزنگار، الگوهای داده‌های ورودی را بدون در نظر گرفتن برچسبهای داده، یاد می‌گیرد. در این مورد باید یاد بگیرد که کدام تراکنش‌های کارت اعتباری شبیه هستند و کدام تراکنش‌ها بی نظیر هستند یا ناهنجاری‌ها هستند باید در نظر داشت که مدلهای خود رمزنگار در داده‌های نامتقارن بسیار پیچیده و حساس هستند که ممکن است الگوهای غیر معمول را شناسایی کنند و ما را گمراه کنند.

در مرحله بعد به کاهش اندازه داده با لایه‌های پنهان پرداخته شد. از آنجایی که از مدل گلوگاه با دو گره در لایه مخفی و در میانه مدل شبکه عصبی استفاده شده است میتوانیم از این کاهش اندازه داده، برای کشف فضای ویژگی‌ها استفاده شود مشابه آنچه که میتوان با تجزیه و تحلیل مولفه اصلی انجام داد) می‌توانیم این ویژگی لایه‌های پنهان را از عملکرد الگوریتم استخراج کرد و آن را برای نمایش داده‌های ورودی استفاده نمود.

برای پیاده سازی الگوریتم از زبان برنامه نویس R استفاده شد که در این راستا از کتابخانه‌های مربوط به داده کاوی و یادگیری ماشین که در این زبان مورد استفاده قرار میگیرد استفاده شده است.

یافته‌ها

برای مدلسازی از یادگیری تقویتی عمیق با شبکه عصبی استفاده شد که برای کشف ناهنجاری در داده از الگوریتمهای شناسایی ناهنجاری مانند خودرمزنگار استفاده شد و مجموعه داده‌ها به مجموعه‌های آموزش و تست تقسیم شد. از آنجا که قرار شد یک مدل پیش آموزش دیده با ناظر بررسی شود، داده‌ها به دو مجموعه آموزش جداگانه، یکی برای آموزش مدل با ناظر و دیگری برای آموزش مدل بدون ناظر در نظر گرفته شد و یک مجموعه آزمون مستقل برای مقایسه مدل نهایی تقسیم گردد.

در مرحله اول، مدل شبکه عصبی بدون ناظر با استفاده از آموزش عمیق خود رمزنگارها آموزش داده شد و در ادامه، یک تکنیک به نام متد آموزش گلوگاه اجرا شد، گلوگاه به جایی در شبکه میگویند که لایه مخفی در میانه شبکه عصبی بسیار کوچک است. این به این معنی

است که مدل مورد بحث، اندازه داده‌های ورودی را کاهش دهد. در این مورد مطالعه، تا ۹ گره یا بعد کاهش یافته است(. کاهش بعد داده‌ها باعث میشود داده‌های ناهنجار با واریانس بالا با دقت بیشتری شناسایی شوند.

مدل خودرمزنگار، الگوهای داده‌های ورودی را بدون درنظرگرفتن برچسب‌های داده، یاد میگیرد. در این مورد باید یاد بگیرد که کدام تراکنش‌های کارت اعتباری شبیه هستند و کدام تراکنش‌ها بی نظیر هستند یا ناهنجاریها هستند.

باید در نظر داشت که مدلهای خودرمزگذار در داده‌های نامتقارن بسیار پیچیده و حساس هستند، که ممکن است الگوهای غیرمعمول را شناسایی کنند و ما را گمراه کنند. به این دلیل از متد گلوگاه استفاده شد تا دقت شناسایی را با کاهش بعد لایه‌های پنهان بالا ببرد. روش گلوگاه با کاهش اندازه ورودی مدل این مهم را میسر میسازد. با پردازش داده‌ها در ۵ لایه با استفاده از الگوریتم نامبرده داده‌های زیر بدست آمد.

layer	units	type	dropout	l1	l2	mean_rate	rate_rms	momentum
1	34	Input	0.00 %					
2	10	Tanh	0.00 %	0.000000	0.000000	0.709865	0.320108	0.000000
3	2	Tanh	0.00 %	0.000000	0.000000	0.048458	0.109033	0.000000
4	10	Tanh	0.00 %	0.000000	0.000000	0.164717	0.192053	0.000000
5	34	Tanh		0.000000	0.000000	0.369681	0.425672	0.000000

روش‌های مختلفی برای شناسایی ناهنجاری وجود دارد که می‌توان به سیستم‌های تشخیص مبتنی بر قانون یا مبتنی بر یادگیری ماشین اشاره کرد. سیستم‌های مبتنی بر قانون، معمولا با تعریف قوانینی که انحراف را توصیف می‌کنند و آستانه‌ها و محدودیت‌ها را تعریف می‌کنند طراحی شده است. به عنوان مثال، چیزی که بالاتر از آستانه یا پایین است به عنوان یک ناهنجاری طبقه بندی می‌شود.

یکی از تکنیکهایی که در اینجا نشان داده میشود این است که با استفاده از یادگیری تقویتی عمیق وفریم‌های داده شناسایی شوند. در ادامه مدل الگوریتم خودرمزنگار H2O تحت نظارت پیش آموزش دیده شده را بررسی کرده و سپس از مدل خودرمزنگار به عنوان ورودی از قبل آموزش دیده، برای یک مدل تحت نظارت استفاده خواهد شد. در اینجا، دوباره از یک شبکه عصبی استفاده شده است. این مدل از وزن مدل خودرمزنگار برای تنظیم گره‌های مدل استفاده کرده است.

