Edge Computing Security Approaches and Their Influence on Latency Reduction in E-Commerce Payment Networks

María Fernanda Álvarez
Universidad Nacional de Oriente, Department of Computer Science, Avenida del Lago, Zona Central, Puerto La Cruz, Venezuela.

Abstract

Edge computing has emerged as a transformative strategy for reducing latency and enhancing user experiences in e-commerce payment networks. By processing transactions and related data closer to the point of origin, retailers and financial institutions can deliver faster responses that minimize checkout abandonment and elevate consumer satisfaction. However, decentralizing infrastructure from core data centers to distributed edge nodes presents new security challenges, especially when handling sensitive information such as payment card data and personal user credentials. This paper examines how security approaches for edge computing can influence latency reduction strategies in modern e-commerce payment systems. Emphasis is placed on robust encryption, secure enclaves, zero-trust policy enforcement, and real-time anomaly detection techniques, all of which must integrate seamlessly with low-latency processing frameworks. The following sections explore architectural considerations, cryptographic protocols, secure data routing, and governance models that unify edge nodes with centralized oversight. Case analyses show that coordinated policy definitions, hardware-assisted safeguards, and machine learning–driven threat monitoring protect cardholder details without compromising the millisecond-level performance gains that edge computing promises. Concluding reflections highlight that balancing security rigor with minimal overhead is paramount: approaches that embed authentication, encryption, and intrusion detection within the edge environment can fortify consumer trust and regulatory compliance while preserving, or even enhancing, the swift payment processing times essential for e-commerce success.

1. Introduction

E-commerce platforms continually seek new methods to decrease latency in payment transactions and enhance reliability in the face of increasing user demands. Traditional cloud-centric models route transactions through centralized data centers, sometimes located far from the consumer’s or merchant’s geographical region. Although scaling resources in the cloud helps manage traffic surges, round-trip delays can become pronounced during peak shopping seasons, leading to potential user dissatisfaction and increased cart abandonment. Edge computing, which moves data processing tasks closer to endpoints, promises to solve these latency problems by localizing key functions—security checks, transaction validation, analytics—within edge nodes situated near merchants or at internet exchange points [1], [2].

1.1 Drivers for Low-Latency E-Commerce Transactions

Online shoppers often demand near-instant checkout experiences. Even minor response lags during card authorization can increase the likelihood of customers abandoning their carts. For retailers, each millisecond saved translates to improved sales conversions and customer loyalty. Meanwhile, payment service providers (PSPs) and acquiring banks aim to secure and clear transactions in near real time to reduce risk windows and minimize the possibility of fraud. Collectively, these demands push the e-commerce sector toward rearchitecting payment workflows to be more distributed, leading them to explore edge computing paradigms that handle resource-intensive tasks—such as encryption or risk scoring—at the network periphery.

1.2 Risks and Complexity Arising from the Edge

Migrating critical payment processes to edge nodes introduces new complexities in security. Traditional data center models centralize oversight, facilitating uniform policy enforcement and consolidated logging. Edge environments, by contrast, involve multiple nodes across diverse geographies, managed either by the retailer or by local service providers. Each node must handle secure key management, real-time encryption, user authentication, and logging, often with minimal local staff. Malicious actors who compromise an edge node may potentially disrupt payment flows or steal cardholder data. Edge nodes also risk hardware tampering or side-channel attacks if located in physically accessible environments with limited onsite security.

1.3 Outline and Purpose

This paper explores how security approaches for edge computing can support or potentially hinder latency-reduction objectives in e-commerce payment networks. Section 2 addresses architectural considerations, emphasizing how distributed computing frameworks reshape network design and data flows. Section 3 presents key edge security mechanisms, highlighting encryption, tokenization, zero-trust enforcement, and anomaly detection, along with how these measures must be adapted for minimal overhead. Section 4 dives into governance and compliance strategies, focusing on how Payment Card Industry Data Security Standard (PCI DSS) and emerging privacy regulations evolve within an edge paradigm. Finally, Section 5 examines prospective developments and strategic recommendations, advocating for a balanced synergy between robust security and performance optimization.

