International Journal of Finance and Investment
ISSN: 3078-6002 (Print), ISSN: 3078-2295 (Online) | Vol. 2, No. 2, 2025

Studies on the Application and Practice of Artificial Intelligence Technology in E-Commerce Platform Risk Management

Haoli Tan

Lyceum of the Philippine University-Batangas, Graduate School, Batangas City, Philippine

Abstract: Cybersecurity and financial transaction fraud prevention are now at danger due to the quick growth of e-commerce platforms. Through the automation of detection, response, and mitigation procedures, artificial intelligence has become a potent instrument for improving risk control systems. Better compliance monitoring and real-time fraud detection predictive analytics are made possible using artificial intelligence into e-commerce risk control. With an emphasis on e-commerce platforms, this study investigates the use and use of artificial intelligence technologies in risk management. The study looks at the uses of artificial intelligence in anomaly detection, cybersecurity, credit risk analysis, and fraud detection. The difficulties in applying AI to risk management are also covered, along with the corresponding solutions. This study offers insights into how companies may improve risk control procedures and guarantee safe online transactions in the e-commerce industry by examining the benefits and drawbacks of artificial intelligence technology.

Keywords: Artificial intelligence, Risk control e-commerce, Fraud detection, Cybersecurity, Machine learning, Predictive analytics, Compliance monitoring, Financial security, Algorithm optimization, Transaction verification, Anomaly detection, Automation, Threat mitigation, Regulatory compliance, Fraud prevention, Risk assessment.

1. Introduction

Global trade has changed because of the growth of e-commerce, which makes online transactions easy. Financial hazards, cyberthreats, and fraudulent activity have all increased because of the quick development of digital commerce. Companies that run e-commerce platforms need to put in place strong risk control procedures to shield consumers from identity theft, illegal transactions, and data breaches. The growing sophistication of cyber fraud schemes makes it difficult for traditional risk management techniques to detect sophisticated threats. Businesses may now use machine learning algorithms and predictive analytics for improved security thanks to artificial intelligence's novel approach to risk control. This study examines the use of artificial intelligence in fraud detection, compliance monitoring, cybersecurity, and anomaly detection in order to investigate its role in e-commerce risk control. The study also addresses practical solutions to these problems and draws attention to the difficulties in artificial intelligence-driven risk management.

2. The Application of Artificial Intelligence in Risk Management

Modern risk management tactics in a variety of industries, including finance, banking, and e-commerce, now heavily rely on artificial intelligence. Businesses can identify security problems and take preemptive measures thanks to artificial intelligence's real-time processing of massive amounts of transactional data. In risk management, artificial intelligence has several important uses.

2.1. Fraud Detection and Prevention

Fraud detection systems driven by artificial intelligence examine past data, user behaviour, and transaction patterns to spot questionable activity. Because machine learning algorithms may identify deviations from typical client behaviour, they can identify fraudulent transactions. Spending patterns are assessed by artificial intelligence systems to detect transactions that pose a high risk. Anomalies are identified via behavioural analysis methods that compare current activity to past trends. According to established fraud indicators, supervised learning models categorise transactions, whereas unsupervised learning techniques identify new fraud schemes. Through constant improvement of algorithmic decision-making, reinforcement learning improves fraud detection. Systems for preventing fraud powered by artificial intelligence use information from several sources, such as device details and geolocation, to confirm the legitimacy of transactions.

2.2. Credit Risk Assessment

Through the analysis of transaction trends and behavioural markers in financial history, artificial intelligence improves the assessment of credit risk. Predictive models driven by AI may help businesses optimise loan decisions and determine the probability of default. Compared to conventional approaches, machine learning-based credit scoring algorithms provide a more accurate assessment of borrower risk. Unknown connections in financial data that point to possible credit concerns are found using artificial intelligence. Automated risk assessment frameworks increase lending efficiency and decrease human processing delays. Financial accounts and credit applications are examined for irregularities using natural language processing. When a borrower's financial situation changes in real time, artificial intelligence models dynamically modify risk scores. Financial institutions can develop personalised loan solutions according to each customer's risk profile with the use of predictive analytics.

