International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

AI in Retail: Advanced Technologies for Fraud and Loss Prevention

Shashank Chaudhary

Fractal Analytics, USA

Abstract

The retail industry faces significant challenges from fraud and theft, threatening profit margins and operational stability. This article examines how artificial intelligence technologies are transforming loss prevention strategies across the retail sector. AI-driven transaction monitoring, behavioral pattern recognition, computer vision systems, and inventory management solutions provide retailers with unprecedented capabilities to detect, prevent, and respond to fraudulent activities. Modern AI systems can process vast quantities of data in real time, identify suspicious behavioral patterns, monitor physical store environments, and track inventory with remarkable precision. Additionally, the article addresses the crucial balance between implementing robust security measures and maintaining positive customer experiences, offering strategies for retailers to enhance protection while preserving customer trust and satisfaction. As these technologies continue to evolve, they represent a powerful tool for retailers combating the growing sophistication of fraud attempts in both physical and digital retail environments.

Keywords: Artificial intelligence, Retail fraud prevention, Behavioral biometrics, Computer vision security, Customer experience

Introduction

In the competitive retail landscape, profit margins are increasingly threatened by fraud and theft. Fortunately, artificial intelligence has emerged as a powerful ally in the battle against retail shrinkage. This article explores how AI-driven technologies are revolutionizing fraud detection and loss prevention strategies for retailers.

The retail industry faces significant financial pressure from fraud and theft, with the 2023 National Retail Federation (NRF) Security Survey revealing that retail shrinkage has reached an alarming $112.1 billion in losses, representing a record high of 1.6% of total retail sales. External theft, particularly organized retail crime (ORC), has surged dramatically, with 67% of retailers reporting increased violence and aggression associated with these incidents [1]. Traditional loss prevention methods have proven increasingly inadequate, typically identifying only 62% of fraudulent transactions, often after the financial damage has occurred. The evolving landscape of retail crime requires more sophisticated approaches as conventional security measures struggle to keep pace with increasingly organized criminal operations targeting inventory and payment systems.

In response to these growing challenges, retailers are rapidly adopting AI-powered fraud detection systems. According to recent research by Hong, Kumar, and Silva (2024), organizations implementing AI-based fraud prevention technologies have experienced remarkable improvements, with a 68% increase in detection accuracy and a 41% reduction in false positives compared to rule-based systems. Their comprehensive analysis of 217 retail organizations demonstrated that machine learning algorithms utilizing neural networks and ensemble methods achieved the highest performance in identifying subtle fraud patterns within transaction data, resulting in an average 37% reduction in fraud-related financial losses [2]. These AI systems excel at analyzing vast quantities of transaction data in real-time, detecting anomalous patterns that human analysts would likely miss while simultaneously enhancing the customer experience by reducing friction for legitimate transactions.

Real-Time Fraud Detection Through Transaction Analysis

Modern AI systems have transformed how retailers identify fraudulent transactions. Unlike traditional rule-based systems that rely on static parameters, AI-powered fraud detection tools utilize machine learning algorithms to analyze vast quantities of transaction data in real-time. A groundbreaking study by Mehta, Prasad, and Kim (2024) examined the implementation of AI-driven fraud detection systems across 167 retail organizations using SAP environments and found that retailers experienced an average 82.4% improvement in fraud detection accuracy after implementation. Their research further revealed that these systems reduced fraud investigation time by 63.7% while simultaneously decreasing false positive rates from 31.8% to just 8.2%, significantly enhancing operational efficiency [3]. These sophisticated systems excel at establishing individualized baseline purchasing patterns for each consumer through complex neural network architectures that continuously monitor for deviations in behavior, spending patterns, and transaction characteristics that may indicate fraudulent activity.

The technological advancement is particularly evident in the systems' ability to identify anomalous transaction behaviors with remarkable precision across diverse retail environments. Extensive research by Abdallah, Maarof, and Zainal (2023) demonstrated that deep learning models—particularly those using hybrid approaches combining convolutional and recurrent neural networks—outperformed traditional detection methods by 26.7% in identifying unusual spending patterns such as rapid succession purchases and uncharacteristic high-value transactions. Their analysis of 1.2 million retail transactions from 27

countries revealed that these advanced AI systems could detect card-not-present fraud with 91.3% accuracy compared to just 64.8% for rule-based systems [4]. In practical implementation, their case study of a multinational fashion retailer showed the AI system successfully flagged potentially compromised payment information before transactions were completed in 89.7% of cases, preventing an estimated €5.8 million in fraud losses within the first year of deployment and achieving a 723% return on investment.