از اجرای الگوریتم یادگیری تقویتی عمیق بر روی داده‌ها برای پیش بینی تقلب خروجی زیر دست آمد که این نتیجه با استفاده از آموزش داده‌ها با فریم داده‌های از پیش آموزش داده شده حاصل شد و قابل ذکر است که برای پیش بینی از خودرمزنگار استفاده شده است.

جدول ۱

نتیجه اجرای الگوریتم

میعار اندازه گیری کارایی	MSE	RMSE	AUC	Gini
مقدار بدست آمده	۰.۰۱۵۰۰۲۱۱	۰.۱۲۳۴۸۳۱	۰.۹۹۹۵۰۷۵	۰.۹۹۹۰۱۴۹

در نتیجه داده‌های واقعی و پیشبینی شده به قرار زیربدست میآید.

E-ISSN: 3041-8585

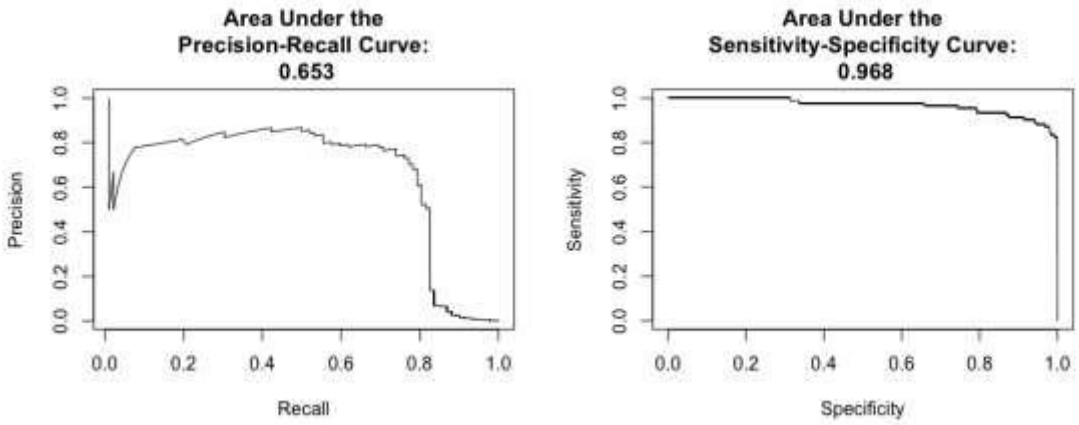
actual	predict	freq
0	0	0.997881057
0	1	0.002118943
1	0	0.173913043
1	1	0.826086957

با این روش نتیجه بهتری بدست آمد. آنچه از نمودار ۱ نمایان است، این است که ۷۰ درصد از موارد تقلب از دست داده شده، اما برای تعداد زیادی از موارد مجاز طبقه بندی به درستی انجام شده است. در حقیقت، اکنون اعتماد بیشتری میتوان به مدل داشت زیرا پارامترهای مدل دقیقتر طراحی شدند، به عنوان مثال، زمان‌هایی که برای جستجو در شبکه برای بهینه سازی پارامترها، بازگشت به ویژگی‌های اصلی و تلاشهایی که برای محاسبه ویژگی‌ها و الگوریتم‌های مختلف صرف شد موثر واقع شدند.

اندازه گیری عملکرد مدل در داده‌های بسیار نامتعادل صورت گرفته است و با توجه به اینکه شناسایی موارد مجاز از حساسیت بالایی برخودار است، نمیتوان از معیارهای عملکرد مانند دقت و یا سطح زیر منحنی استفاده کرد، زیرا نتایج بسیار خوشبینانه را براساس درصد بالایی از طبقه بندی‌های صحیح طبقه AUC اکثریت ارائه میدهند.

شکل ۱

ارزیابی نهایی مدل



در نمودار ۱ دو شاخص حساسیت و صحت برای ارزیابی مدل نمایش داده شده استت. از آنجایی که اطلاعات مدل به دو قسمت متقلبانه و مجاز تقسیم می‌شود می‌توان برای ارزیابی مدل از نمودارهای حساسیت و صحت استفاده نمود. زیرا این نمودارها برای مدلهای دودویی کاربرد دارند.

