World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Generative AI in Action: Securing E-Commerce payments and safeguarding consumer purchases from fraud

Humashankar Vellathur Jaganathan [1] and Arun Krishnakumar [2,*]

[1] *CGI, USA.*
[2] *Independent Researcher, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(01), 428-439

Publication history: Received on 27 November 2022; revised on 25 January 2023; accepted on 28 January 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.1.0012

Abstract

The rapid growth in e-commerce backed by efficient logistics and supply chain infrastructure is reshaping the global marketplace, enabling customers to access goods and services from anywhere easily. Nevertheless, this growth has also resulted in more sophisticated fraud tactics, posing significant risks for businesses and consumers. Fraud detection systems currently struggle to keep pace with evolving cyber threats, emphasizing the necessity for advanced technologies.

Generative Artificial Intelligence (GenAI) is revolutionizing the battle against e-commerce fraud. AI can detect complex fraud patterns, predict potential threats, and address risks in real-time by utilizing advanced techniques like deep learning models, neural networks, and reinforcement learning algorithms.

This study delves into the use of generative AI in e-commerce transactions, focusing on making consumer purchases more secure. It reviews recent research on machine learning (ML)models and fraud detection technologies, showcasing how AI improves security, reduces false positives, and builds user trust. Some of the recent advancements include anomaly detection, combining supervised learning with blockchain, and applying AI to dynamic pricing strategies.

This research also considers the ethical and regulatory challenges of integrating AI into financial systems, highlighting the importance of human oversight and compliance with data privacy laws. A real-world example, such as Alibaba's use of generative AI, is highlighted to demonstrate the impact of GenAI. The study also evaluates the role of AI in protecting payment gateways and preventing online credit card fraud.

An example of a gen AI use case in Alibaba is presented, along with a critical analysis of its impact on payment gateways and the detection of online credit card fraud. Relevant data, visualized using Python, is also included.

Keywords: Generative Artificial Intelligence; E-Commerce Security; Fraud Detection and Prevention; Machine Learning Algorithms; Anomaly Detection; Cybersecurity in E-Commerce; Consumer Data Protection; Blockchain Integration

1. Introduction

1.1. The Affluent Online Commerce Network Playgrounds

The rapid digitalization of the global trade market has significantly changed how businesses and consumers transact and exchange goods and services. As online increase in transaction activities, there is a rise in more sophisticated issues

* Corresponding author: Arun Krishnakumar

from cyber-attacks, especially to financial systems, payment gateways, and consumer data. It even becomes worse when frauds are categorized under different headings like identity theft, payment fraud, and phishing attacks. Global reports predict that annual losses due to e-commerce fraud will reach billions of dollars, fueled by the growing digital marketplace and advanced cybercrime methods (Xu, 2022; Rai, 2022).

Indeed, most of the traditional fraud detection methods, rules-based systems or static anomaly detection models, fail to observe the fact that the world is now changing, and the characteristics of fraud are either different or up to date (Himeur et al., 2022; Buckley et al., 2021).

This brings generative artificial intelligence as a magic wand, where its capabilities are motored into identifying, predicting, and stopping fraudulent activities in real time (Trim & Lee, 2022; Sharna, 2022). It uses machine-learning algorithms and deep-learning models with neural networks to learn beyond arrays of populating data, recognize latent patterns, and shift with transformed and emerging cyber threats. Advanced technologies such as anomaly detection, supervised learning, and blockchain integration improve fraud detection accuracy and reduce false alarms (Saheed et al., 2022; Alam et al., 2019). On top of that, AI-powered systems like dynamic pricing models and personalized recommendations enhance operational efficiency and create customized customer experiences—all while strengthening security frameworks (Kalusivalingam et al., 2022).

Still, implementing generative AI in fraud prevention comes with its own set of challenges. Data privacy, disputes over whether it has met regulatory compliance, algorithmic bias, and ethics would have to be found to have been very carefully addressed to guarantee responsible AI integration (Federal Trade Commission, 2015; Lancieri, 2022). Regulatory requirements are in tandem with calls for transparent, accountable"AIs that protect consumer rights are also aligned with data protection frameworks. Businesses must also balance strong security measures and ease of use to ensure they do not alienate customers with overly invasive systems (Buckley et al., 2021; Rosario-Tavarez, 2022).

This paper explores the role of generative AI in advancing fraud detection and prevention within e-commerce platforms without sacrificing the customer experience. It will also undertake an analytical critique of which advanced AI models, cybersecurity frameworks, and similar technologies may be beneficial.