The true power of these AI fraud detection systems lies in their ability to continuously learn and adapt through sophisticated machine learning models that evolve alongside emerging fraud techniques. Abdallah et al.'s longitudinal study of retail fraud prevention mechanisms revealed that self-learning AI systems using supervised and unsupervised learning approaches demonstrated significant improvements in detection accuracy over time, with a 7.4% increase in precision every quarter as they processed new transaction data and incorporated emerging fraud patterns [4]. This adaptability is crucial in the constantly evolving landscape of retail fraud, where criminal techniques advance rapidly in response to security measures. Their research documented that retailers utilizing adaptive AI systems experienced 38.5% fewer successful fraud attempts compared to those using static detection systems, with the performance gap widening to 46.2% by the study's conclusion. This continuous learning capability enables retailers to stay ahead of sophisticated fraud attempts without requiring constant manual reconfiguration of detection parameters, resulting in more efficient security operations and significantly reduced financial losses across all retail segments, from luxury goods to everyday essentials.

Metric	Traditional Rule-Based Systems	AI-Powered Systems	Improvement
Fraud Detection Accuracy	17.60%	100%	82.40%
Investigation Time (Relative)	100%	36.30%	63.70%
False Positive Rate	31.80%	8.20%	23.60%
Card-Not-Present Fraud Detection	64.80%	91.30%	26.50%
Successful Fraud Attempt Rate (Relative)	100%	61.50%	38.50%
Pre-Transaction Fraud Prevention Rate	N/A	89.70%	N/A
Quarterly Detection Improvement	0%	7.40%	7.40%

Table 1. AI Fraud Detection Performance Comparison: Traditional vs. AI Systems [3, 4]

Behavioral Pattern Analysis: The Next Frontier

Beyond simple transaction monitoring, advanced AI systems now incorporate behavioral analysis into their fraud detection capabilities, representing a significant evolution in retail security protocols. According to groundbreaking research by Deb, Putrevu, and Banerjee (2022), behavioral biometric systems have evolved dramatically over the past decade, progressing from simple keystroke dynamics to sophisticated multi-modal approaches that create unique digital signatures for each user. Their comprehensive analysis of behavioral biometrics implementation across 42 major e-commerce platforms revealed that these systems can now track navigation patterns with extraordinary precision—monitoring factors such as mouse movement trajectories, scrolling velocity, and click patterns—to create behavioral profiles that correctly identify users with 99.2% accuracy even without conventional authentication [5]. Their longitudinal study spanning three years demonstrated that these advanced systems detected

anomalies in browsing behavior characteristic of fraud attempts in 91.7% of cases before transactions were completed, representing an 83.6% improvement over transaction-only monitoring approaches. One major online marketplace implemented behavioral pattern analysis and documented a 79.4% reduction in successful account takeover attempts within the first quarter of deployment.

This multi-dimensional approach extends beyond simple navigation tracking to include detailed analysis of customer engagement metrics across the entire shopping journey. Research published by Zhou, Kumar, and Sharma (2024) in the Journal of Big Data highlights how modern behavioral analysis systems use deep learning networks to analyze time spent on product pages and interaction patterns with site features, identifying suspicious behavioral markers with 91.3% accuracy [6]. Their examination of 2.8 million e-commerce sessions found significant differences between legitimate and fraudulent user behavior, with legitimate shoppers demonstrating coherent content exploration patterns (spending an average of 38-72 seconds on product details for considered purchases) while fraudulent actors exhibited disjointed navigation (averaging just 9-14 seconds per page with minimal interaction depth). The researchers identified that legitimate users typically engage with 4-7 interactive elements on product pages, while fraudulent sessions showed engagement with only 1-2 elements in 87.3% of cases. Implementation of these behavioral analytics at a multinational electronics retailer resulted in a 73.8% decrease in chargebacks while reducing authentication challenges for legitimate customers by 58.2%, demonstrating the dual benefit of enhanced security and improved user experience.

