World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

# Combating credit card skimming on E-Commerce websites: Advanced detection methods and preventative technologies

Smita Verma *

*Brigham Young University, USA.*

World Journal of Advanced Research and Reviews, 2025, 26(01), 1309-1314

Publication history: Received on 24 February 2025; revised on 07 April 2025; accepted on 09 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1153

## Abstract

E-commerce websites face increasing threats from credit card skimming attacks that have evolved from simple code injections to sophisticated operations targeting vulnerabilities in payment systems. These attacks, characterized by malicious code that captures sensitive payment information while allowing websites to function normally, pose significant risks to both businesses and consumers. This article examines the growing landscape of digital skimming threats and advanced detection methodologies, including machine learning-based anomaly detection, integrity-checking systems, automated vulnerability scanning, and real-time transaction monitoring. It further explores preventative technologies such as tokenization, secure payment gateways, web application firewalls, and SSL/TLS encryption. The discussion extends to regulatory compliance frameworks and implementation strategies for comprehensive security, highlighting the multi-layered approach necessary to protect e-commerce platforms in today's digital marketplace.

**Keywords:** Credit Card Skimming; E-commerce Security; Tokenization; Machine Learning Detection; Payment Fraud Prevention

## 1. Introduction

As e-commerce continues to grow worldwide, cybercriminals have increasingly targeted online payment systems through sophisticated skimming attacks. These attacks, which involve injecting malicious code into websites to steal credit card information, pose significant risks to both businesses and consumers. A recent analysis of e-commerce security incidents reveals that skimming attacks have evolved significantly, with a 26% year-over-year increase in detected cases across major retail platforms. The most concerning trend is the shift toward supply chain attacks, where perpetrators target third-party service providers rather than individual merchants directly, affecting thousands of websites simultaneously through a single compromise. Research indicates that 87% of these attacks specifically exploit payment processing pages, with attackers developing increasingly sophisticated methods to evade traditional security tools [1]. The financial consequences extend beyond immediate losses, as the global cost of payment fraud reached $12.8 billion in 2022, while organizations face extended recovery periods averaging 277 days to fully identify and contain payment data breaches. Furthermore, the average total cost of these breaches has climbed to $4.35 million per incident, representing a 2.6% increase from previous years. This cost includes not only direct financial losses but also regulatory penalties, legal fees, customer notification expenses, and significant brand damage that often leads to customer churn rates of up to 3.4% in the retail sector following publicized breaches [2]. These alarming trends underscore the critical importance of implementing multi-layered security approaches that combine both preventative technologies and advanced detection methods to protect merchant systems and consumer financial data in today's digital marketplace.

* Corresponding author: Smita Verma

## 2. The Growing Threat of E-Commerce Skimming

Credit card skimming attacks on e-commerce platforms have become more sophisticated in recent years. Unlike physical skimming devices attached to ATMs or point-of-sale terminals, digital skimming is harder to detect because the website continues to function normally while secretly capturing sensitive payment data. Comprehensive security analyses have revealed that these attacks have evolved from simple code injections to highly sophisticated operations, with incident rates increasing by 117% over the past three years across global e-commerce platforms. The attack vectors predominantly target vulnerabilities in content management systems, third-party plugins, and payment processing modules, with approximately 67% of successful breaches exploiting outdated components or weak authentication mechanisms. Modern skimming operations typically employ obfuscated JavaScript that mimics legitimate payment functionality while secretly duplicating data transmission to attacker-controlled servers, often in regions with minimal cybercrime enforcement. A concerning trend is the persistence of these attacks, which remain undetected for an average of 209 days in mid-sized e-commerce operations that lack sophisticated monitoring tools [3]. When successful, these attacks lead to severe consequences that ripple through the entire e-commerce ecosystem. Consumer financial impact has been extensively documented, with average losses per compromised card reaching $1,156 in high-income markets and victims typically spending between 16-32 hours resolving fraudulent transactions with financial institutions. For merchants, the consequences extend far beyond direct financial liabilities, as security breaches significantly impact customer retention metrics, with studies indicating that 43% of consumers permanently abandon online retailers following publicized data breaches. The financial burden for businesses includes not only regulatory penalties—which may reach up to 4% of annual global turnover under GDPR provisions—but also extensive remediation costs averaging $2.1 million for mid-sized e-commerce operations. These remediation efforts typically include forensic investigation, security infrastructure upgrades, customer notification processes, credit monitoring services, and extensive public relations campaigns necessary to rebuild damaged brand trust. Most concerning is the growing sophistication gap between attack methods and defensive measures, with research indicating that 65% of e-commerce platforms fail to implement adequate client-side security controls that could detect and prevent modern skimming attempts [4].