2.3. Cybersecurity and Threat Mitigation

Via network traffic monitoring, threat detection, and unauthorised access attempt detection, artificial intelligence enhances cybersecurity. By using anomaly detection tools, firms may reduce cyber threats before they become more serious. Security solutions powered by AI detect malware phishing attempts and cyber intrusions instantly. Attack patterns are examined by automated threat intelligence technologies, which then suggest mitigating techniques. The accuracy of intrusion detection is increased by deep learning algorithms, which analyse enormous volumes of cybersecurity data. Authentication systems with AI capabilities improve security by identifying unusual login behaviour. Digital assets should be continuously monitored to assist organisations detect and address security issues. Response methods that stop suspicious activity before damage is done are automated by artificial intelligence. To anticipate new threats and stop security problems, cyber risk management platforms make use of artificial intelligence.

2.4. Regulatory Compliance Monitoring

With its ability to detect financial transactions, monitor regulatory requirements, and generate audit reports, artificial intelligence automates compliance verification. Human error is decreased and regulatory conformity is enhanced by automated compliance technologies. To verify compliance with financial rules, compliance tools driven by artificial intelligence examine court papers. Businesses may anticipate changes in regulations and modify their policies accordingly with the aid of predictive compliance monitoring. Manual oversight is decreased by real-time compliance audits produced by automated reporting systems. Fraud detection powered by AI makes sure that transactions adhere to anti-money laundering laws. Contracts and regulatory papers contain important compliance phrases that are extracted by natural language processing. Frameworks for risk assessment using artificial intelligence examine financial transactions to stop legal infractions. Businesses combine legal compliance systems with artificial intelligence to increase industry standards compliance.

2.5. Predictive Risk Analysis

Businesses may anticipate future dangers by using artificial intelligence to analyse market patterns and historical data. Predictive analytics enhances financial risk management and fraud prevention decision-making. Emerging financial hazards are indicated by patterns found by machine learning techniques. Artificial intelligence-driven models evaluate possible risk situations and suggest ways to reduce them. Based on economic patterns, predictive analytics assists companies in modifying their financial strategies. Macroeconomic indicators are analysed by artificial intelligence to evaluate possible dangers to the entire sector. Models for risk forecasting combine market analysis and insights from artificial intelligence to enhance decision-making. In response to shifting financial conditions, automated data-driven risk models make dynamic adjustments. Potential market disruptions are identified by artificial intelligence-based early warning systems before they have an effect on firms.

3. The Application of Artificial Intelligence Technology in the Risk Control of E-Commerce Platforms

Managing risk is particularly difficult for e-commerce platforms because of the number of digital transactions and the growing complexity of cyber-crime. The following are some ways that artificial intelligence technology has been successfully incorporated into risk management plans.

3.1. Machine Learning for Fraud Detection

Real-time fraud detection rates are increased using supervised machine learning models that identify fraud trends using labelled transaction data. Based on trends in past data, algorithms categorise transactions as either authentic or fraudulent. With ongoing learning, detection accuracy gradually increases. To identify signs of fraud, supervised models are trained on big datasets.

Anomaly detection and clustering are two unsupervised learning approaches that aid in the discovery of hitherto undiscovered fraud schemes. In order to identify anomalies and fraudulent patterns, AI examines transaction patterns. Without the use of labels, these methods assist in identifying new dangers. The classification of fraudulent activity is predicated on departures from typical behavioural patterns.

Adaptive fraud detection is improved by reinforcement learning algorithms, which constantly improve detection parameters according to transaction results. In order to enhance decision-making, AI agents assess previous fraud detection successes and failures. Based on fresh data, fraud trends are continually updated. As risks change, reinforcement learning models adjust to improve fraud detection over time.

Rapid analysis of large datasets using AI-powered fraud detection systems improves accuracy and lowers false positives. AI evaluates risk ratings quickly by comparing transaction data with past fraud histories. Processing millions of transactions per second improves the capacity to avoid fraud. As more training data is added to machine learning models, the accuracy of fraud detection increases.

New fraud tendencies are regularly included into machine learning models to improve their prediction power. AI incorporates real-time threat intelligence to adjust to changing fraud strategies. It is easier to identify and stop new fraud operations. Frameworks for detecting fraud are always learning from new fraud patterns.