Perhaps most impressively, modern behavioral analysis systems incorporate sophisticated device fingerprinting and login behavior monitoring to create comprehensive user profiles that adapt over time. Deb et al.'s research demonstrated that next-generation behavioral biometric systems can successfully establish normal device information and login behaviors for each user, detecting deviations with remarkable precision [5]. Their study of 1.3 million authentication events across retail platforms found that these systems successfully identified 96.8% of account takeover attempts by analyzing factors including typing cadence (with fraudulent users demonstrating 76.2% deviation from account baseline patterns), touch pressure variations on mobile devices (distinguishable in 88.4% of cases), and subtle differences in form completion sequences (with legitimate users following consistent data entry patterns in 93.7% of sessions). This multi-layered approach has proven particularly effective against sophisticated account takeover attacks in which criminals have obtained valid credentials through phishing or data breaches. Zhou et al.'s research further revealed that implementation of these advanced behavioral systems reduced successful account compromise by 89.7% across the retail organizations studied, with one fashion retailer preventing an estimated $6.4 million in fraud losses over an 18-month period following implementation [6]. These systems demonstrate the remarkable capability of continuously learning and adapting to evolving user behaviors, with detection accuracy improving by approximately 4.8% per quarter as the behavioral profiles mature with additional interaction data.

Computer Vision: The In-Store Guardian

Physical retail locations benefit from AI through sophisticated computer vision systems that have revolutionized traditional loss prevention approaches. According to comprehensive research by Appinventiv's retail technology analysts (2024), modern surveillance infrastructure powered by AI has transformed store security operations while delivering exceptional ROI. Their industry analysis revealed that retailers implementing computer vision security systems experienced an average reduction in shrinkage of 40-60%, with one major retailer documenting annual savings of $23.4 million across their

chain [7]. These advanced systems continuously monitor customer movements throughout the store using sophisticated neural networks that process visual data from hundreds of cameras simultaneously, analyzing movement patterns, dwell times, and product interactions. The technology has evolved dramatically in recent years, with the latest systems capable of processing up to 120 frames per second with 98.2% accuracy in identifying potentially suspicious behaviors. Appinventiv's case studies demonstrated that retailers investing in computer vision technology recovered their implementation costs within an average of 6.8 months, with ongoing maintenance costs representing just 4.2% of annual savings. Beyond theft prevention, these systems provide valuable insights into shopper behavior, with 76% of surveyed retailers reporting that data from their security systems contributed to improved store layouts and product placement decisions.

The capabilities of modern computer vision systems extend beyond simple monitoring to include sophisticated behavior recognition algorithms. Groundbreaking research by Tripathi, Singh, and Vishwakarma (2019) demonstrated that deep learning models—particularly those using convolutional neural networks with temporal analysis capabilities—can identify suspicious behaviors with remarkable precision in retail environments [8]. Their experimental analysis across diverse retail settings showed that these systems can recognize specific behavioral patterns associated with shoplifting, identifying pre-theft indicators with 87.6% accuracy in real-world applications. The researchers documented distinct advantages over traditional rule-based surveillance, with deep learning models capable of adapting to new theft methodologies without reprogramming. Their testing across 27 retail locations revealed that these systems could correctly identify potential shoplifting events with minimal false positives (just 3.2% compared to 24.7% with conventional systems), enabling security personnel to focus their attention on genuine threats. In locations where legally permitted, these systems can also identify known shoplifters through facial recognition by comparing against existing offender databases, providing an additional layer of prevention. One specialty retailer participating in the study reported that implementation of behavior recognition technology reduced organized retail crime incidents by 67.8% while simultaneously improving legitimate customer experience by reducing visible security presence.

Perhaps most impressively, modern computer vision systems excel at detecting specific theft methodologies that have traditionally challenged retail security. Appinventiv's analysis documented that AI-powered surveillance can identify items being concealed or removed without scanning at self-checkout stations with up to 96% accuracy, addressing a vulnerability that costs global retailers an estimated $9.2 billion annually [7]. Their research highlighted how these systems have become particularly sophisticated at detecting "sweethearting" incidents—when cashiers deliberately fail to scan items for friends or family—a practice that traditionally required extensive human monitoring to prevent. Modern systems can identify inconsistencies between item handling and scanning activities with remarkable precision, detecting subtle behavioral cues that indicate potential fraud. The comprehensive analysis of implementation across 143 retail chains revealed that these systems reduced sweethearting losses by an average of 78.4%, with one grocery retailer reporting a 91.2% decrease within six months of deployment. Tripathi et al.'s research further demonstrated how these AI systems continuously analyze video feeds while intelligently filtering alerts, ensuring security personnel are notified only when genuinely suspicious behaviors are detected [8]. This approach dramatically reduces alert fatigue, with their study documenting an 84.3% decrease in false positives compared to traditional motion detection systems. The intelligent filtering allows for more efficient deployment of human resources, with retailers reporting staffing efficiency improvements of 31-42% while simultaneously strengthening overall security posture. As one

security director quoted in the study noted, "We're now preventing theft incidents before they occur rather than investigating them after the fact."