**Table 1** E-Commerce Credit Card Skimming Attack Metrics (2020-2023) [3, 4]

| **Metric** | **Value** |
|---|---|
| Increase in skimming incident rates (3-year period) | 117% |
| Breaches exploiting outdated components or weak authentication | 67% |
| Average detection time for skimming attacks (days) | 209 |
| Average financial loss per compromised card | $1,156 |
| Time spent by victims resolving fraudulent transactions (hours) | 16-32 |
| Percentage of consumers abandoning retailers after data breaches | 43% |
| Average remediation costs for mid-sized e-commerce operations | $2.1 million |
| Percentage of platforms lacking adequate client-side security controls | 65% |

## 3. Advanced Detection Methods

Several technologies have emerged to help identify and mitigate skimming attacks. Machine Learning-Based Anomaly Detection systems establish baselines of normal website behavior and transaction patterns then alert security teams when deviations occur. By analyzing factors such as script behavior, network connections, and data flow, ML systems can identify suspicious activities that might indicate a skimming attack. Experimental evaluations of these detection systems across diverse e-commerce environments demonstrate significant efficacy, with advanced neural network architectures achieving detection accuracy rates of 96.7% for previously unseen attack patterns. Deep learning models utilizing convolutional and recurrent neural networks have proven particularly effective at capturing the temporal and spatial characteristics of malicious code execution, operating with remarkably low false positive rates of 0.8% when trained on sufficiently diverse datasets. A longitudinal study comparing 23 major online retailers found that those implementing ML-based detection experienced a 78.3% reduction in successful skimming incidents over 24 months, with average breach detection time dramatically reduced from 209 days to approximately 3.2 days. The most promising implementations leverage ensemble models combining both supervised classification algorithms for known attack patterns and unsupervised anomaly detection for novel threats, with hybrid approaches demonstrating 22.7% higher detection rates than single-algorithm solutions for zero-day attacks [5]. Integrity-Checking Systems monitor website code for unauthorized changes. By creating cryptographic hashes of legitimate code, they can detect when critical files have been modified, potentially indicating an injection attack. Research shows these systems have become increasingly sophisticated, with modern implementations using distributed verification across multiple nodes to prevent attackers from compromising the integrity verification system itself. When properly deployed, file integrity monitoring can detect 94.2% of code injection attempts within minutes of modification, compared to the industry average detection time of over 6 months for unmonitored systems. Automated Vulnerability Scanning technologies have shown significant advancement, with comprehensive scanning tools now capable of identifying 87.6% of known vulnerabilities in standard e-commerce configurations. Regular security scans help identify weaknesses in website infrastructure before they can be exploited, with studies showing that organizations performing weekly automated scans experience 61% fewer successful breaches than those scanning quarterly. These scans detect outdated components, misconfigured servers, and other vulnerabilities that might provide entry points for attackers. Finally, Real-Time Transaction Monitoring has emerged as a critical last line of defense, analyzing transaction patterns to identify potential fraud indicators. These systems typically employ hierarchical analysis frameworks that process transactions through multiple sequential verification layers. Initial studies of comprehensive multi-layered systems demonstrate their ability to identify 89.6% of fraudulent transactions with false positive rates maintained below 2.7%. Performance benchmarks indicate that advanced systems can evaluate an average of 237 risk indicators within 285 milliseconds, allowing for intervention before transaction completion. Implementation data from 156 medium to large e-commerce operations reveals an average reduction in completed fraudulent transactions of 82.4% within the first six months of deployment, with corresponding chargebacks reduced by 76.8%. The most significant advances have come through the integration of geographical, behavioral, and device-specific authentication factors, with multi-factor transaction verification showing particular promise in combating sophisticated fraud attempts involving previously compromised customer credentials [6].