3.2. Natural Language Processing for Identity

Verification By examining speech, text, and communication patterns, natural language processing improves client authentication. To identify irregularities, AI assesses writing style, typing speed, and speaking tone. These methods aid in the prevention of social engineering scams. AI-powered authentication uses voice recognition to improve security.

NLP is used by AI-driven biometric authentication systems to analyse speech patterns and recognise voices in order to confirm identities. To verify identification correctness, AI compares voiceprints with biometric data that has been saved. Adding voice authentication to multi-factor authentication improves security. The accuracy of verification is increased via automated biometric analysis.

NLP-based character recognition ensures the legitimacy of scanned IDs and passports processed by AI-based document

verification. Artificial intelligence (AI) retrieves and validates information from papers by comparing them with official records. The use of automated validation lowers identity theft. The accuracy of document verification procedures is continually improved by AI.

During identity verification procedures, chatbots driven by natural language processing (NLP) spot questionable linguistic patterns in real time. Artificial intelligence scans consumer interactions for irregularities that can point to fraud. Prompt reaction systems highlight possible occurrences of identity theft. Risk assessment is automated by AI during identification verification.

AI models use face recognition and natural language processing (NLP) to enhance security through multi-modal authentication. In order to confirm authenticity, AI compares biometric data with identification documents. Verification procedures are strengthened by this multi-layered approach. AI security solutions change to meet new dangers like identity theft.

3.3. Behavioral Analytics for User Risk Profiling

AI evaluates user behaviour, including device usage, transaction history, and frequency of logins, to determine risk levels. Based on consistent behaviour, AI gives consumers dynamic risk rankings. Changes to devices or unusual access points lead to extra security checks. Based on user action, risk assessment models adapt dynamically.

By identifying odd activity, such logins from unidentified places, AI-driven behavioural analytics stop unwanted access. In order to identify account takeovers, AI analyses login patterns with previous data. Users and administrators are alerted via automated systems when questionable activity occurs. Behavioural pattern analysis increases the precision of risk identification.

Behavioural risk assessment is used to dynamically modify security processes using risk-based authentication. By requesting further verification for transactions deemed high-risk, AI personalises authentication techniques. The security measures implemented depend on the behaviour of the user. Measures for authentication powered by AI adjust to trends in fraud.

The accuracy of fraud detection is increased by machine learning algorithms that generate customised user profiles. AI monitors consumer browsing and purchasing patterns to create comprehensive profiles. Activity patterns that deviate from the norm are noted for examination. AI adjusts authentication according to user risk.

Real-time user activity is compared to past behavioural trends by AI to identify behavioural abnormalities. Inconsistencies in mouse movements, transaction preferences, and typing speed are used by AI to detect fraudulent activity. Automated risk rating improves the prevention of fraud.

3.4. Automated Transaction Monitoring

Real-time payment flows are tracked by AI-driven transaction monitoring, which promptly detects questionable transactions. AI continually examines transaction frequencies and volumes to find irregularities. Procedures for fraud investigations are triggered by unusual expenditure patterns. Fraud prevention strategies are enhanced by AI-driven risk assessment.

Unusual activity, such several expensive transactions from a new device, is flagged by automated fraud detection systems. AI analyses past transactions to find odd trends. When transactions diverge from typical spending patterns, alerts are produced. AI improves the control of fraud risk.

By examining transaction dispute trends, AI-powered monitoring systems detect chargeback fraud. AI can identify discrepancies between client claims and transaction records. Automated verification procedures stop fraudulent chargebacks. AI lowers monetary losses brought on by chargeback fraud.

Adaptive algorithms incorporate external threat knowledge to improve transaction risk assessment. AI improves detection accuracy by integrating fraud data from international security networks. In real time, new fraud strategies are detected and countered. Transaction security is enhanced by AI-driven fraud detection.

Predictive monitoring is made possible by AI, which uses historical transaction patterns to predict possible fraudulent activity. AI uses past data trends to forecast high-risk transactions. Before fraudulent transactions are completed, preventive procedures are implemented. Risk assessment is continually improved by AI fraud detection models.

3.5. Cybersecurity Protection Measures

AI improves cybersecurity by using pattern recognition to find malware, phishing attempts, and other online dangers. AI can identify malware signatures, phoney websites, and dangerous email content. To combat new threats, security procedures are automatically updated. AI cybersecurity models improve the prevention of fraud.