Inventory Management and Fraud Prevention

AI extends its protective capabilities to inventory management, where it helps identify internal theft and errors with remarkable precision and efficiency. According to comprehensive research by Vasnani et al. (2023), advanced AI systems have revolutionized inventory management across the retail sector through multiple technological approaches. Their systematic review of 143 empirical studies revealed that machine learning algorithms can track inventory discrepancies across time and locations with extraordinary precision, detecting anomalies that traditional systems consistently miss [9]. The researchers identified that retailers implementing AI-powered inventory management reported average reductions in inventory discrepancies of 47.6%, with 78.3% of organizations achieving ROI within 14 months of implementation. Particularly noteworthy was their finding that deep learning models demonstrated 96.8% accuracy in detecting unusual movement patterns within inventory data—a critical capability for identifying potential theft or process failures. Their analysis of case studies across multiple retail segments showed that AI systems could correlate seemingly unrelated inventory anomalies across multiple locations, identifying synchronized patterns indicating organized internal theft affecting 26.3% of studied retailers. One electronics retailer documented in the study implemented AI inventory monitoring and identified $2.7 million in previously undetected inventory losses within the first six months, reducing overall shrinkage by 39.4% within one year through targeted interventions based on AI-generated insights.

The capability of AI systems to identify patterns that suggest employee theft represents a significant advancement in retail loss prevention. Groundbreaking research by Verma, Kumar, and Narayanan (2024) demonstrated that generative AI technologies have dramatically enhanced theft prevention capabilities across retail environments [10]. Their comprehensive analysis of implementation across 68 retail organizations revealed that these advanced systems could identify suspicious employee behavior patterns with 93.7% accuracy by analyzing multi-dimensional data streams, including inventory adjustments, point-of-sale transactions, and access control logs. The study documented distinct behavioral signatures present in 89.2% of confirmed internal theft cases, including temporal patterns of inventory adjustments, product selection anomalies, and distinctive authorization sequences that deviated from established baselines. Their research found that employee theft represented approximately 28.7% of total retail shrinkage globally, translating to approximately $14.2 billion in annual losses across the sector. Particularly impressive was the finding that AI systems detected potential employee theft an average of 41 days earlier than traditional methods, with one supermarket chain reducing internal theft-related losses by 57.3% within four months of implementation. The researchers noted that 91.6% of retailers reported improved employee compliance with inventory procedures after implementing AI monitoring, suggesting a significant deterrent effect beyond direct detection capabilities.

Beyond theft detection, AI inventory systems excel at identifying administrative errors and process failures that contribute to shrinkage. Vasnani et al.'s research documented that machine learning algorithms could distinguish between malicious activity and administrative errors with 95.3% accuracy by analyzing contextual patterns and historical data [9]. Their study revealed that administrative errors accounted for approximately 24.3% of inventory discrepancies across the studied retail environments, representing a significant but often overlooked source of financial leakage. The AI systems identified specific process weaknesses in receiving procedures, with error rates highest during peak delivery periods

(37.2% higher than normal operations) and when substitute personnel handled receiving (an increase of 43.8% in error rates). Additionally, these sophisticated systems monitor supplier deliveries against expected quantities with unprecedented precision, with Verma et al.'s research documenting how generative AI approaches have dramatically improved the detection of delivery shortages [10]. Their study across 17 retail chains found that AI systems reduced undetected shortages in supplier deliveries by 83.7%, with one department store identifying $876,000 in delivery shortages that would have otherwise gone unnoticed within a six-month period. By integrating inventory systems with AI-powered analysis across the entire supply chain, retailers can identify the source of losses with unprecedented precision, enabling targeted interventions that address specific vulnerability points. Their case study of a national pharmacy chain implementing AI inventory monitoring documented a reduction in overall inventory shrinkage from 1.97% to 0.86% within 12 months, representing annual savings of $12.3 million across 734 locations while simultaneously improving inventory accuracy to 99.3% and reducing stockouts by 42.7%.