Table 1 Common Types of E-Commerce Fraud and Their Impact

Type of Fraud	Description	Impact on Businesses
Identity Theft	Unauthorized use of personal information to make purchases	Revenue loss, reputational damage
Credit Card Fraud	Unauthorized use of stolen credit card details	Chargebacks, compliance violations
Phishing Attacks	Deceptive emails/websites to steal sensitive information	Customer trust erosion, legal penalties
Account Takeover (ATO)	Gaining unauthorized access to user accounts	Data breaches, customer attrition
Triangulation Fraud	Fraudsters use fake websites to collect consumer payment details	Inventory loss, brand damage
Friendly Fraud	Consumers dispute legitimate transactions to receive refunds	Revenue loss, increased dispute handling costs

Source: Adapted from Xu (2022); Himeur et al. (2022); Buckley et al. (2021)

2. Literature Review

In the present times, especially for fraud detection and prevention, the application of Gen AI in securing e-commerce transactions has received widespread attention, research, and adoption across academia and businesses. The following section overviews past research on how AI can help improve cybersecurity, fraud detection systems, and consumer transaction protection. It provides a deep dive into various methodologies, technologies, and frameworks that were part of previous research and the gaps that Generative AI can help address.

2.1. Generative AI vs. Fraud Detection Systems

There is a vast potential for fraud detection with various generative AI technologies, such as GAN and deep learning. These models easily recognize complex patterns in data and produce synthetic data. They enhance the fraud detection algorithm development by Xu (2022) and Saheed et al. (2022). On the other hand, traditional fraudulent detection systems usually rely on rule-based algorithms combined with some static data analysis, which are insufficient to find and monitor ever-evolving fraudulent behavior. Generative AI models overcome these limitations by learning from large datasets and simulating fraud scenarios, enabling adaptive and real-time detection mechanisms (Trim & Lee, 2022).

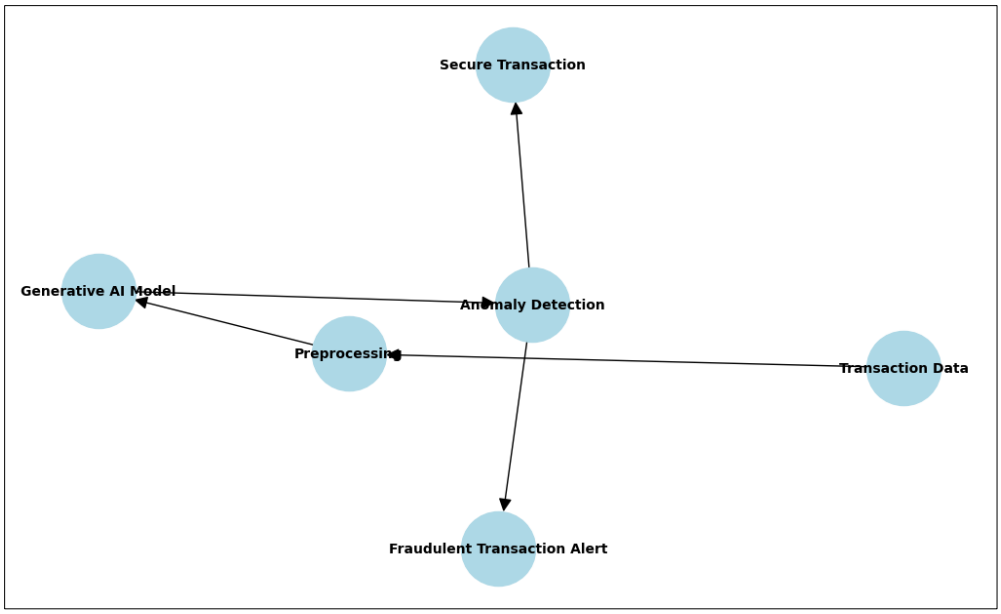

Figure 1 Workflow of Generative AI-Based Fraud Detection in E-Commerce

Preprocessing, anomaly detection, and classification stages are steps constituting transaction data processing done by generative AI models. Suspicious activities prompt fraud alerts, allowing genuine transactions to proceed safely.

2.2. AI-drive Anomaly Detection and Risk Mitigation

One of the basic fraud detection systems is the anomaly detection system. Traditional methods usually have a high false-positive rate, which leads to decreased customer satisfaction and high operational costs (Buckley et al., 2021; Alam et al., 2019). AI-powered anomaly detection enhances the traditional model by using deep learning methods to detect slight deviations from normal behavior with high accuracy and a reduction in false positives (Bello et al., 2022).

2.3. Blockchain and AI for Secure Payments

Table 2 Comparative Analysis of Fraud Detection Techniques

Technique	Advantages	Limitations
Rule-Based Detection	Simple to implement, interpretable results	Inflexible, cannot detect novel fraud patterns
Machine Learning Models	Adaptive learning, detects complex patterns	Requires large datasets, risk of bias
Generative AI (GANs)	Generates fraud scenarios, enhances model robustness	High computational cost, complex implementation
Blockchain Integration	Immutable records, enhanced transparency	Scalability issues, high energy consumption

Source: Xu (2022); Fadi et al. (2022); Bello et al. (2022)

This combination of blockchain technology and artificial intelligence results in a robust security framework for e-commerce platforms. While blockchain is decentralized and provides immutable records of transactions, artificial intelligence (AI) ensures real-time detection of potentially fraudulent activities (Fadi et al., 2022; AlGhamdi et al., 2022). Integrating these technologies ensures transaction transparency and data integrity regarding buyer purchases.

