Cyber Security in Digital Commerce: Data security in Online Transactions

N. Maheswari

Head & Assistant Professor, Department of Commerce with Computer Applications, St. Joseph's College (Autonomous), Tiruchirappalli

Corresponding Author Email: maheswari_cc2@mail.sjctni.edu

Abstract

The rapid growth of digital commerce has fundamentally transformed business operations, consumer engagement, and global trade. Cybersecurity in digital commerce is indispensable for sustaining trust, safeguarding consumer interests, and ensuring uninterrupted economic activity. As digital ecosystems expand, robust security strategies, compliance with legal frameworks, and stakeholder collaboration will determine the resilience of digital commerce against cyber threats. With the proliferation of online transactions, ensuring the confidentiality, integrity, and availability of data has become a critical priority. This paper examines the major cybersecurity challenges in digital commerce, explores threats to data protection in online transactions, analyzes current defense mechanisms, and proposes future directions for securing digital financial ecosystems.

Keywords: Cybersecurity, Digital Commerce, Data Protection, E-commerce Security, Cyber Threats, Online Transactions

1. Introduction

Digital commerce, encompassing e-commerce, mobile payments, and peer-to-peer financial exchanges, has emerged as a cornerstone of the 21st-century economy. The reliance on digital payment platforms has introduced significant cyber risks, as sensitive data including personal identifiers, authentication credentials, and financial details are transferred across potentially vulnerable networks. Cyberattacks targeting these transactions can undermine consumer trust, cause financial loss, and disrupt economic stability. Thus, robust cybersecurity mechanisms—including end-to-end controls, continuous monitoring, and robust governance—are imperative for the sustainability of digital commerce. Beyond the perimeter, the rise of mobile and cloud-native commerce increases attack surface, requiring formal methods to validate transactional correctness, advanced analytics for fraud, and adaptive encryption for confidentiality at scale.

2. Methodology

This study employs a qualitative, descriptive–analytical methodology that integrates a systematic literature review (SLR), framework comparison, and conceptual synthesis to examine cybersecurity in digital commerce with emphasis on data protection in online transactions. The methodology aligns the domains of cybersecurity, digital commerce, data protection, e-commerce security, cyber threats, and online transactions through triangulated evidence from academic research, standards, and policy guidance.

Secondary data were collected from: Academic literature: peer-reviewed journals and conference papers, Industry standards and frameworks, Policy and regulatory research: economic and policy analysis for cybersecurity in e-commerce supply chains.

3. Literature Review

Payment data protection is institutionalized through the PCI Security Standards Council and PCI DSS, which codify control requirements, scanning procedures, and third-party assessment through Qualified Security Assessors (QSAs), anchoring merchant security practices in standardized governance and compliance regimes [1].

Consumer trust remains sensitive to privacy assurances; privacy seals and related cues influence behavior but are often misunderstood by consumers, highlighting the need for usable transparency and authenticatable assurances rather than symbolic compliance alone [2].

Mobile e-commerce introduces device-level and wireless vulnerabilities, expanding threat vectors to include insecure application code, session hijacking, and location-linked risks that demand tailored mitigations for constrained devices and variable networks [3].

Authentication in e-commerce requires multidimensional approaches that evolve over the lifecycle of relationships, going beyond identification to authenticate parties, products, and processes in dynamic, risk-based contexts [4].

Formal verification using model checking can increase assurance in e-commerce transaction protocols, reducing logic and state-machine errors that lead to exploitable flaws [5]. Cloud-scale anomaly detection using robust, online learning-driven feature extraction can reduce noise sensitivity and adapt to evolving patterns, improving time-to-detection for operational threats [6].

Behavior-based fraud detection that models fine-grained co-occurrences across transactional attributes via knowledge graphs and heterogeneous network embeddings improves detection accuracy across population-, individual-, and agent-based models [7].

Searchable encryption that is secure against adaptive adversaries enables privacy-preserving retrieval in cloud storage, a cornerstone capability for secure, compliant data processing in commerce analytics and customer service contexts [8].