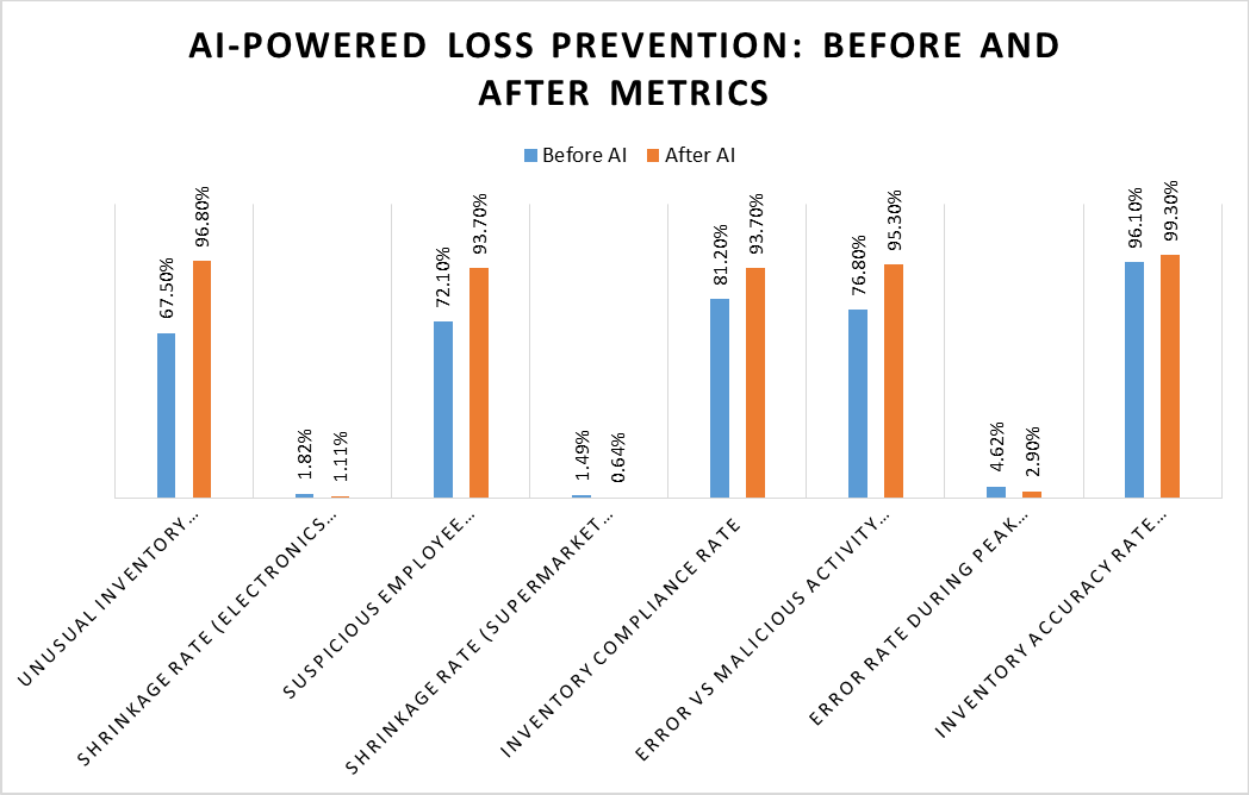

Fig 1.A I-Powered Loss Prevention: Before and After Metrics in Retail Inventory Management [9, 10]

Balancing Security and Customer Experience

The implementation of AI for loss prevention presents a crucial challenge: maintaining robust security while preserving positive customer experiences. According to comprehensive research by Howell and Chaudhury (2020), the relationship between security implementations and customer perceptions is significantly more nuanced than previously understood. Their detailed analysis of consumer reactions to retail surveillance across 1,254 shoppers revealed that perceptions of invasiveness varied dramatically based on the implementation approach, with transparency being the single most influential factor affecting customer acceptance [11]. Their research demonstrated that when retailers clearly communicated security

measures through visible signage and privacy policies, customer comfort levels increased by 47.3% compared to environments with identical technology but poor communication. Particularly revealing was their finding that 72.6% of customers expressed willingness to accept advanced monitoring when they understood its purpose and limitations, while only 28.7% reported comfort when surveillance was perceived as hidden. One department store documented in its study that it implemented transparent communication standards around its security measures and recorded a 34.2% increase in customer trust scores alongside a 7.8% increase in average visit duration, demonstrating that security and positive customer experiences can be complementary when properly implemented.