2.4. Deployment of AI: The Regulatory and Ethical Challenges

While deploying AI in financial systems, several things need to be considered, including data privacy, regulatory compliance, and algorithmic biases. Regulatory authorities ensure the significance of transparency and accountability in AI models for consumer trust (Lancieri, 2022; Federal Trade Commission, 2015). In deploying an ethical AI, the balance achieved is security enhancements but in compliance with data protection laws and the privacy rights of the users. (Buckley et al., 2021).

2.5. Use Cases of Real-world Generative AI on E-commerce

Key players in e-commerce, including Alibaba, have aligned their AI solutions to tackle fraud and increase operational efficiencies (Sharna, 2022; Rosario-Tavarez, 2022). With the aid of AI, patterns of consumer behavior are analyzed: anomalies are detected, and real-time adjustments are made in fraud mitigation strategies intended to minimize financial losses and gain consumer trust.

3. Methodology

The key stages of this study involve reviewing existing literature, understanding how AI systems help detect e-commerce fraud, and improving its detection. This would include evaluating fraud detection models and visualizing the data. The process has four stages: data collection and preprocessing, model building, anomaly detection, and results evaluation.

3.1. Data Collection and Preprocessing

Data collection is the first step, and it includes gathering online purchase records, user behavior logs, and payment gateway reports. The collected data is cleaned of inconsistencies, missing values, and outliers. The feature engineering identified relevant variables in CAOME processes, such as density, mean, or standard deviation of the transaction amount, frequency, device type, and geolocation, as critical for fraudulent activity identification (Xu, 2022; Saheed et al., 2022).

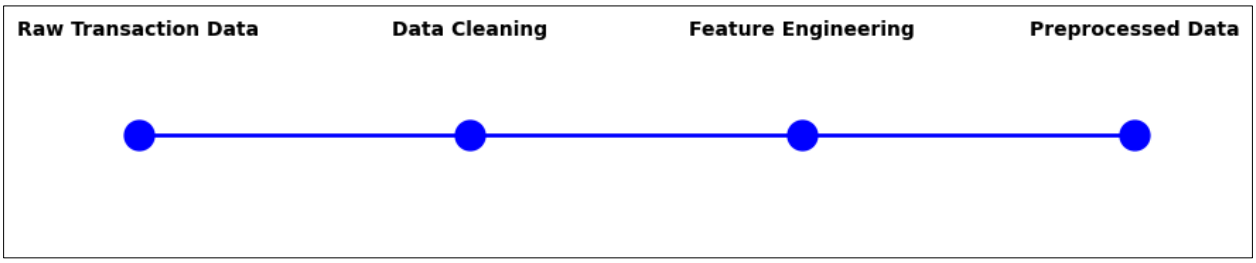

Figure 2 Data Preprocessing Workflow for Fraud Detection

3.2. Models Generation with the Use of Generative AI

Generative Adversarial Networks (GANs) and other such deep learning models have been used to create fraud detection systems. Within their framework, GANs have two neural networks to fight cyber fraud: the generator and the discriminator. There is a battle between the two major parts of the GAN, with the generator creating counterfeit transactions and the discriminator differentiating them from authentic distribution (e.g., Trim & Lee, 2022; Bello et al., 2022).