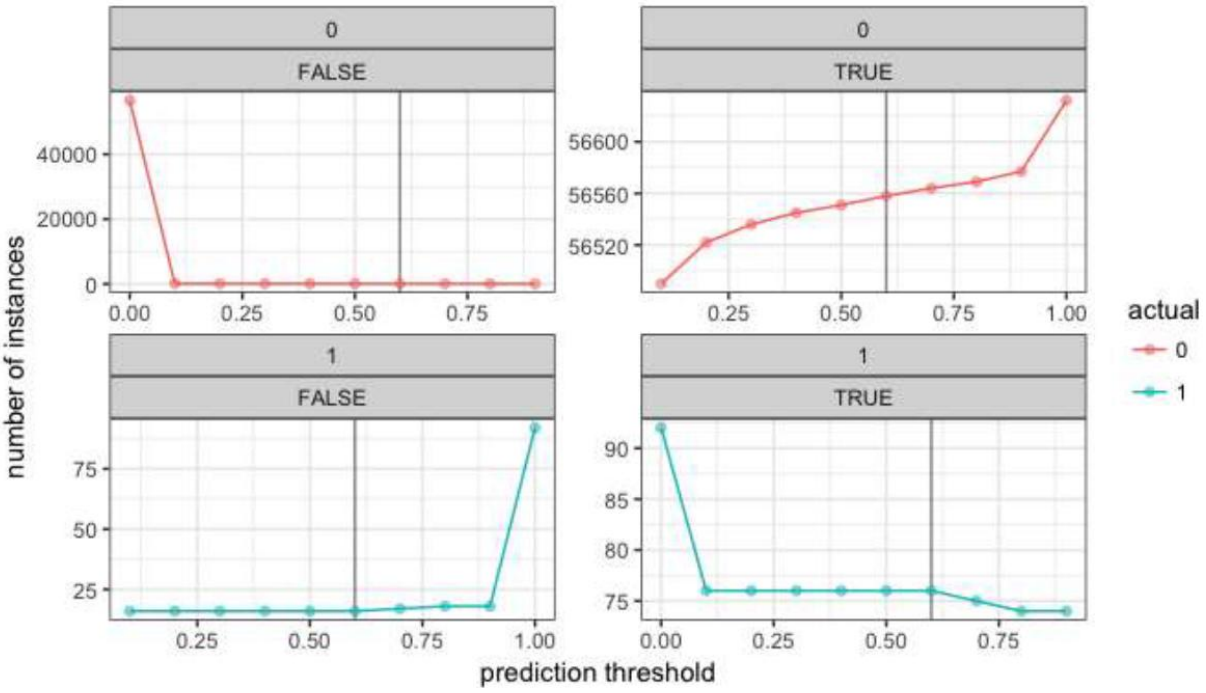
صحت، در این مدل نسبت موارد مورد آزمایش پیش بینی شده متقلبانه که در واقع جعلی هستند بیان میشود یعنی همان پیش بینی‌های مثبت واقعی، در حالی که حساسیت، نسبت موارد سالم است که به عنوان غیرمتقلبانه شناخته شدها ند. و مشخصه یا ویژگی نسبت موارد غیر تقلب است که به عنوان عدم تقلب شناخته شده است.

منحنی یادآوری صحت نسبت تقلب واقعی به موارد تقلب که شناسایی شده است را نشان می‌دهد. به عنوان مثال مواردی از تقلب، و همچنین مواردی از موارد مجاز که پیش بینی کرده ایم که تقلب است و بالعکس. منحنی حساسیت به این ترتیب ارتباط بین دسته بندی‌هایی

که به درستی شناسایی شده برای هر دو برچسب را بیان میکند یعنی اینکه ما موارد تقلب را به درستی تقلب پیش بینی کرده باشیم و موارد مجاز را هم به درستی مجاز تشخیص داده باشیم. همچنین می‌توان با نگاهی متفاوت به این مسئله و دقت بته آستانه‌های پیش بینی‌های مختلف و محاسبه تعداد موارد درست در دو کلاس، داده‌ها را طبقه بندی کرد.

شکل ۲

نمودارهای حساسیت و دقت نتیجه مدل



این نمودار نشان می‌دهد که می‌توان تعداد موارد به درستی طبقه بندی شده موارد غیرتقلب را بدون از بین بردن موارد طبقه تقلب، درست طبقه بندی کرد، هنگامی که آستانه پیش بینی را از پیش فرض ۰.۵ تا ۰.۶ افزایش داد. و در آخر مدل نهایی به درستی ۸۳ ٪ موارد تقلب و تقریبا ۱۰۰ ٪ موارد غیر تقلب را شناسایی کرده است.

در این بخش عملکرد شبکه عمیق پیشنهادی را بررسی و ارزیابی خواهیم کرد بدین منظور از مجموعه داده معیار CCFD بهره خواهیم گرفت که از آدرس learning/creditcard قابل دسترس است. این مجموعه داده شامل ۲۸۴۸۰۷ تراکنش میشود که در طی دو روز در سپتامبر ۲۰۱۳ توسط مشتریان اروپایی به ثبت رسیده اند. در این بین تعداد ۴۹۲ تراکنش وجود دارند که برچسب غیرقانونی داشته و در مجموع ۱۷۲/۰ درصد از کل تراکنش‌ها در مجموعه داده معیار را تشکیل میدهند که حاکی از عدم توازن شدید در این داده هاست. برای حفظ محرمانگی اطلاعات ویژگی‌های اصلی و اطلاعات پیش زمینه درباره آنها در اختیار قرار داده نشده اند. فقط ویژگی‌های عددی این مجموعه داده و آنهم بعد از ناشناس سازی در دسترس هستند. این ویژگی‌های عددی که با اعمال تحلیل عناصر اصلی (PCA) بر روی ویژگی‌های اصلی مجموعه داده معیار به دست آمده اند با برچسبهای V۱ تا V۲۸ نشانه گذاری شده.اند تنها ویژگی‌هایی که با PCA تغییر نیافته اند، زمان و میزان تراکنش هستند. ویژگی زمان نشانگر تعداد ثانیه‌های سپری شده بین هر تراکنش با تراکنش و اول در مجموعه داده معیار است. ویژگی

E-ISSN: 3041-8585

کلاس بیان کننده متغیر پاسخ یا برچسب هر تراکنش است درصورتی که تراکنش غیرقانونی باشد مقدار یک را به خود میگیرد و در صورت قانونی بودن مقدار صفر را خواهد داشت.