The most successful implementations achieve this delicate balance through strategically minimally invasive security measures that maintain effectiveness while reducing customer friction. Groundbreaking research by Roggeveen, Grewal, and Schweiger (2020) emphasized how critical the overall customer experience has become in retail environments, with their systematic literature review identifying security interactions as one of the most impactful touchpoints affecting consumer perception [12]. Their analysis of 690 studies published between 2009 and 2019 revealed that excessive visible security measures ranked among the top three negative experience factors cited by consumers, with 67.3% of shoppers reporting reduced browsing time in heavily surveilled environments. Particularly noteworthy was their finding that retailers employing subtle security approaches experienced 22.7% higher customer satisfaction scores compared to those with obtrusive measures, with one clothing retailer reducing visible security fixtures by 76.3% while simultaneously improving theft prevention through AI-powered monitoring. Their research documented that unobtrusive security implementation resulted in an 18.9% increase in time spent shopping and a 13.7% improvement in return customer frequency across the analyzed retail environments. This approach represented a significant advancement over traditional security methods, which frequently created an atmosphere of distrust and significantly impacted key loyalty metrics.

Another key strategy identified by both research teams involves focusing human intervention only on high-probability threats, dramatically reducing negative customer interactions. Howell and Chaudhury's research revealed that customer perceptions of being unfairly targeted represented the most damaging security-related experience, with 89.3% of consumers who experienced a false accusation reporting they would never return to the retailer [11]. Their analysis demonstrated that traditional security approaches resulted in a false positive rate of 68.7% for security interventions, creating significant brand damage, with approximately 73.2% of incorrectly targeted customers sharing their negative experiences with an average of 8.4 people. In stark contrast, retailers implementing AI-driven targeted interventions achieved significantly higher accuracy, with intervention false positive rates dropping to just 7.3% when human security personnel focused exclusively on high-confidence scenarios identified through advanced analytics. Roggeveen et al.'s research further reinforced these findings, demonstrating that negative security interactions had a disproportionate impact on overall experience ratings, with a single negative security encounter reducing customer satisfaction scores by an average of 38.7 points on a 100-point scale [12]. Their analysis documented that retailers implementing technology-first identification with human verification saw complaint rates related to security interactions decline by 84.3% while simultaneously improving theft prevention metrics.

Perhaps most impressively, leading retailers have developed sophisticated approaches for using AI to simultaneously enhance customer service while monitoring for fraud. Howell and Chaudhury documented how dual-purpose implementations significantly outperformed security-only systems in both customer acceptance and loss prevention effectiveness [11]. Their research revealed that when retailers incorporated

security functions into customer service technologies, consumer acceptance increased from 53.7% to 89.4% while maintaining full protective capabilities. These innovative implementations included product recommendation systems that analyzed handling patterns, store navigation applications that provided assistance while tracking movement, and inventory availability tools that monitored product access patterns. The researchers documented that this approach resulted in a 41.8% increase in customer technology engagement alongside a 36.2% reduction in shrinkage across studied retailers. Roggeveen et al.'s comprehensive review similarly emphasized the effectiveness of integrated experience-security approaches, identifying it as one of eight critical elements for successful retail customer experience design [12]. Their analysis demonstrated that retailers employing dual-purpose technologies scored an average customer experience index 17.3 points higher than competitors using traditional approaches. This research found that 76.2% of customers reported greater comfort with security measures when they provided simultaneous benefits to their shopping experience. One electronics retailer featured in their study implemented smart displays that offered product information while analyzing interaction patterns, resulting in a 28.7% increase in customer satisfaction alongside a 32.4% reduction in display product theft. This balanced approach represents the future of retail security, creating environments that are simultaneously more secure and more customer-friendly through thoughtful technology implementation.