Security solutions with AI capabilities stop account takeovers by identifying attempts at illegal access. AI keeps an eye out for unusual activity, such repeated unsuccessful login attempts. Suspicious access requests are blocked by automated security mechanisms. Authentication powered by AI fortifies cybersecurity defences.

Payment gateways are secured by AI-based encryption algorithms that safeguard private financial information. AI-powered cryptography techniques protect personal information and credit card numbers. Secure encryption guards against breaches and guarantees data integrity. Transaction security is improved by AI-driven encryption.

Threat intelligence tools powered by AI examine worldwide cyberattack trends to improve security tactics. AI learns from global cyberthreats to continually update security frameworks. Based on real-time intelligence, proactive threat mitigation measures are put into place. AI models constantly improve cybersecurity tactics.

AI constantly looks for security flaws, enabling e-commerce systems to proactively repair security breaches. AI simulates cyberattack scenarios to evaluate system vulnerabilities. Timely security upgrades are guaranteed via automated vulnerability discovery. Cybersecurity methods powered by AI change to counter new threats.

3.6. Algorithmic Risk Control Optimization

By altering judgement criteria to reduce false positives and negatives, AI improves fraud detection systems. AI balances security and user experience by optimising fraud detection settings. Strategies to avoid fraud are improved by ongoing model training. Security evaluations are more accurate when fraud is detected by AI.

Automated compliance checks lower legal risks by ensuring that transactions adhere to regulatory regulations. AI confirms adherence to financial laws, including those

pertaining to anti-money laundering. Adherence to regulations is made easier by automated reporting. Compliance technologies powered by AI increase the accuracy of fraud detection.

Preemptive risk control procedures are improved by AI-powered risk assessment models that forecast possible fraud tendencies. AI looks at worldwide fraud trends to predict new dangers. Financial losses are decreased by preventive fraud detection techniques. Predictive analytics powered by AI enhance fraud protection systems.

New threat intelligence insights are used by AI-driven optimisation frameworks to modify fraud detection systems. Real-time fraud updates are integrated by AI to enhance detection models. For improved effectiveness, fraud prevention techniques are constantly improved. AI algorithms adjust dynamically to changing fraud threats.

AI regularly assesses how well risk control tactics are working, enhancing platform security. For continuous enhancements, AI examines fraud detection systems and security procedures. Improved fraud prevention techniques guarantee platform security over time. AI-powered security models enhance the control of fraud risk.

4. The Challenges Faced and Countermeasures

Notwithstanding the advantages of AI in e-commerce risk management, companies still confront a few obstacles that need for calculated answers.

4.1. Data Privacy and Security

Large volumes of user data are processed by artificial intelligence systems, which raises questions regarding data security and customer privacy. To secure sensitive data, businesses need to have encryption, access restrictions, and compliance frameworks in place. By transforming data into unintelligible forms, encryption protects it from unwanted access. By demanding several verification methods, multi-factor authentication improves security. By eliminating personally identifying information from datasets, data anonymisation lowers privacy threats. Sensitive data is shielded from data breaches by secure storage systems. Strict data handling procedures are required by regulatory compliance measures like the CCPA and GDPR in order to protect user information. Artificial intelligence (AI)-powered monitoring systems identify odd data access trends and stop illegal use. Employees that participate in cybersecurity training programs learn best practices for reducing data handling hazards. Businesses use privacy impact assessments to analyse the hazards of processing data generated by AI. Protocols are outlined in secure data-sharing agreements for managing client data across platforms.

4.2. Bias in Artificial Intelligence Algorithms

Biases in artificial intelligence algorithms may result in misleading risk evaluations. Businesses must train AI systems on a variety of datasets and carry out frequent bias assessments to guarantee algorithmic fairness. In order to accurately reflect a variety of user groups, bias prevention strategies entail rebalancing databases. By modifying algorithmic decision-making procedures, fairness-aware machine learning models lessen biassed results. Risk assessment models are auditable and explicable when AI development is transparent. In order to detect any biases, algorithmic fairness testing entails examining model outputs. The accuracy of risk assessments is continuously improved by regular updates to AI training datasets. Independent assessments of AI fairness and bias are offered via external audits. Best practices for creating objective AI systems are established by ethical AI guidelines. Potential discrepancies in decision-making processes are recognised and flagged by bias detection systems. Initiatives for AI fairness is strengthened by cooperation with diversity and ethics experts.