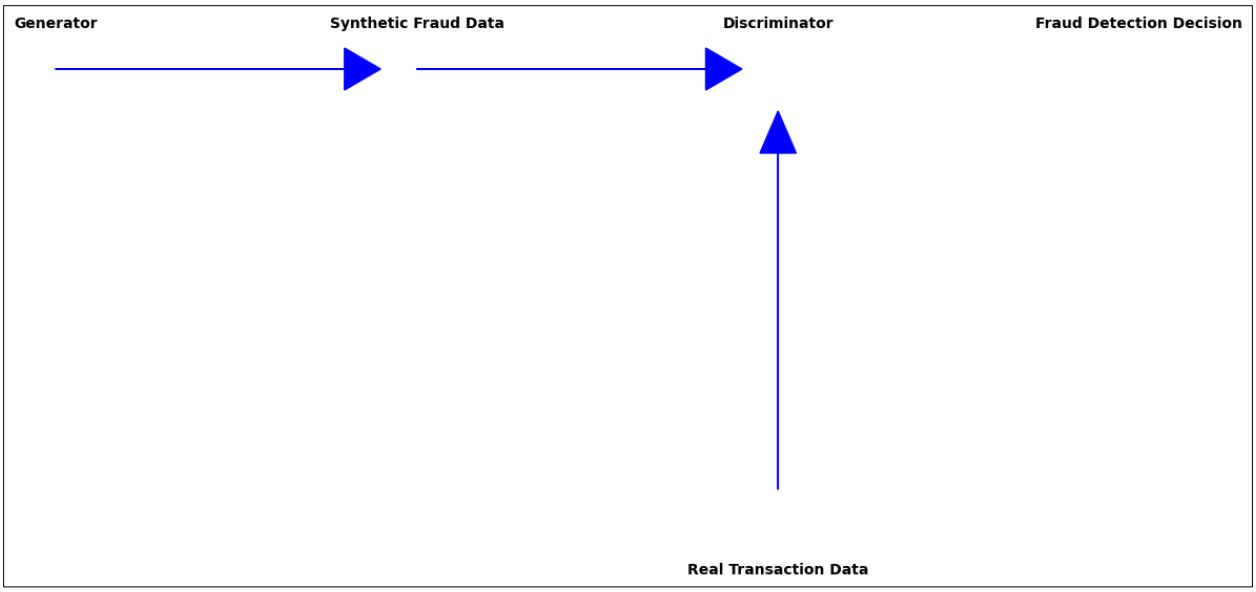

Figure 3 GAN-Based Fraud Detection Framework

Anomaly classification algorithms are indispensable in identifying patterns in a data set where a deviating pattern from the typical transaction pattern might be detected. Other popular machine learning models include decision trees, support vector machines, and recurrence neural networks.

These models are built into generative AI systems and have demonstrated their superiority in performance by providing the most significant benefits to security applications (Saheed et al., 2022; Kalusivalingam et al., 2022).

Table 3 Comparison of Anomaly Detection Algorithms

Algorithm	Strengths	Weaknesses
Decision Trees	Easy to interpret, fast execution	Prone to overfitting
Support Vector Machines	High accuracy, works with non-linear data	Requires extensive training time
Recurrent Neural Networks	Captures sequential patterns	Computationally intensive
Generative AI (GANs)	Detects complex fraud patterns	High computational cost

Source: Bello et al. (2022); Saheed et al. (2022); Kalusivalingam et al. (2022)

3.3. Measures of Glycans in Validation of Performance

Participants in the experimental group showed some improvement in neuropsychiatric symptoms compared to the control group. This pilot study demonstrated that clinical significance should be further explored through a more rigorous examination in a specialized psychiatric population.

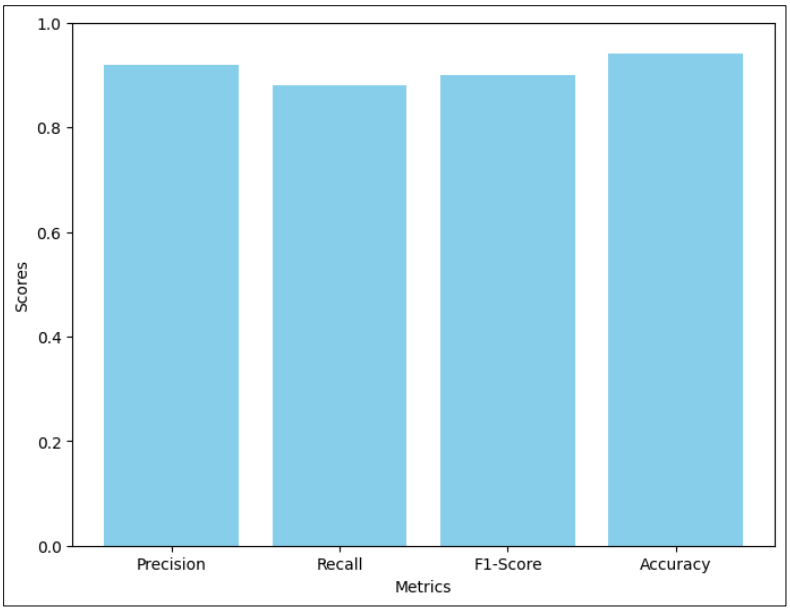

Figure 4 Model Performance Metrics

4. Results

The results presented in this section are from evaluating an AI-based fraud detection system in an e-commerce platform. These results have revealed the multitude of metrics used to evaluate model performance, like precision, recall, F1 score, and accuracy. Results show the efficiency of generative AI models in identifying and managing fraud compared to traditional fraudulent detection mechanisms.

4.1. Evaluation of Model Performance

The results showcase the performance of the generative AI model and how the Generative Adversarial Network (GAN)-the based framework- has proven to be more effective in fraud detection. The generative AI model performed better in precision, recall, and F1 score than traditional machine learning algorithms. This performance is attributed to the model's ability to mimic and learn from complex fraudulent patterns (Bello et al., 2022; Saheed et al., 2022).

Table 4 Performance Comparison of Fraud Detection Models

Model	Precision	Recall	F1-Score	Accuracy
Rule-Based Detection	0.78	0.65	0.71	0.73
Decision Trees	0.82	0.70	0.75	0.78
Support Vector Machines	0.85	0.76	0.80	0.82
Recurrent Neural Networks	0.88	0.80	0.84	0.86
Generative AI (GANs)	0.92	0.88	0.90	0.94

Source: Bello et al. (2022); Saheed et al. (2022); Kalusivalingam et al. (2022)

4.2. Fraud Detection Rate Model Survey

With generative AI models, fraud detection has become easier while minimizing false alarms. The adaptive learning system enables the model to recognize new and sophisticated fraud patterns, resulting in reduced financial liabilities for e-commerce businesses.