Government penalties in e-commerce supply chains can, under specific welfare considerations, improve social outcomes; optimal penalty intensity interacts with the cost-benefit profile of security-enhancing technologies such as blockchain, shaping incentives in complex ecosystems [9].

This body of work indicates that technical, organizational, behavioral, and policy dimensions must be integrated to protect online transactions effectively [1] [2] [3] [4] [5] [6] [7] [8] [9].

4. Threats to Data Security in Online Transactions

4.1 Phishing and Social Engineering

Attackers exploit human factors to obtain login credentials and payment details, bypassing technical safeguards. Misinterpretation of trust cues (for example, privacy seals or padlocks) and the lack of lifecycle authentication controls exacerbate susceptibility, indicating the need for dynamic, context-aware authentication and consumer education initiatives [2][4].

4.2 Malware and Ransomware

E-commerce platforms and their supporting infrastructure are prime targets for malware and ransomware campaigns aimed at credential theft, data exfiltration, and availability disruption. Mobile environments contribute additional risk vectors such as malicious apps and insecure APIs, intensifying exposure in Omni channel commerce [3].

4.3 Man-in-the-Middle (MITM) and Session Hijacking

Unsecured or misconfigured connections enable adversaries to intercept communications between customers, payment gateways, and merchants, compromising transaction confidentiality and integrity. Mobile and public Wi-Fi contexts are particularly vulnerable, demanding strict transport security and channel binding [3].

4.4 SQL Injection and Web Exploits

Vulnerable web applications expose transaction records and personal data to unauthorized access. Formal verification and model checking of protocol logic can reduce classes of exploitable errors, complementing secure coding, dependency hygiene, and regular compliance scanning [1][5].

4.5 Insider Threats and Third-Party Risk

Employees or contractors with privileged access may misuse or leak financial data. PCI DSS emphasizes segmentation, least privilege, monitoring, and third-party oversight to reduce insider risk and supply chain exposure [1]. Cloud log analytics and online anomaly detection help identify misuse patterns at scale [6].

5. Cyber Security Solutions for Digital Commerce

5.1 Encryption and Secure Protocols

Enforce TLS 1.2+ with strong cipher suites, HSTS, certificate pinning (for mobile), and forward secrecy to protect data-in-transit, especially across variable mobile networks [3].

Apply data-at-rest encryption and granular tokenization for cardholder data, aligning with PCI DSS scoping and key management requirements [1].

Use searchable encryption for privacy-preserving retrieval over encrypted indices, adopting schemes secure against adaptive adversaries to resist more capable servers in cloud environments [8].

5.2 Multi-Factor and Lifecycle Authentication

Implement MFA using possession (hardware tokens, device-bound keys), inherence (biometrics), and context (risk signals), with adaptive step-up challenges for high-risk events. Employ a lifecycle authentication framework that authenticates parties, products, and processes at onboarding, transaction time, and post-transaction dispute resolution, aligning with risk-based models [4].

5.3 Application and Protocol Assurance

Integrate secure SDLC with threat modeling, SAST/DAST, SBOM-based dependency management, and runtime protections.

Apply model checking to verify transactional protocols (ordering, non-repudiation, fairness), reducing logic flaws that evade traditional testing [5].

Conduct PCI DSS-aligned vulnerability scans and penetration testing; maintain compensating controls and continuous compliance monitoring [1].

5.4 Fraud Detection via Artificial Intelligence

Deploy behavior-based models using fine-grained co-occurrence of attributes (device, merchant category, geolocation, time), enriched by knowledge graphs and heterogeneous network embedding to detect sophisticated fraud patterns [7].

Operate robust online anomaly detection on logs to adapt to distribution drift and remove noise, improving timeliness and accuracy of incident response in cloud-native commerce platforms [6].

5.5 Mobile and Edge Security

Harden mobile applications with secure storage, certificate pinning, anti-tamper, and secure session management; mitigate risks of wireless interception and OS-level compromise in m-commerce [3].

Implement device posture checks and channel binding to reduce session hijacking risk on mobile networks [3].