لازم به ذکر است که برای انجام آزمایشهای عددی ارائه شده در این بخش از کتابخانه‌های scikit learn- و tensorflow در زبان پایتون کمک گرفته شده است.

زمان آموزش شبکه عمیق پیشنهادی بر روی کامپیوتری با یک پردازنده چهار هسته‌ای با قدرت پردازش ۳/۳ گیگاهرتز و چهار گیگابایت رم در حدود یک دقیقه است بعلاوه خوانندگان میتوانند برای دسترسی به شبکه آموزش داده شده نهایی با نویسندگان مقاله مکاتبه نمایند.

برای آماده سازی دادگان ابتدا تمامی ۳۰ ویژگی یاد شده شامل ویژگی‌های ۱V تا ۲۸V زمان و میزان و تراکنش به صورت مجزا نرمال میشوند بدین ترتیب که میانگین هر ویژگی از هر عنصر آن کاسته شده حاصل بر انحراف استاندارد آن ویژگی تقسیم میشود. سپس با استفاده از نمونه برداری محدود یک مجموعه داده متوازن شده متشکل از ۹۸۴ تراکنش به دست میآید. بدین منظور ابتدا ۴۹۲ تراکنش قانونی به تصادف از مجموعه تراکنش‌های قانونی انتخاب میشوند و سپس با ۴۹۲ تراکنش غیرقانونی موجود در مجموعه داده معیار ترکیب میگردند تا مجموعه دادهای متوازن با نسبت ۵۰ درصد از دو نوع تراکنش حاصل گردد. در ادامه این مجموعه داده متوازن شده به صورت تصادفی و با نسبت ۷ به ۳ به مجموعه دادگان یادگیری و آزمون تقسیم بندی میگردد. بدین ترتیب تعداد ۶۸۸ تراکنش برای یادگیری و تعداد ۲۹۶ تراکنش برای آزمون الگوریتم پیشنهادی مورد استفاده قرار خواهند گرفت.

مطابق نتایج به دست آمده میزان صحت این الگوریتم ۰.۹۵ و میزان دقت آن ۰.۹۷ محاسبه میگردد که نشان از عملکرد قابل قبول این الگوریتم دارد.

جدول ۲ عملکرد این الگوریتم را بر روی دادگان آزمون با استفاده از شاخص‌های حساسیت یا یادآوری، دقت، معیار F و صحت نشان میدهد. حساسیت بیانگر توانایی کشف یک مورد تراکنش غیرقانونی است به شرط آنکه واقعاً غیرقانونی باشد. به عبارت دیگر حساسیت نسبت تراکنش‌های غیرقانونی درست تشخیص داده شده تعداد مثبت (درست به کل تراکنش‌های غیرقانونی (مجموع مثبت درست و منفی نادرست است. دقت نسبت تراکنش‌های غیرقانونی درست تشخیص داده شده (تعداد مثبت درست) به کل تراکنش‌هایی است که غیرقانونی تشخیص داده شده اند مجموع مثبت درست و مثبت نادرست). معیار F، میانگین هارمونیک حساسیت و دقت است و صحت نسبت پیش بینی‌هایی است که درست تشخیص داده شده اند. همان طور که در این جدول دیده میشود عملکرد الگوریتم پیشنهادی در تمامی معیارها مذکور قابل قبول است.

جدول ۲

مقایسه عملکرد الگوریتم پیشنهادی

الگوریتم	صحت	دقت	معیار F	حساسیت
الگوریتم پیشنهادی	۰.۹۵۹	۰.۹۷۹	۰.۹۵۸	۰.۹۳۹

بحث و نتیجه‌گیری

یافته‌های پژوهش حاضر نشان داد که استفاده از یادگیری تقویتی عمیق، شبکه‌های عصبی و الگوریتم‌های خودرمزنگار در شناسایی تراکنش‌های مشکوک به پولشویی و تقلب مالی، عملکرد قابل‌قبولی دارد و می‌تواند با دقت بالا، الگوهای غیرعادی و رفتارهای متقلبانه را در میان حجم عظیم تراکنش‌های بانکی شناسایی کند. نتایج حاصل از اجرای مدل بر روی داده‌های واقعی و مجموعه داده معیار نشان داد که مدل پیشنهادی توانسته است نرخ بالایی از تراکنش‌های متقلبانه را شناسایی کند و هم‌زمان میزان خطا در تشخیص تراکنش‌های سالم را کاهش دهد. این موضوع نشان می‌دهد که استفاده از مدل‌های ترکیبی مبتنی بر یادگیری عمیق می‌تواند محدودیت‌های روش‌های سنتی مبتنی بر قواعد ثابت را تا حد زیادی برطرف کند. نتایج پژوهش حاضر با یافته‌های (Goecks et al., 2022) همسو است؛ زیرا این پژوهش نیز نشان داد که سامانه‌های مبتنی بر یادگیری ماشین و یادگیری عمیق نسبت به رویکردهای سنتی عملکرد دقیق‌تر و انعطاف‌پذیرتری در کشف جرایم مالی دارند. همچنین یافته‌های مطالعه حاضر با نتایج (Yusoff et al., 2023) هماهنگ است که بر نقش فناوری‌های داده‌محور در افزایش توان سامانه‌های ضدپولشویی تأکید کرده بود. افزون بر این، (Alhajeri & Alhashem, 2023) نیز بیان می‌کند که استفاده از هوش مصنوعی در حوزه مبارزه با پولشویی می‌تواند سرعت و دقت شناسایی فعالیت‌های غیرقانونی را افزایش دهد که این موضوع با نتایج به‌دست‌آمده در پژوهش حاضر مطابقت دارد.