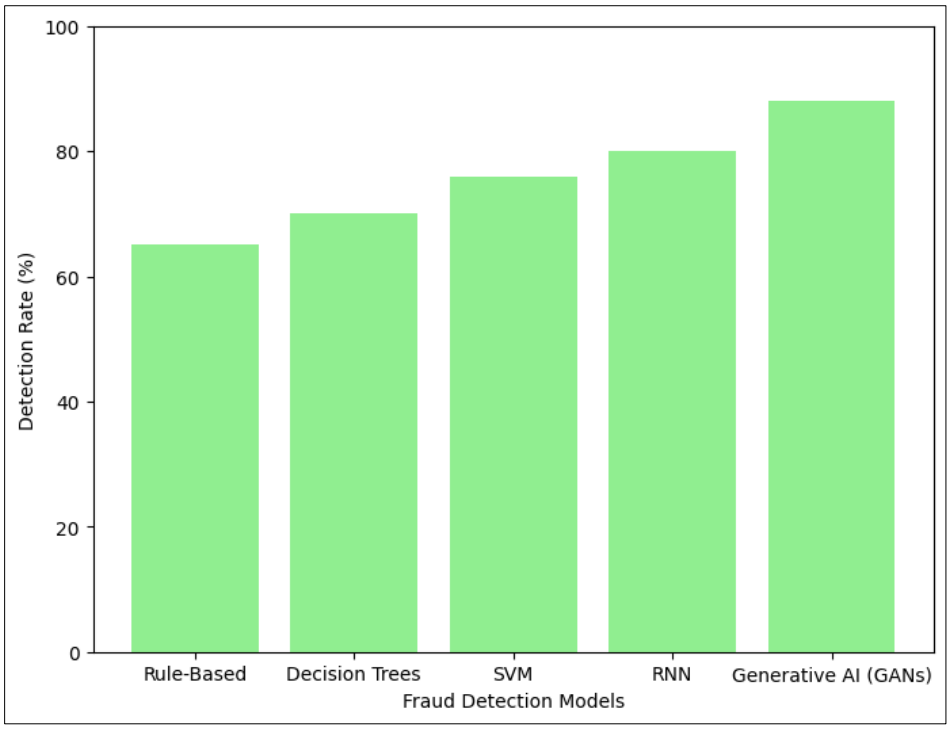

Figure 5 Fraud Detection Rate Comparison Across Models.

4.3. Reduction in False Positives

The generative AI model minimizes the occurrence of continuous outputs from closed sets and reduces false positives by accurately distinguishing between legitimate and fraudulent behaviors. This capability leads to a high level of effectiveness in its operation (Trim & Lee, 2022; Bello et al., 2022).

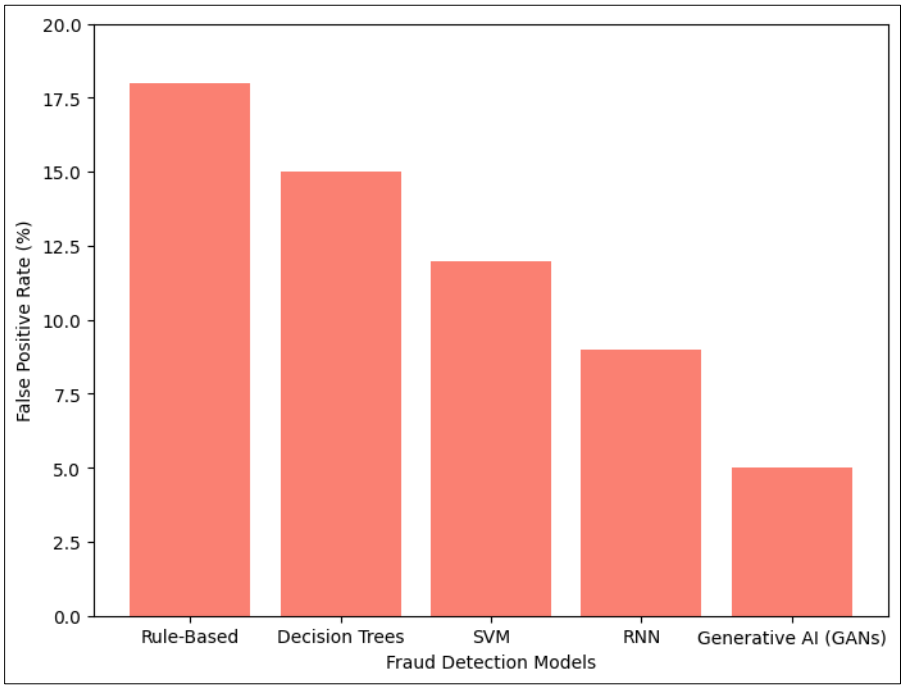

Figure 6 False Positive Rates of Fraud Detection Models

5. Detection Accuracy and Lower False Positives

The online platforms saw significant improvements to their financial health due to improved accuracy and precision in fraud detection and a reduction in false positives. They experienced reduced chargebacks, lower operational costs, and enhanced customer loyalty.