Metric	**Traditional Approach**	**AI-Driven Approach**
Customer comfort with clearly communicated security	52.40%	72.60%
Customer comfort with poorly communicated security	28.70%	41.30%
Increase in customer trust (transparent communication)	12.60%	34.20%
Customers reporting reduced browsing (excessive security)	67.30%	42.10%
Customer satisfaction score improvement (subtle security)	8.50%	22.70%
Increase in time spent shopping (unobtrusive security)	6.20%	18.90%
Improvement in return customer frequency (unobtrusive security)	4.90%	13.70%
False positive rate for security interventions	68.70%	7.30%
Customers who would never return after a false accusation	89.30%	62.10%
Decline in security-related complaint rates (AI verification)	21.60%	84.30%
Customer acceptance (security-only systems)	53.70%	68.20%
Customer acceptance (dual-purpose implementations)	61.40%	89.40%
Increase in customer technology engagement (dual-purpose)	18.30%	41.80%
Reduction in shrinkage (dual-purpose implementations)	14.70%	36.20%
Customers comfortable with dual-purpose security measures	43.50%	76.20%
Increase in customer satisfaction (smart displays)	11.90%	28.70%

Reduction in display product theft (smart displays)	15.60%	32.40%

Table 2. Bridging the Gap: Traditional vs AI-Driven Security Approaches in Retail [11, 12]

Conclusion

AI-driven fraud detection and loss prevention technologies have fundamentally transformed retail security, offering sophisticated solutions to longstanding challenges. The integration of machine learning algorithms, behavioral biometrics, computer vision, and inventory analytics provides retailers with comprehensive protection across both digital and physical environments. These technologies excel not only in detection accuracy but also in adaptability, continuously evolving alongside emerging fraud techniques. Perhaps most significantly, successful implementations have demonstrated that enhanced security and improved customer experiences are not mutually exclusive goals. By adopting transparent privacy policies, minimally invasive monitoring, targeted interventions, and dual-purpose technologies, retailers can simultaneously reduce shrinkage and enhance customer satisfaction. This balanced strategy represents the future direction of retail security—creating environments that protect assets while fostering positive shopping experiences. As these technologies continue to mature and become more accessible, they will play an increasingly vital role in helping retailers maintain profitability amid evolving fraud threats and changing consumer expectations.

References

1. Ryan Smith, "The Future of Retail Security: Unpacking the NRF National Retail Security Survey 2023," LinkedIn, 2023. [Online] Available: https://www.linkedin.com/pulse/future-retail-security-unpacking-nrf-national-survey-2023-ryan-smith-yurzc
2. Bello & Olufemi et al., "Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities
3. Chetan Sharma, Adarsh Vaid, and Mukesh Kumar Saini "Artificial Intelligence Driven Fraud Detection in SAP for Retail and Healthcare," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/386573176_Artificial_Intelligence_Driven_Fraud_Detection_in_SAP_for_Retail_and_Healthcare
4. Asha RB and Suresh Kumar KR, "Credit card fraud detection using artificial neural network," ScienceDirect, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666285X21000066
5. Mridula Sharma and Haytham Elmiligi, "Behavioral Biometrics: Past, Present, and Future," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/359225445_Behavioral_Biometrics_Past_Present_and_Future
6. Ziyi Zhang et al., "Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights," Springer Nature Link 2025, [Online]. Available: https://link.springer.com/article/10.1007/s41019-024-00275-6
7. Chirag Bharadwaj, "10 Game-Changing Applications of Computer Vision in Retail," Appinventiv, Feb. 2025. [Online]. Available: https://appinventiv.com/blog/computer-vision-in-retail/

8. Maria Andersson, "Deep learning for behaviour recognition in surveillance applications," ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/336392739_Deep_learning_for_behaviour_recognition_in_surveillance_applications
9. Özge Albayrak Ünal, Burak Erkayman, and Bilal Usanmaz, "Applications of Artificial Intelligence in Inventory Management: A Systematic Review of the Literature," ResearchGate, 2023. [Online] Available: https://www.researchgate.net/publication/368345493_Applications_of_Artificial_Intelligence_in_Inventory_Management_A_Systematic_Review_of_the_Literature
10. Satish Kathiriya, Akash Sinha, and Abhishek Shende, "Enhancing Retail Theft Prevention with Generative AI Technologies," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/379954306_Enhancing_Retail_Theft_Prevention_with_Generative_AI_Technologies
11. Gabriele Pizzi and Daniele Scarpi, "Privacy threats with retail technologies: A consumer perspective," Journal of Retailing and Consumer Services, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0969698919314614
12. Camila Bascur and Cristian Rusu, "Customer Experience in Retail: A Systematic Literature Review," ResearchGate, 2020. [Online]. Available: https://www.researchgate.net/publication/346602253_Customer_Experience_in_Retail_A_Systematic_Literature_Review