یکی از مهم‌ترین یافته‌های پژوهش حاضر، توانایی مدل در مدیریت داده‌های نامتوازن و کاهش خطاهای طبقه‌بندی بود. در داده‌های مالی، تعداد تراکنش‌های مشکوک در مقایسه با تراکنش‌های سالم بسیار کم است و این عدم توازن می‌تواند عملکرد بسیاری از الگوریتم‌های یادگیری ماشین را تحت تأثیر قرار دهد. در پژوهش حاضر، استفاده از تکنیک‌های کاهش ابعاد، خودرمزنگار و یادگیری عمیق موجب شد مدل بتواند رفتارهای غیرعادی را با دقت بیشتری شناسایی کند. این نتیجه با یافته‌های (Ruchay et al., 2023) همخوانی دارد؛ زیرا آنان نیز نشان دادند که استفاده از الگوریتم‌های یادگیری ماشین پیشرفته در داده‌های نامتوازن، عملکرد سامانه‌های کشف تقلب را بهبود می‌بخشد. همچنین نتایج پژوهش حاضر با مطالعه (Aldahasi et al., 2024) همسو است که نشان داد ترکیب تکنیک‌های کاهش عدم توازن داده با الگوریتم‌های یادگیری ماشین، موجب افزایش دقت در کشف تقلب مالی می‌شود. علاوه بر این، (Labanca et al., 2022) تأکید می‌کند که استفاده از یادگیری فعال می‌تواند داده‌های مهم‌تر و حساس‌تر را برای آموزش مدل انتخاب کند و این موضوع به بهبود عملکرد مدل در محیط‌های دارای داده نامتوازن کمک می‌کند؛ یافته‌ای که با عملکرد مطلوب مدل پیشنهادی در این پژوهش هم‌راستا است.

نتایج این پژوهش نشان داد که یادگیری عمیق و شبکه‌های عصبی قادرند الگوهای پیچیده و پنهان در تراکنش‌های مالی را شناسایی کنند؛ الگوهایی که معمولاً توسط روش‌های سنتی قابل کشف نیستند. این مسئله به‌ویژه در حوزه پولشویی اهمیت زیادی دارد؛ زیرا مجرمان مالی همواره تلاش می‌کنند رفتار خود را مشابه تراکنش‌های عادی جلوه دهند. در این پژوهش، مدل پیشنهادی توانست با تحلیل ویژگی‌های تراکنش‌ها و یادگیری روابط میان داده‌ها، رفتارهای غیرعادی را استخراج کند. این یافته با نتایج (Tsapa, 2023) همسو است که بیان می‌کند هوش مصنوعی در سامانه‌های ضدپولشویی می‌تواند الگوهای پیچیده رفتاری را تحلیل کرده و فعالیت‌های مشکوک را در زمان واقعی شناسایی کند. همچنین (Rouhollahi, 2021) تأکید می‌کند که هوش مصنوعی از طریق تحلیل رفتار مشتریان و کشف روابط پنهان میان تراکنش‌ها، نقش مهمی در تحول سامانه‌های کشف جرایم مالی ایفا می‌کند. افزون بر این، یافته‌های پژوهش حاضر با مطالعه (Nicholls et al., 2021) هم‌راستا است؛ زیرا آنان نیز نشان دادند که یادگیری عمیق می‌تواند در مقابله با جرایم مالی پیچیده و در حال تحول، عملکرد مؤثری داشته باشد.

E-ISSN: 3041-8585

یافته‌های پژوهش حاضر همچنین نشان داد که استفاده از ساختارهای گرافی و تحلیل ارتباطات میان تراکنش‌ها می‌تواند دقت شناسایی پولشویی را افزایش دهد. هرچند مدل حاضر مستقیماً بر مبنای یادگیری گراف طراحی نشده بود، اما عملکرد آن در تحلیل روابط میان تراکنش‌ها نشان داد که رویکردهای شبکه‌ای می‌توانند نقش مهمی در کشف الگوهای پنهان داشته باشند. این نتیجه با یافته‌های (Karim et al., 2024) هماهنگ است که استفاده از یادگیری نیمه‌نظارتی مبتنی بر گراف را در کشف شبکه‌های پیچیده پولشویی مؤثر دانست. همچنین (Dumitrescu et al., 2022) نشان داد که تشخیص ناهنجاری در گراف تراکنش‌های بانکی، توانایی بالایی در شناسایی فعالیت‌های غیرقانونی دارد. علاوه بر این، (Kurshan & Shen, 2020) تأکید می‌کند که محاسبات گرافی می‌توانند ساختارهای پنهان شبکه‌های جرایم مالی را آشکار سازند و آینده سامانه‌های کشف تقلب را شکل دهند. نتایج پژوهش حاضر نیز بیانگر آن است که تحلیل روابط پیچیده میان تراکنش‌ها و کاربران، می‌تواند به افزایش نرخ کشف فعالیت‌های مشکوک کمک کند.