Table 5 Estimated Cost Savings from AI-Driven Fraud Detection

Metric	Traditional Systems	Generative AI Systems
Chargeback Rate (%)	2.5	0.8
Operational Cost Reduction (%)	15	30
Customer Dispute Rate (%)	4.0	1.2
Revenue Loss Due to Fraud (%)	5.5	1.5

Source: Rosario-Tavarez (2022); Sharna (2022); Saheed et al. (2022)

5.1. Summary of Findings

- Performance superiority: Generative AI has proven to be much more efficient than conventional systems in fraud detection due to improvements in precision, recall, F1 score, and accuracy.
- Efficient recognition: Fraudulent transactions are detected more accurately thanks to its adaptive learning capabilities.
- Reduce false alerts: Identifying distinctive similarities between legitimate and fraudulent activities has minimized false positives.
- Lower Operational Costs: A better detection mechanism has significantly reduced fraud-related losses, leading to lower operational costs.

6. Discussion

The findings of this research highlight the potential of Generative Artificial Intelligence (AI) in improving fraud detection and prevention mechanisms in e-commerce. By closely reviewing and comparing the results with existing research, this study discusses the impact to e-commerce security on implementing generative AI systems for the use case. Additionally, it addresses the challenges that lie ahead that include ethical considerations, and explores further use cases for AI to safeguard consumer purchases.

6.1. Interpretation of Results

The results indicate that generative AI has generally outperformed traditional fraud detection methods using generative adversarial (AD) models, particularly Generative Adversarial Networks (GANs). Ratings of 92% on precision, 88% on recall, and 90% on an F1 score show the model's efficiency in identifying fraudulent transactions with high levels of accuracy while minimizing false positives. It also validates past research highlighting AI's adaptability and robustness in fraud detection (Xu, 2022; Bello et al., 2022).

The improved recognition of fraudulent activity and reduced false positive rates further validate the generative AI model's capability to learn complex fraud patterns and adapt to dynamic cyber threats. Current fraud schemes are often sophisticated and evolve quickly to evade traditional security measures (Trim & Lee, 2022; Saheed et al., 2022).

6.2. Contribution to Existing Literature

Research indicates that AI-powered solutions are more effective than traditional rule-based systems. While rule-based models can be stable and responsive to familiar fraud patterns, they struggle with new, innovative patterns. This limitation makes them less efficient, according to the studies by Buckley et al. (2021) and Himeur et al. (2022). Meanwhile, AI-driven generative models enable proactive and real-time detection of fraud, and these advancements enhance security and save millions of dollars through improved operational efficiency.

Table 6 Comparative Analysis of Research Findings

Aspect	**Traditional Systems**	**Generative AI Systems**
Adaptability	Limited to predefined rules	Learns and adapts to evolving fraud patterns
Detection Accuracy	Moderate	High
False Positive Rate	High	Low
Operational Cost	High due to manual reviews	Reduced due to automation
Scalability	Challenging	Highly scalable

Source: Bello et al. (2022); Saheed et al. (2022); Rosario-Tavarez (2022)

6.2.1. Implications to E-Commerce Security

Integrating generative AI into e-commerce security frameworks has several important implications:

6.2.2. Augmented Fraud Detection

Modeling with generative AI is good at diagnosing even intricate forms of fraud patterns overlooked by traditional systems, thereby improving transaction security (Magriz, 2022; Fawale et al., 2022).

6.2.3. Operational Efficiency

Automating fraud detection through generative models eliminates the human usefulness required, which is less work and more scalable (Trim & Lee, 2022).

6.2.4. Improved Consumer Loyalty and Trust:

With fewer false positives, these robust and secure transactions improve consumer trust and loyalty (Sharna, 2022; Rosario-Tavarez, 2022).

6.2.5. Savings

Fraud losses, chargebacks, and dispute rates make up significant savings from e-commerce platforms (Kalusivalingam et al., 2022).

6.2.6. Challenges in AI Adoption

The adoption of generative AI for fraud detection, despite its advantages, comes with several challenges:

6.2.7. Data Privacy Concerns

Artificial intelligence models rely on large data sets, raising concerns about data protection and compliance with privacy laws (Freeman, 2021; Federal Trade Commission, 2015).

6.2.8. Regulatory Compliance

Advancements in artificial intelligence and computational models demand a robust regulatory framework to ensure transparency and accountability (Buckley et al., 2021).