2. Architectural Considerations for Edge-Enabled Payment Systems

Adopting edge computing for e-commerce payments involves restructuring how transactions flow, where data is processed, and how systems interconnect. An effective edge architecture must ensure that local nodes can handle the bulk of transaction validation, cryptographic operations, and risk checks without excessive communication to central servers.

2.1 Hybrid Cloud-Edge Topologies

E-commerce providers frequently mix on-premises infrastructure, public cloud services, and now, edge nodes. In a hybrid edge configuration, certain resources—like user authentication or loyalty program data—remain in the cloud for global accessibility, while latency-sensitive tasks—such as transaction authorization—run at edge sites. These edge nodes may be installed at internet exchange points (IXPs), local data centers near heavily populated regions, or even merchant premises. Payment gateways harness containerized microservices that spin up to handle demand spikes locally, reducing the path length for transaction approval [3]. Meanwhile, central cloud-based back-ends handle advanced analytics, machine learning model training, and data warehousing.

2.2 Payment Workflow Distribution

Traditional payment flows involve an e-commerce frontend communicating with a payment gateway hosted in the provider's central infrastructure. With edge computing, these flows are partly offloaded to localized gateways deployed near the merchant or end user. Instead of relaying all data to a distant data center, the edge node completes critical steps like:

1. **Initial Card Validation**: Checking card format, expiration, or the Luhn algorithm for basic correctness.

2. **Multi-Factor Authentication**: If required by 3D Secure or similar standards, the edge node can challenge the user with a local verification prompt.

3. **Tokenization**: Generating or substituting sensitive card details with tokens before forwarding minimal necessary data to the central system.

If the node deems the transaction low-risk—based on local risk scoring or past user behavior logs—it can finalize the authorization quickly, only updating the main server asynchronously. This real-time local decision-making cuts down on round-trip times, especially for repeating customers or widely used payment methods [4].

2.3 Latency Optimization and Data Routing

Edge-based deployments rely on local data routing between the user's device and the nearest node. By limiting hops to regional networks, the effective round-trip time (RTT) can be cut drastically. Payment providers may partner with content delivery networks (CDNs) that originally specialized in accelerating static content but now incorporate edge computing capabilities. The challenge is ensuring that encryption overhead or re-routing for fraud checks does not eclipse the latency savings gained by localizing transaction flow [5].

DNS-based load balancing steers user sessions to the nearest edge gateway based on geolocation. Some providers embed intelligence in the merchant's application logic, detecting user IP addresses or device attributes, then offering the nearest node for payment processing. Ensuring consistent session handling across multiple edge nodes calls for stateful approaches or stateless designs that store ephemeral session data in distributed caches.

2.4 Challenges in Orchestration and Deployment

Provisioning edge nodes at scale demands automation to handle wide variations in hardware, connectivity quality, and network policies. Container orchestrators such as Kubernetes or Docker Swarm can unify deployment across data center and edge environments, but these orchestrators must be fine-tuned to operate on resource-constrained edge hardware. Observability systems that gather logs and metrics from hundreds of globally distributed nodes must remain lightweight to avoid saturating WAN links. Managing version drift and ensuring timely patches or security updates across edge clusters is essential; unpatched edge nodes can become easy gateways for attackers [6].

2.5 Balancing Edge Resources and Centralized Services

A purely decentralized approach would push nearly all tasks to the edge, but hardware constraints, especially around memory and CPU, limit advanced AI-based fraud detection or large-scale data retention at local sites [7]. Payment networks typically adopt a layered approach: local real-time checks and encryption for minimal overhead, with more complex analysis—like historical pattern matching or anomaly detection—running in centralized analytics engines. Periodic data synchronization or streaming aggregates transaction logs from all edges, supporting machine learning pipelines that update risk models. Over time, these updated models propagate back to edge nodes, refining real-time decision-making.