از دیگر یافته‌های مهم پژوهش حاضر، قابلیت مدل در شناسایی الگوهای مشکوک در تراکنش‌های رمزارزی و محیط‌های مالی دیجیتال بود. با گسترش استفاده از رمزارزها و فناوری بلاکچین، الگوهای جدیدی از پولشویی شکل گرفته‌اند که شناسایی آن‌ها به روش‌های پیشرفته نیاز دارد. نتایج این پژوهش با یافته‌های (Chitsungo, 2024) همسو است که بیان می‌کند جرایم مبتنی بر رمزارزها، از جمله پولشویی و جرایم سایبری، در حال افزایش هستند و مقابله با آن‌ها نیازمند سامانه‌های هوشمند است. همچنین (Ouyang et al., 2024) نشان داد که یادگیری کنتراستی زیرگراف‌ها در شبکه بیت‌کوین می‌تواند الگوهای پولشویی را با دقت بالایی شناسایی کند. نتایج پژوهش حاضر با یافته‌های (Stefánsson et al., 2022) نیز هم‌راستا است؛ زیرا آنان نیز از یادگیری ماشین بدون ناظر برای شناسایی آدرس‌های مشکوک در بلاکچین استفاده کردند و به نتایج مطلوبی دست یافتند. علاوه بر این، (Martins & Brito, 2023) و (Turner et al., 2020) نیز بر نقش تحلیل شبکه‌ای و داده‌کاوی در شناسایی تراکنش‌های غیرقانونی رمزارزی تأکید کرده‌اند که با یافته‌های پژوهش حاضر هماهنگی دارد.

در پژوهش حاضر، استفاده از ترکیب روش‌های با ناظر و بدون ناظر، یکی از عوامل مؤثر در بهبود عملکرد مدل بود. الگوریتم‌های بدون ناظر توانستند ناهنجاری‌ها و الگوهای ناشناخته را شناسایی کنند، درحالی‌که روش‌های با ناظر برای طبقه‌بندی دقیق‌تر تراکنش‌ها به کار گرفته شدند. این رویکرد ترکیبی سبب شد مدل بتواند علاوه بر شناسایی الگوهای شناخته‌شده، رفتارهای جدید و ناشناخته را نیز کشف کند. این نتیجه با یافته‌های (Kute et al., 2021) مطابقت دارد که تأکید می‌کند ترکیب یادگیری عمیق و هوش مصنوعی توضیح‌پذیر می‌تواند دقت و قابلیت اعتماد سامانه‌های ضدپولشویی را افزایش دهد. همچنین (Husnaningtyas et al., 2023) بیان می‌کند که ادغام یادگیری ماشین و یادگیری عمیق، یکی از رویکردهای مؤثر در توسعه سامانه‌های هوشمند ضدپولشویی است. افزون بر این، (Japinye, 2024) نیز نشان داد که ادغام یادگیری ماشین با سامانه‌های ضدپولشویی مبتنی بر رمزارز، موجب افزایش دقت و کاهش هشدارهای کاذب می‌شود.

نتایج پژوهش حاضر همچنین نشان داد که کلان‌داده و تحلیل داده‌های عظیم مالی، نقش اساسی در توسعه سامانه‌های هوشمند کشف پولشویی دارند. مدل پیشنهادی با پردازش حجم گسترده‌ای از تراکنش‌ها توانست رفتارهای مشکوک را با سرعت و دقت مناسب شناسایی کند. این نتیجه با یافته‌های (Jiao, 2023) همسو است که تحلیل کلان‌داده‌ها را عامل مهمی در بهبود انطباق سامانه‌های بانکی با الزامات ضدپولشویی می‌داند. همچنین (Jensen & Iosifidis, 2023) تأکید می‌کند که یادگیری ماشین و تحلیل آماری می‌توانند رفتارهای غیرعادی را بهتر از روش‌های سنتی شناسایی کنند. افزون بر این، (Wang, 2022) نیز بیان می‌کند که عامل‌های هوشمند مبتنی بر هوش مصنوعی قادرند به‌صورت خودکار الگوهای پولشویی را کشف کرده و از وقوع جرایم مالی جلوگیری کنند.

به‌طور کلی، یافته‌های پژوهش حاضر نشان می‌دهد که استفاده از یادگیری تقویتی عمیق، شبکه‌های عصبی و الگوریتم‌های هوشمند در کشف تراکنش‌های مشکوک به پولشویی و تقلب مالی، می‌تواند به‌عنوان رویکردی نوین و کارآمد در سامانه‌های بانکی مورد استفاده قرار

گیرد. این مدل توانست علاوه بر افزایش دقت کشف تقلب، نرخ هشدارهای کاذب را کاهش دهد و قابلیت شناسایی رفتارهای پیچیده و ناشناخته را فراهم سازد. همچنین نتایج پژوهش بیانگر آن است که توسعه سامانه‌های هوشمند ضدپولشویی می‌تواند نقش مهمی در افزایش امنیت بانکداری الکترونیک، کاهش ریسک جرایم مالی و ارتقای اعتماد مشتریان به نظام مالی داشته باشد. در مجموع، پژوهش حاضر نشان می‌دهد که آینده سامانه‌های ضدپولشویی به‌طور فزاینده‌ای به استفاده از هوش مصنوعی، یادگیری عمیق، تحلیل گراف و کلان‌داده وابسته خواهد بود و سازمان‌های مالی برای مقابله مؤثر با جرایم مالی ناگزیر به بهره‌گیری از این فناوری‌ها هستند.