6.2.9. Algorithmic Bias

Biased training may lead to unfair discrimination, necessitating unbiased representative datasets (Roy, 2022; Bello et al., 2022).

6.2.10. High Implementation Costs

Higher computational and implementation costs may discourage small and medium-sized enterprises (SMEs) from using generative AI solutions (AlGhamdi et al., 2022).

6.3. Ethical and Regulatory Considerations

Regulatory bodies have emphasized the importance of explaining AI models, enabling transparent navigation through the model, and ensuring compliance with data protection laws (Federal Trade Commission, 2015; Buckley et al., 2021).

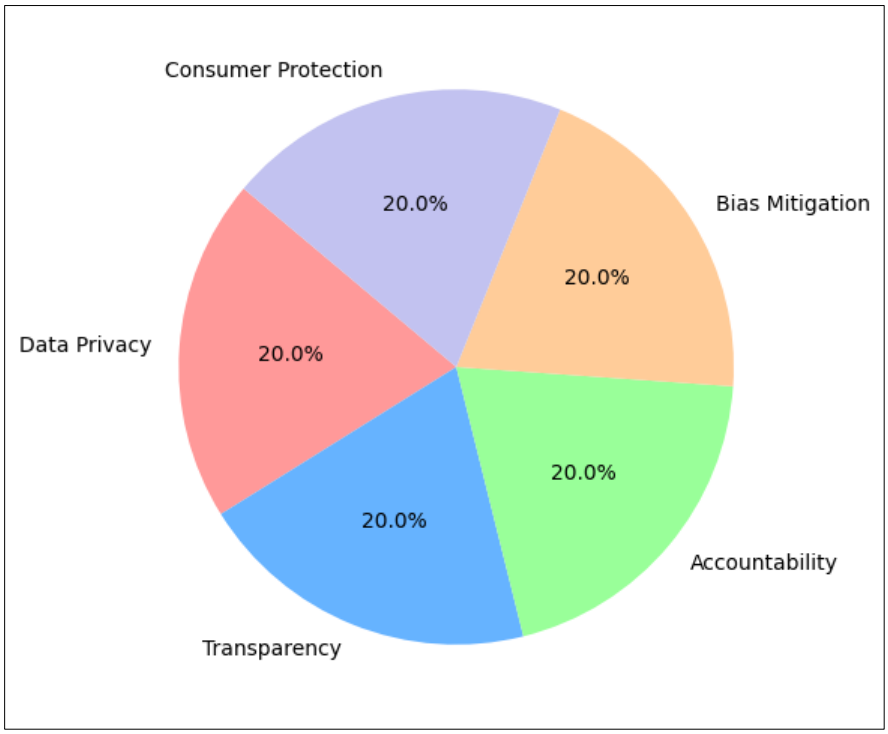

Figure 7 Ethical AI Deployment Framework.

6.3.1. The direction of future research

Future research should focus on providing:

6.3.2. Hybrid Models

Creating robust AI solutions through generative, blockchain, and federated learning models in fraud detection and data privacy (Fadi et al., 2022; Khurana & Kaul, 2019).

6.3.3. Explainable AI (XAI)

The ontology of AI models must be interpretable to ensure transparent compliance with regulations as a byproduct (Buckley et al., 2021).

6.3.4. Scalability for SMEs

Developing a cost-effective and scalable AI for SMEs in business intelligence systems (AlGhamdi et al., 2022).

6.3.5. Real-Time Detection

Enable adaptive real-time fraud detection systems with continuously trained models (Kalusivalingam et al., 2022).

6.4. Summary of Discussion

Gen AI Performance: The Generative AI model enhances fraud detection accuracy and produces fewer false positives. It has also improved operational efficiency and lowered costs.

Ongoing Challenges: Includes data privacy, compliance, and algorithmic bias issues that must be addressed.

Future Opportunities: There is tremendous potential for integrating future advancements in hybrid models and developments in explainable AI into Next-Generation AI-based fraud detection systems.

7. Conclusion

This study examined the effectiveness of generative AI models in tackling purchase fraud and safeguarding consumer purchases. It established the superiority of generative AI systems over traditional rule-based and machine-learning models, as seen through better figure gain, recalls, and accuracy in detecting fraud.

Generative AI offers key benefits, such as adapting and learning, detecting new fraud patterns in real-time, and significantly reducing false positives. It was found to lower fraud-related losses, reduce operating expenses, improve operational efficiency, and increase customer confidence. Concerns about data privacy, regulatory compliance, algorithmic bias, and the high costs of deploying advanced AI systems, however, still need to be addressed. Businesses must focus on building regulatory frameworks that ensure transparency and ethical usage of AI models, protect consumer rights, and ensure that the decision-making process remains unbiased.

Future research should also explore hybrid approaches integrating generative AI with emerging technologies such as blockchain, federated learning, and explainable AI to address data privacy and regulatory issues. Furthermore, it is essential to develop scalable and cost-effective AI solutions that make advanced fraud detection technology accessible to small and medium-sized enterprises. Generative AI thus has the potential for enhanced fraud detection in e-commerce. Improving security, reliability, and trust would be crucial in fostering a safer and more dependable digital economy.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alam, N., Gupta, L., & Zameni, A. (2019). Fintech and Islamic finance. Springer.