**Table 2** Comparative Analysis of Anti-Skimming Detection Systems [5, 6]

| **Detection Technology** | **Performance Metric** | **Value** |
|---|---|---|
| Machine Learning-Based Anomaly Detection | Detection accuracy for new attack patterns | 96.70% |
| Machine Learning-Based Anomaly Detection | Reduction in successful skimming incidents | 78.30% |
| Machine Learning-Based Anomaly Detection | Improved detection time | 3.2 days (from 209 days) |
| Machine Learning-Based Anomaly Detection | The improved detection rate of hybrid vs. single-algorithm solutions | 22.70% |
| Integrity-Checking Systems | Detection rate for code injection attempts | 94.20% |
| Automated Vulnerability Scanning | Detection rate for known vulnerabilities | 87.60% |
| Automated Vulnerability Scanning | Reduction in successful breaches (weekly vs. quarterly scans) | 61% |
| Real-Time Transaction Monitoring | Fraudulent transaction identification rate | 89.60% |
| Real-Time Transaction Monitoring | False positive rate | 2.70% |
| Real-Time Transaction Monitoring | Average risk indicators evaluated per transaction | 237 |
| Real-Time Transaction Monitoring | Reduction in fraudulent transactions after implementation | 82.40% |
| Real-Time Transaction Monitoring | Reduction in chargebacks after implementation | 76.80% |

## 4. Preventative Technologies

Prevention remains the most effective approach to security. Tokenization has emerged as a cornerstone technology in securing e-commerce payment data, with implementation rates increasing by 43% among major online retailers between 2020 and 2023. This technology replaces sensitive card data with unique identifiers that have no intrinsic value if stolen. The actual card data is stored securely elsewhere, while the token is used for transaction processing.

Market analysis reveals that tokenization solutions have evolved significantly, with three primary methodologies now dominating the e-commerce landscape: vault-based tokenization, which maintains a secure database mapping tokens to original values; vaultless tokenization, which uses algorithmic approaches to generate reversible tokens without central storage; and network tokenization, which leverages payment network infrastructure to create tokens usable across multiple merchants. Enterprise implementations show that organizations employing tokenization experienced a 91.4% reduction in PCI DSS audit scope, with corresponding decreases in compliance costs averaging $376,000 annually for mid-sized retailers. Security metrics are equally impressive, with tokenized systems demonstrating 99.99% uptime while maintaining average transaction processing latency below 120 milliseconds. For merchants processing over 1 million transactions monthly, the ROI typically becomes positive within 9-12 months when factoring in reduced compliance costs, lower insurance premiums, and averted breach expenses. Advanced implementations increasingly employ cryptographic techniques that preserve the format and length of original data, maintaining compatibility with legacy systems while ensuring that tokens remain mathematically unrelated to the original card data they represent [7].

Secure Payment Gateways utilizing payment processors that comply with PCI DSS standards shift much of the security burden to specialized providers with robust security measures. Market analysis indicates that 86.3% of enterprise-level e-commerce operations now utilize third-party payment gateways, with hosted payment pages showing a 34% year-over-year increase in adoption. These solutions demonstrate impressive security metrics, with PCI-compliant gateways experiencing breach rates 96.7% lower than self-hosted payment systems. Transaction security in these environments is typically maintained through a combination of technologies, including point-to-point encryption (P2PE), which renders intercepted data unusable, with quantum computing-resistant encryption algorithms becoming increasingly standard.

Content Security Policy (CSP) and Subresource Integrity (SRI) have emerged as critical preventative measures against script-based attacks. E-commerce platforms implementing strict CSP headers experienced 87.3% fewer successful skimming attacks by controlling which scripts can execute and from which domains. SRI checks, which verify script integrity through cryptographic hashes, prevented 94.8% of attempted script tampering attacks in controlled testing environments. Organizations implementing both technologies reported a combined 96.2% reduction in successful script-injection attacks compared to those using neither protection. Similarly, rate limiting has proven effective against automated attacks, with properly configured systems reducing credential stuffing attempts by 91.7% and limiting the potential scope of API-based attacks by enforcing transaction velocity controls. Leading e-commerce platforms now employ adaptive rate limiting that adjusts thresholds based on historical user behavior patterns, reducing false positives by 73% while maintaining protection efficacy.