4.3. High Implementation Costs

A significant financial commitment is necessary for the integration of artificial intelligence technologies. By working with technology providers and using cloud-based artificial intelligence technologies, businesses may cut expenses. Businesses may acquire AI capabilities through cloud computing without having to make costly infrastructure investments. AI services that are subscription-based provide scalable price structures that lower initial expenditures. Open-source AI frameworks provide firms creating unique risk control solutions affordable options. Businesses may use pre-trained models for cybersecurity and fraud detection using AI-as-a-service platforms. Businesses may get AI knowledge without incurring large in-house development expenditures through partnerships with technology firms. Automation streamlines fraud detection and compliance procedures, which lowers operating costs. Businesses can reduce implementation costs with the use of financial incentives like government subsidies and support for AI research. Businesses may progressively grow AI use with modular AI solutions. Return on investment analysis guarantees that investments in AI are in line with corporate goals.

4.4. Evolving Cybersecurity Threats

New attack techniques are continuously being developed by cybercriminals to get beyond artificial intelligence protection systems. Companies ought to use artificial intelligence models that are adaptable, meaning they will change when new dangers arise. Threat intelligence systems with artificial intelligence (AI) examine worldwide cyberattack patterns to identify new dangers. Adaptive machine learning models use emerging fraud tendencies to improve risk detection algorithms. Suspicious activities are flagged by real-time anomaly detection before they become security breaches. Cyber dangers are lessened by automated response systems, which immediately prevent unwanted access attempts. AI-powered intrusion detection systems and firewalls are integrated into multi-layered security frameworks. Finding flaws in AI-based security measures is possible through ongoing penetration testing. The development of AI systems that can resist complex attacks is the main goal of cyber resilience tactics. Artificial intelligence (AI) systems that hunt threats proactively look for weaknesses before hackers take advantage of them. Working together with researchers in cybersecurity improves AI security. False attack surfaces are produced by AI-driven deception technologies to trick hackers.

4.5. Regulatory Compliance Challenges

Numerous regulatory frameworks must be adhered to by e-commerce platforms. Artificial intelligence-powered compliance monitoring systems are a good way for businesses to make sure that financial security regulations are followed. Platforms for regulatory compliance using AI capabilities

examine transactions to look for unusual activity that could be against financial rules. For regulatory audits, automated reporting systems produce compliance documentation. Risk assessment methods powered by AI compare company activities to regulatory standards. Contractual compliance is ensured by scanning legal papers using natural language processing technologies. With predictive compliance monitoring, possible regulatory infractions are foreseen before they happen. The adaptation of compliance models to changing legal criteria is ensured by ongoing AI training. Solutions for industry-specific compliance take care of sector-specific legal needs. Businesses are assisted in navigating international trade restrictions by cross-border e-commerce compliance technologies. AI-powered document verification tools confirm user identities in order to comply with KYC laws. Responsible AI practices are established in compliance-sensitive workplaces via ethical AI governance frameworks.

4.6. Scalability and System Adaptation

Models of AI must evolve together with the market and the number of transactions. Real-time AI solutions that adapt to changing risk variables should be purchased by businesses. Scalable AI systems can handle growing numbers of transactions without sacrificing efficiency. Load balancing powered by AI maximises system resources to manage periods of high transaction volume. Cloud-based artificial intelligence systems offer adaptable processing capacity to support expansion. Latency in risk assessments is decreased by edge AI systems, which analyse data closer to the source. Automation powered by AI accelerates the identification of fraud and the enforcement of compliance. Self-learning AI models ensure ongoing progress by changing as new fraud trends appear. Algorithms for scalable fraud detection adjust to changes in user behaviour and transaction trends. More questions about security are answered by AI-enhanced customer service platforms. On the basis of past data trends, predictive analytics forecast future scalability requirements. AI-driven risk control may be optimised with the help of integration with sophisticated analytics tools.

References

[1] Tao, C., & Liu, Y. (2024). Application and Development of Artificial Intelligence Risk Control in Internet Finance. Frontiers in Business, Economics and Management, 14(2), 10-12.