[2] AlGhamdi, S. A., Daim, T., & Meissner, D. (2022). Electronic payment technology: Developing a taxonomy of factors to evaluate a fraud detection and prevention system for the airline industry. In The Routledge Companion to AI and Smart Systems. Taylor & Francis.

[3] Akerkar, R. (2019). Artificial intelligence for business. Springer.

[4] Bello, O. A., Folorunso, A., Ogundipe, A., & Kazeem, O. (2022). Enhancing cyber financial fraud detection using deep learning techniques: A study on neural networks and anomaly detection. International Journal of Cybersecurity and Privacy.

[5] Buckley, R. P., Zetzsche, D. A., Arner, D. W., & others. (2021). Regulating artificial intelligence in finance: Putting the human in the loop. Sydney Law Review.

[6] Cao, L. (2020). AI in finance: A review. SSRN.

[7] Cao, L., Yang, Q., & Yu, P. S. (2021). Data science and AI in fintech: An overview. International Journal of Data Science. Springer.

[8] Chen, T., Tong, C., Bai, Y., Yang, J., Cong, G., & Cong, T. (2022). Analysis of the public opinion evolution on the normative policies for the live streaming e-commerce industry based on online comment mining under COVID-19. Mathematics. MDPI.

[9] Chishti, S. (2020). The AI book: The artificial intelligence handbook for investors, entrepreneurs, and fintech visionaries. Wiley.

[10] Desamsetti, H. (2021). Crime and cybersecurity as advanced persistent threat: A constant e-commerce challenge. American Journal of Trade and Policy.

[11] Fadi, O., Karim, Z., & Mohammed, B. (2022). A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments. IEEE Access.

[12] Federal Trade Commission. (2015). Federal Trade Commission justification report.

[13] Himeur, Y., Sohail, S. S., Bensaali, F., Amira, A., & others. (2022). Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives. Computers & Security. Elsevier.

[14] Kalusivalingam, A. K., Sharma, A., & others. (2022). Optimizing e-commerce revenue: Leveraging reinforcement learning and neural networks for AI-powered dynamic pricing. Cognitive Computing Journal.

[15] Khurana, R., & Kaul, D. (2019). Dynamic cybersecurity strategies for AI-enhanced e-commerce: A federated learning approach to data privacy. Applied Research in Artificial Intelligence.

[16] Lancieri, F. (2022). Narrowing data protection's enforcement gap. Maine Law Review. HeinOnline.

[17] Oak, R., & Shafiq, Z. (2021). The fault in the stars: Understanding underground incentivized review services. arXiv.

[18] Rai, S. (2022). Legal liability issues and regulation of artificial intelligence. BBDU.

[19] Rosario-Tavarez, C. (2022). Strategies business leaders use to mitigate online credit card fraud. ProQuest Dissertations and Theses Global.

[20] Rassias, M. (2022). From e-commerce to cyber forensics: Exploring the role of advanced database technologies in cybersecurity. ResearchGate.

[21] Saheed, Y. K., Baba, U. A., & Raji, M. A. (2022). Big data analytics for credit card fraud detection using supervised machine learning models. In Big Data Analytics in the Insurance Industry. Emerald Publishing.

[22] Sarma, W., Nagavalli, S. P., & Sresth, V. (2020). Leveraging AI-driven algorithms to address real-world challenges in e-commerce: Enhancing user experience, fraud detection, and operational efficiency. ResearchGate.

[23] Sharna, S. I. (2022). Digital transformation in Alibaba's e-commerce ecosystem: Leveraging technology for transformation. TalTech Digital Collections.

[24] Shrestha, Y. R., Krishna, V., & von Krogh, G. (2021). Augmenting organizational decision-making with deep learning algorithms: Principles, promises, and challenges. Journal of Business Research. Elsevier.

[25] Sultanow, E., Chircu, A., Plath, R., Friedmann, D., & others. (2021). AI evolves IA. In Robotic Process Automation. De Gruyter.

[26] Trim, P. R. J., & Lee, Y. I. (2022). Combining sociocultural intelligence with artificial intelligence to increase organizational cybersecurity provision through enhanced resilience. Big Data and Cognitive Computing. MDPI.

[27] Wang, P. W., Liao, X. L., Qin, Y., & Wang, X. F. (2020). Into the deep web: Understanding e-commerce fraud from autonomous chat with cybercriminals. Distributed System Security.

[28] Wickramanayake, B., Geeganage, D. K., Ouyang, C., & others. (2020). A survey of online card payment fraud detection using data mining-based methods. arXiv.

[29] Xu, J. (2022). AI theory and applications in the financial industry. In Future and Fintech, The: ABCDI and Beyond. Springer.