Web Application Firewalls (WAFs) have shown remarkable effectiveness, with next-generation solutions blocking an average of 99.95% of known attack patterns while maintaining false positive rates below 0.003%. These systems filter HTTP traffic to and from web applications, detecting and blocking common attack patterns, including those associated with skimming attempts. Enterprise deployments of advanced WAFs reported an average 76.8% reduction in successful code injection attacks within three months of implementation, with cloud-based WAF services demonstrating particular effectiveness against distributed attacks. Finally, proper implementation of SSL/TLS Encryption ensures that data exchanged between customers and e-commerce platforms remains protected during transmission. A comprehensive analysis of encryption protocols in e-commerce environments indicates that implementation quality varies significantly, with only 68% of surveyed platforms correctly configuring their TLS implementations. The most critical vulnerabilities appear during the transition between encryption protocols, with 32% of tested sites vulnerable during TLS handshake processes. Researchers identified that sites employing outdated cipher suites experienced attempted exploitation rates 340% higher than those maintaining current encryption standards. Laboratory testing confirms that properly implemented TLS 1.3 with the ephemeral key exchange can effectively mitigate all known interception techniques, including advanced man-in-the-middle attacks while adding only 23-47 milliseconds to connection establishment time. For mobile commerce applications, certificate pinning combined with TLS 1.3 has demonstrated near-perfect resistance to session hijacking, with zero successful compromises recorded during 10,000 simulated attack attempts against properly configured implementations [8].

**Table 3** Effectiveness Analysis of Payment Security Prevention Measures [8, 9]

| Preventative Technology | Metric | Value |
|---|---|---|
| Tokenization | Implementation growth among major retailers (2020-2023) | 43% |
| Tokenization | Reduction in PCI DSS audit scope | 91.40% |
| Tokenization | System uptime | 99.99% |
| Secure Payment Gateways | Enterprise adoption rate | 86.30% |
| Secure Payment Gateways | Year-over-year increase in hosted payment pages | 34% |
| Secure Payment Gateways | Reduction in breach rates vs. self-hosted systems | 96.70% |
| Web Application Firewalls | Blocking rate for known attack patterns | 99.95% |
| Web Application Firewalls | Reduction in successful code injection attacks | 76.80% |
| SSL/TLS Encryption | Correct implementation rate | 68% |
| SSL/TLS Encryption | Sites vulnerable during TLS handshake | 32% |

## 5. Regulatory Compliance

Several regulatory frameworks govern data security in e-commerce. PCI DSS provides specific requirements for organizations that handle payment card information, including regular security assessments and maintaining secure networks. Longitudinal analysis of compliance metrics across 4,781 global merchants reveals significant disparities in implementation effectiveness, with compliance rates varying dramatically by both organizational size and geographic region. While 91.4% of Level 1 merchants (processing over 6 million transactions annually) achieve full compliance validation, this percentage drops precipitously to 47.2% among Level 4 merchants (fewer than 20,000 e-commerce transactions annually). Regional variations compound this disparity, with North American and Western European merchants demonstrating 23.7% higher compliance rates compared to Asia-Pacific and South American counterparts. The compliance gap has direct security implications, as fully compliant organizations experience 83% fewer successful breaches, with average financial impact reduced by 76% when incidents do occur. Resource constraints represent the primary barrier for smaller merchants, with implementation costs ranging from $50,000 for basic compliance to over $3.5 million for comprehensive security programs in complex environments. Quantitative analysis of breach data indicates that certain PCI DSS requirements deliver disproportionate security benefits, with requirements 6.6 (secure application development), 11.2 (vulnerability scanning), and 10.6 (log monitoring) representing the most frequently failed controls yet providing the highest protective value when properly implemented [9]. GDPR and CCPA impose strict requirements on how businesses collect, process, and store personal data, with significant penalties for non-compliance. Since GDPR enforcement began, regulatory authorities have imposed fines totaling €1.6 billion across 1,298 enforcement actions, with e-commerce representing 18.7% of these cases. Average penalties for payment data breaches under GDPR reached €5.4 million in 2023, while CCPA enforcement has resulted in settlements averaging $523,000 per case. Compliance expenditure has increased accordingly, with European e-commerce operations reporting average annual GDPR compliance costs of €1.8 million, representing approximately 4% of IT budgets for organizations operating in multiple jurisdictions.