از محدودیت‌های پژوهش حاضر می‌توان به محدود بودن داده‌های واقعی در دسترس، محرمانه بودن بسیاری از اطلاعات بانکی، عدم دسترسی به برخی ویژگی‌های رفتاری مشتریان و محدودیت در برچسب‌گذاری دقیق داده‌های مشکوک اشاره کرد. همچنین، به دلیل ماهیت پویا و متغیر روش‌های پولشویی، امکان تغییر الگوهای مجرمانه در طول زمان وجود دارد که ممکن است بر عملکرد مدل در آینده تأثیر بگذارد. از سوی دیگر، هزینه‌های پردازشی بالا و نیاز به زیرساخت‌های سخت‌افزاری قوی برای آموزش مدل‌های یادگیری عمیق، از دیگر محدودیت‌های این پژوهش محسوب می‌شود.

پیشنهاد می‌شود در پژوهش‌های آینده، از روش‌های پیشرفته‌تر یادگیری گراف، یادگیری فدرال، یادگیری توضیح‌پذیر و مدل‌های ترکیبی مبتنی بر بلاکچین برای ارتقای دقت سامانه‌های ضدپولشویی استفاده شود. همچنین، بررسی عملکرد مدل‌ها در داده‌های واقعی چندبانکی، تحلیل رفتار مشتریان در بازه‌های زمانی طولانی‌تر و استفاده از داده‌های بین‌المللی می‌تواند به افزایش تعمیم‌پذیری مدل‌ها کمک کند. افزون بر این، مطالعه درباره کاهش هشدارهای کاذب و افزایش تفسیرپذیری مدل‌های یادگیری عمیق می‌تواند زمینه مناسبی برای تحقیقات آینده فراهم سازد.

در حوزه کاربردهای عملی، پیشنهاد می‌شود بانک‌ها و مؤسسات مالی از سامانه‌های مبتنی بر هوش مصنوعی و یادگیری عمیق برای پایش برخط تراکنش‌ها استفاده کنند تا بتوانند فعالیت‌های مشکوک را در کوتاه‌ترین زمان شناسایی نمایند. همچنین، توسعه زیرساخت‌های داده‌محور، آموزش نیروی انسانی متخصص در حوزه تحلیل داده و همکاری نزدیک میان بانک‌ها، نهادهای نظارتی و مراکز پژوهشی می‌تواند اثربخشی سامانه‌های ضدپولشویی را افزایش دهد. علاوه بر این، استفاده از فناوری‌های نوین مانند بلاکچین، تحلیل گراف و سامانه‌های یادگیری تطبیقی می‌تواند به ارتقای امنیت مالی و کاهش ریسک جرایم اقتصادی در نظام بانکی کمک کند.

تقدیر و تشکر

از تمامی کسانی که در انجام این مطالعه همراهی نمودند تشکر و قدردانی می‌گردد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

E-ISSN: 3041-8585

موازین اخلاقی

در پژوهش حاضر تمامی موازین اخلاقی رعایت گردیده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021). A Semantic Rule Based Digital Fraud Detection. *Peerj Computer Science*, *7*, e649. https://doi.org/10.7717/peerj-cs.649

Akhtar, N., Khan, A. N., & Raza, M. (2023). Technological Advancements and Legal Challenges to Combat Money Laundering: Evidence From Pakistan. *Pakistan Journal of Humanities and Social Sciences*, *11*(1), 473-483. https://doi.org/10.52131/pjhss.2023.1101.0365

Aldahasi, E., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2024). Optimizing Fraud Detection in Financial Transactions With Machine Learning and Imbalance Mitigation. *Expert Systems*, *42*(2). https://doi.org/10.1111/exsy.13682

Alhajeri, R., & Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*, *15*(04), 284-305. https://doi.org/10.4236/iim.2023.154014

Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering. *IEEE Access*, *9*, 18481-18496. https://doi.org/10.1109/access.2021.3052313

Chitsungo, C. (2024). Harnessing Digital Strategies to Combat Cryptocurrency-Enabled Crimes: Addressing Money Laundering, Illicit Trade, and Cyber Threats. *Ajir*, *9*(7), 77-106. https://doi.org/10.47672/ajir.2523

Dumitrescu, B., Bălțoiu, A., & Budulan, Ș. (2022). Anomaly Detection in Graphs of Bank Transactions for Anti Money Laundering Applications. *IEEE Access*, *10*, 47699-47714. https://doi.org/10.1109/access.2022.3170467

Goecks, L. S., Korzenowski, A. L., Neto, P. G. T., Souza, D. L. d., & Mareth, T. (2022). Anti-money Laundering and Financial Fraud Detection: A Systematic Literature Review. *Intelligent Sys in Account*, *29*(2), 71-85. https://doi.org/10.1002/isaf.1509

Hampo, J. A., Nwokorie, E. C., & Odii, J. N. (2023). A Web-Based kNN Money Laundering Detection System. *European Journal of Theoretical and Applied Sciences*, *1*(4), 277-288. https://doi.org/10.59324/ejtas.2023.1(4).27

Husnaningtyas, N., Hanin, G. F., Dewayanto, T., & Malik, M. F. (2023). A Systematic Review of Anti-Money Laundering Systems Literature: Exploring the Efficacy of Machine Learning and Deep Learning Integration. *Jema Jurnal Ilmiah Bidang Akuntansi Dan Manajemen*, *20*(1), 91-116. https://doi.org/10.31106/jema.v20i1.20602