[2] Micu, A., Micu, A. E., Geru, M., Căpățînă, A., & Muntean, M. C. (2021). The impact of artificial intelligence use on the e-commerce in Romania. Amfiteatru Economic, 23(56), 137-154.

[3] Srivastava, A. (2021). The Application & Impact of Artificial Intelligence (AI) on E-Commerce. Contemporary Issues in Commerce & Management, 1(1), 165-175.

[4] Bawack, R. E., Wamba, S. F., Carillo, K. D. A., & Akter, S. (2022). Artificial intelligence in E-Commerce: a bibliometric study and literature review. Electronic markets, 32(1), 297-338.

[5] Khrais, L. T. (2020). Role of artificial intelligence in shaping consumer demand in E-commerce. Future Internet, 12(12), 226.

[6] Areiqat, A. Y., Alheet, A. F., Qawasmeh, R. A., & Zamil, A. M. (2021). Artificial intelligence and its drastic impact on e-commerce progress. Academy of Strategic Management Journal, 20, 1-11.

[7] Renrui, L. (2022). Discussion on the Application of Artificial Intelligence in e-Commerce. Journal of Electronics and Information Science, 7(1), 55-59.

[8] Micu, A., Micu, A. E., Geru, M., Căpățînă, A., & Muntean, M. C. (2021). The impact of artificial intelligence use on the e-commerce in Romania. Amfiteatru Economic, 23(56), 137-154.

[9] Kashyap, A. K., Sahu, I., & Kumar, A. (2022). Artificial Intelligence and Its Applications in E-Commerce–a Review Analysis and Research Agenda. Journal of Theoretical and Applied Information Technology, 100(24), 7347-7365.

[10] Bawack, R. E., Wamba, S. F., Carillo, K. D. A., & Akter, S. (2022). Artificial intelligence in E-Commerce: a bibliometric study and literature review. Electronic markets, 32(1), 297-338.

[11] Vanneschi, L., Horn, D. M., Castelli, M., & Popovič, A. (2018). An artificial intelligence system for predicting customer default in e-commerce. Expert Systems with Applications, 104, 1-21.

[12] Kalia, P. (2021). Artificial intelligence in e-commerce: a business process analysis. In Artificial Intelligence (pp. 9-19). CRC Press.

[13] Micu, A., Micu, A. E., Geru, M., Căpățînă, A., & Muntean, M. C. (2021). The impact of artificial intelligence use on the e-commerce in Romania. Amfiteatru Economic, 23(56), 137-154.

[14] Khrais, L. T. (2020). Role of artificial intelligence in shaping consumer demand in E-commerce. Future Internet, 12(12), 226.

[15] Kang, K., Wang, X., & Yang, W. (2024). The analysis of social E-commerce with artificial intelligence. Applied and Computational Engineering, 47, 67-74.

[16] Fedorko, R., Kráľ, Š., & Bačík, R. (2022, July). Artificial intelligence in e-commerce: A literature review. In Congress on Intelligent Systems: Proceedings of CIS 2021, Volume 2 (pp. 677-689). Singapore: Springer Nature Singapore.

[17] Song, X., Yang, S., Huang, Z., & Huang, T. (2019, August). The application of artificial intelligence in electronic commerce. In Journal of Physics: Conference Series (Vol. 1302, No. 3, p. 032030). IOP Publishing.

[18] Gochhait, S., Mazumdar, O., Chahal, S., Kanwat, P., Gupta, S., Sharma, R., ... & Sachan, R. (2020, May). Role of artificial intelligence (AI) in understanding the behavior pattern: a study on e-commerce. In ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications (pp. 1600-1606). Singapore: Springer Singapore.

[19] Kolodin, D., Telychko, O., Rekun, V., Tkalych, M., & Yamkovyi, V. (2020, March). Artificial intelligence in E-commerce: Legal aspects. In III International Scientific Congress Society of Ambient Intelligence 2020 (ISC-SAI 2020) (pp. 96-102). Atlantis Press.

[20] Cong, X. (2021, June). Research on financial risk management of E-commerce enterprises in the era of big data. In Proceedings of the 7th International Conference on Frontiers of Educational Technologies (pp. 195-199).

[21] Zhao, M. (2022). Research on financial risk assessment based on artificial intelligence. In SHS Web of Conferences (Vol. 151, p. 01017). EDP Sciences.