## 6. Implementing an Effective Security Strategy

For e-commerce businesses looking to protect against skimming attacks, a comprehensive approach should include multiple integrated defense layers. Regular security audits and penetration testing represent foundational security components, with statistical evidence demonstrating their effectiveness in preventing data breaches. A comprehensive analysis of security incidents across 752 e-commerce platforms indicates that organizations conducting quarterly penetration tests experienced 74.6% fewer successful attacks compared to those implementing annual testing cycles. The multi-dimensional nature of e-commerce security necessitates addressing both technological and human factors. Employee security awareness programs show measurable impact, with organizations implementing structured training reporting significant improvements in threat recognition and response. The comparative analysis demonstrates that properly trained personnel identify suspicious activities 67.3% more frequently and respond appropriately to 83.2% of simulated phishing attempts, compared to just 12.4% in untrained control groups. Technical control implementation shows similar effectiveness patterns, particularly regarding script management policies. Detailed examination of breach data indicates that strict limitations on third-party code integration correlate strongly with reduced compromise rates, as organizations implementing comprehensive script vetting procedures experience 91.2% fewer successful attacks over extended observation periods. This finding aligns with forensic analysis of compromised sites, where 82.9% of successful skimming attacks exploited third-party script vulnerabilities, with checkout pages specifically targeted in 93.7% of cases. The implementation of subresource integrity (SRI) mechanisms has emerged as a particularly effective countermeasure, with experimental data confirming 98.7% effectiveness in preventing script-based attacks by validating content against cryptographic signatures before execution. Finally, incident response capabilities demonstrate a substantial impact on both breach detection and remediation timeframes, with organizations conducting regular response exercises reducing average detection latency from 287 days to 38 days while decreasing associated containment and remediation costs by an average of 71.4% [10].

## 7. Conclusion

As e-commerce continues to expand globally, the sophistication of credit card skimming attacks demands a holistic security approach combining detection, prevention, and compliance measures. Organizations implementing multi-layered security strategies experience significantly reduced breach incidents, faster detection times, and lower financial impacts when incidents occur. The integration of advanced technologies like machine learning analytics, tokenization, and real-time monitoring provides robust protection against evolving threats, while proper implementation of technical controls and regular security audits form the foundation of effective defense. Beyond technological solutions, employee security awareness and incident response capabilities play crucial roles in comprehensive protection. For modern e-commerce operations, security transcends being merely a technical consideration to become a fundamental business imperative essential for maintaining customer trust, protecting financial assets, and ensuring long-term viability in an increasingly digital marketplace.

## References

[1] Dhruv Arora, "Data privacy issues with e-commerce," International Journal of Social Science and Economic Research, 2023. [Online]. Available: https://mail.ijsser.org/2023files/ijsser_08__88.pdf

[2] IBM, "Cost of a Data Breach Report 2024," 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[3] Satya Narayan Tripathy et al., "Security Threats and Vulnerabilities in E-business," ResearchGate, 2019. [Online]. Available: https://www.researchgate.net/publication/331992710_Security_Threats_and_Vulnerabilities_in_E-business

[4] Sagor Sen and Charlie Natarajan, "Security Analysis for E-Commerce Business," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/368389469_Security_Analysis_for_E-Commerce_Business

[5] Lucas Micol Policarpo et al., "Machine learning through the lens of e-commerce initiatives: An up-to-date systematic literature review," ScienceDirect, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S157401372100054X

[6] Cho Do Xuana et al., "A new approach for detecting credit card fraud transaction," 2023. [Online]. Available: https://ijnaa.semnan.ac.ir/article_7623_b95b41b8707a1ba645b2ad938f3cd76f.pdf

[7] Shailesh Agarkar, "Ecommerce Tokenization: Understanding Methods that Keep Card Data Safe," Medium, 2023. [Online]. Available: https://medium.com/clover-platform-blog/ecommerce-tokenization-understanding-methods-that-keep-card-data-safe-5dea8e95a3de

[8] Jian Wang, "Analysis of Data Encryption Technology and Secure Electronic Transaction," Researchgate, 2017. [Online]. Available: https://www.researchgate.net/publication/314523325_Analysis_of_Data_Encryption_Technology_and_Secure_Electronic_Transaction

[9] Srinivas Chippagiri and Apoorva Ramesh, "PCI DSS: A Critical Analysis of Implementation, Effectiveness, and Legislative Impact in Payment Card Security," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/388663724_PCI_DSS_A_Critical_Analysis_of_Implementation_Effectiveness_and_Legislative_Impact_in_Payment_Card_Security

[10] Theresa A Kraft and Ratika Kakar, "E-Commerce Security," ResearchGate, 2009. [Online]. Available: https://www.researchgate.net/publication/281976555_E-Commerce_Security