Japinye, A. O. (2024). Integrating Machine Learning in Anti-Money Laundering Through Crypto: A Comprehensive Performance Review. *European Journal of Accounting Auditing and Finance Research*, *12*(4), 54-80. https://doi.org/10.37745/ejaafr.2013/vol12n45480

Jensen, R. I. T., & Iosifidis, A. (2023). Fighting Money Laundering With Statistics and Machine Learning. *IEEE Access*, *11*, 8889-8903. https://doi.org/10.1109/access.2023.3239549

Jiao, M. (2023). Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry. *Highlights in Science Engineering and Technology*, *49*, 302-309. https://doi.org/10.54097/hset.v49i.8522

Karim, M. R., Hermsen, F., Chala, S. A., Perthuis, P. d., & Mandal, A. (2024). Scalable Semi-Supervised Graph Learning Techniques for Anti Money Laundering. *IEEE Access*, *12*, 50012-50029. https://doi.org/10.1109/access.2024.3383784

Ketenci, U. G., Kurt, T., Önal, S., Erbil, C., Aktürkoğlu, S., & İlhan, H. Ş. (2021). A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering. *IEEE Access*, *9*, 59957-59967. https://doi.org/10.1109/access.2021.3072114

Kurshan, E., & Shen, H. (2020). Graph Computing for Financial Crime and Fraud Detection: Trends, Challenges and Outlook. *International Journal of Semantic Computing*, *14*(04), 565-589. https://doi.org/10.1142/s1793351x20300022

Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review. *IEEE Access*, *9*, 82300-82317. https://doi.org/10.1109/access.2021.3086230

Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M., & Zanero, S. (2022). Amaretto: An Active Learning Framework for Money Laundering Detection. *IEEE Access*, *10*, 41720-41739. https://doi.org/10.1109/access.2022.3167699

Lokanan, M. (2022). Financial Fraud Detection: The Use of Visualization Techniques in Credit Card Fraud and Money Laundering Domains. *Journal of Money Laundering Control*, *26*(3), 436-444. https://doi.org/10.1108/jmlc-04-2022-0058

Lokanan, M., & Maddhesia, V. (2023). Predicting Suspicious Money Laundering Transactions Using Machine Learning Algorithms. https://doi.org/10.21203/rs.3.rs-2530874/v1

Martins, A. P., & Brito, M. A. (2023). Fraud Detection and Anti-Money Laundering Applying Machine Learning Techniques in Cryptocurrency Transactional Graphs. https://doi.org/10.33965/mccsis2023_202305c016

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, *9*, 163965-163986. https://doi.org/10.1109/access.2021.3134076

Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B., & Chenglin, Z. (2021). Blockchain-Enabled Transaction Scanning Method for Money
 Laundering Detection. https://doi.org/10.20944/preprints202106.0172.v1

Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B., & Zhao, C. (2021). Blockchain-Enabled Transaction Scanning Method for Money Laundering Detection. *Electronics*, *10*(15), 1766. https://doi.org/10.3390/electronics10151766

Ouyang, S., Bai, Q., Feng, H., & Hu, B. (2024). Bitcoin Money Laundering Detection via Subgraph Contrastive Learning. *Entropy*, *26*(3), 211. https://doi.org/10.3390/e26030211

Rouhollahi, Z. (2021). Towards Artificial Intelligence Enabled Financial Crime Detection. https://doi.org/10.48550/arxiv.2105.10866

Ruchay, A., Feldman, E. V., Cherbadzhi, D., & Sokolov, A. N. (2023). The Imbalanced Classification of Fraudulent Bank Transactions Using Machine Learning. *Mathematics*, *11*(13), 2862. https://doi.org/10.3390/math11132862

Stefánsson, H. P., Grímsson, H. S., Þórðarson, J. K., & Óskarsdóttir, M. (2022). Detecting Potential Money Laundering Addresses in the Bitcoin Blockchain Using Unsupervised Machine Learning. https://doi.org/10.24251/hicss.2022.194

Tan, X., Tse, T.-F. T., Yiu, S. M., & Lam, H.-M. H. (2024). A Case Study on Multi-Countries Money Laundering Scheme and a Proposed Automatic Detection System. *International Conference on Cyber Warfare and Security*, *19*(1), 385-394. https://doi.org/10.34190/iccws.19.1.1984

Tsapa, J. A. (2023). Artificial Intelligence Use Cases for Banking Anti-Money Laundering. *Journal of Artificial Intelligence Machine Learning and Data Science*, *1*(2), 259-264. https://doi.org/10.51219/jaimld/joseph-aaron-tsapa/81

Turner, A., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. *Frontiers in Computer Science*, *2*. https://doi.org/10.3389/fcomp.2020.600596

Wang, Q. (2022). A Robust AI Agent-Based Approach to Tackle and Prevent Money Laundering. https://doi.org/10.31219/osf.io/bd38t

Yusoff, Y. H., Azlan, N. A. F., Zamzuri, N. N. M., Sufian, N., Kurniawan, S. N. R., & Hassan, R. (2023). Areas of Technology That Helps in Combating Money Laundering: A Concept Paper. *International Journal of Academic Research in Business and Social Sciences*, *13*(5). https://doi.org/10.6007/ijarbss/v13-i5/16588

Zheng, L. (2025). Networked Markets, Fragmented Data: Adaptive Graph Learning for Customer Risk Analytics and Policy Design. https://doi.org/10.48550/arxiv.2512.24487

E-ISSN: 3041-8585