5.6 Regulatory and Compliance Frameworks

Align with PCI DSS for cardholder data protection: network segmentation, access controls, logging, regular scanning, and QSA assessments to validate control effectiveness [1]. Enhance consumer trust through genuine, verifiable privacy practices rather than symbolic seals; design transparent disclosures that users can interpret correctly to reduce trust miscalibration [2].

Consider policy instruments and penalties in e-commerce supply chains; when governments value consumer surplus sufficiently, penalty schemes can increase social welfare, with optimal fine levels influenced by the cost-benefit of security-enhancing technologies [9].

5.7 Privacy-Preserving Data Analytics

Combine tokenization and encryption with searchable encryption to enable support operations and analytics without exposing plaintext sensitive data [8].

Apply data minimization and purpose limitation in line with privacy-by-design principles, supported by lifecycle authentication and verifiable consent mechanisms [4][8].

6. Case Studies and Applied Scenarios

PCI DSS Implementation in a Marketplace Platform: A multi-tenant marketplace applies network segmentation to score cardholder environments, tokenizes PAN data to reduce exposure, and uses continuous vulnerability scanning and QSA assessments, achieving measurable reduction in incident frequency and blast radius [1].

Behavior-Based Fraud Control in Online Banking: Using knowledge graphs to encode co-occurrence of transaction attributes and heterogeneous embedding, a bank boosts detection metrics across population and individual models, reducing fraud loss and false positives in production [7].

Cloud Log Anomaly Detection: A commerce SaaS adopts robust, online evolving anomaly detection, enabling near-real-time detection of configuration drift and credential misuse with improved accuracy under noisy log streams [6].

Formal Verification of Checkout Protocols: Model checking ensures atomicity and fairness of payment-fulfillment flows, preventing race-condition charge disputes and state desynchronization under failure scenarios [5].

7. Conclusion

The security of online transactions remains a paramount concern for digital commerce. While encryption, authentication, AI-driven surveillance, and compliance frameworks have advanced protections, evolving adversarial tactics necessitate continued innovation. Strengthening governance with PCI DSS and lifecycle authentication, extending protections to mobile and cloud contexts, applying formal verification to transaction protocols, and advancing behavior-based fraud analytics are crucial steps. Policy mechanisms, when designed with attention to welfare and technology cost-benefit dynamics, can complement private investment in security across supply chains. Future resilience will depend on integrating advanced technologies, ensuring regulatory and incentive alignment, and improving consumer understanding of privacy protections. Trust in digital commerce is inextricably linked to the effective safeguarding of data, making cybersecurity not just a technical obligation but a foundation for sustainable economic growth [1][2][3][4][5][6][7][8][9].

References

1) LIU, Jing, et al. A Survey of Payment Card Industry Data Security Standard. Ieee Communications Surveys and Tutorials, 2010, 12: 287-303.

2) MOORES, Trevor T. Do consumers understand the role of privacy seals in e-commerce?. Commun Acm, 2005, 48: 86-91.

3) GHOSH, Anup K.; SWAMINATHA, Tara M. Software security and privacy risks in mobile e-commerce. Commun Acm, 2001, 44: 51-57.

4) BASU, A.; MUYLLE, Steve. Authentication in e-commerce. Commun Acm, 2003, 46: 159-166.

5) ANDERSON, B., et al. The application of model checking for securing e-commerce transactions. Communications of the Acm, 2006, 49: 97-101.

6) HA N, Shangbin, et al. Log-Based Anomaly Detection With Robust Feature Extraction and Online Learning. Ieee Transactions of on Information Forensics and Security, 2021, 16: 2300-2311.

7) WANG, Cheng; ZHU, Hangyu. Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services. Ieee Transactions of on Dependable and Secure Computing, 2022, 19: 301-315.

8) LI, Mingchu, et al. Encrypted Searching with Adaptive Symmetric Searchable Encryption Security in Cloud Storage. Information Sciences, 2015.

9) LUO, Suyuan; CHOI, T. E-commerce supply chains with considerations of cyber-security: Should governments play a role?. Production and Operations Management, 2022, 31: 2107-2126.