Architectural shifts toward edge-enabled payment flows can radically reduce checkout times. However, each edge node becomes a security focal point, prompting the deployment of robust cryptographic and policy measures that preserve data confidentiality and system integrity. The ensuing section delves into these security components, illustrating how they intersect with the latency benefits sought in distributed payment networks.

3. Security Mechanisms for Edge-Based Payment Processing

Edge security strategies must combine standard e-commerce protection requirements—encryption, tokenization, intrusion detection—with specialized measures tailored to decentralized topologies. Minimizing overhead remains vital; excessive encryption layers or resource-intensive scanning can erode the very latency gains that edge computing pursues.

3.1 Lightweight Encryption and Tokenization at the Edge

Payment networks have long used TLS for data in transit, ensuring that card numbers and personal user details remain unreadable if intercepted. Edge nodes also adopt TLS or QUIC protocols, leveraging hardware accelerators for cryptographic operations to keep latencies low. Beyond transport-level encryption, advanced tokenization replaces card numbers and other identifiers with randomly generated tokens. By performing tokenization at or near the user's location, the system limits exposure of raw card data to a minimal perimeter. If the tokenization keys remain in secure hardware modules, even a compromised edge node yields minimal sensitive data.

Performing tokenization at the edge has a twofold benefit:

1. **Latency Reduction**: Freed from sending unencrypted data to a remote location for token generation.
2. **Containment**: Full card details never traverse wide-area networks unprotected, curbing data exfiltration risk.

3.2 Secure Enclaves and Trusted Execution Environments

Hardware-based TEEs, such as Intel SGX or ARM TrustZone, can isolate critical payment code within secure enclaves on the edge device. These enclaves store cryptographic keys and perform sensitive computations without exposing them to the broader system. Payment applets running in enclaves verify user credentials or sign transactions with keys that remain inaccessible to even root-level processes. This approach considerably narrows the potential of memory inspection or kernel-level malware capturing data. Paired with ephemeral containers, TEEs ensure ephemeral usage of secrets, bolstering PCI DSS compliance and diminishing the impact of local physical attacks on edge devices in publicly accessible areas.

3.3 Anomaly Detection and Machine Learning at the Edge

One of the main draws of edge computing is localized, real-time analytics. Minimal-latency fraud detection demands on-site machine learning inference. Models pre-trained in the cloud can be pushed to edge nodes, enabling them to classify transaction risk within milliseconds. These models examine user location, device attributes, historical purchase patterns, or even biometric signals. Edge-based anomaly detectors benefit from immediate local data, reducing round-trip times for risk decisions. If suspicious patterns exceed a certain threshold, the node can escalate the transaction to the central system for deeper scrutiny or enforce additional authentication steps. This layered approach balances security with speed, as routine low-risk transactions finalize instantly while truly risky attempts face a robust screening pipeline.

3.4 Zero-Trust Policy Enforcement

Zero-trust frameworks require continuous authentication and authorization checks, even for internal communications. Within an edge environment, every service—whether for user authentication, payment processing, or analytics—receives ephemeral identity tokens via a centralized identity provider. Micro-segmentation ensures that only authorized components can connect, employing mutual TLS or short-lived certificates for service-to-service encryption. Administrators define context-based rules: for instance, a payment container must only reach a card vault microservice if it presents the correct identity claim and is running on a verified node. The overhead of these microservices' handshakes can be minimized with hardware accelerators and carefully optimized certificate lifecycles, preserving edge node throughput.

3.5 Intrusion Detection and Honeypots

Distributed intrusion detection systems (IDS) monitor logs, network traffic, and system events at each edge node for malicious signatures or suspicious anomalies. Rolling up these insights into a cloud-based SIEM yields cross-regional threat intelligence. If an attacker tries scanning multiple nodes for a known vulnerability, aggregated alerts can highlight broad campaign patterns. Some e-commerce providers go further by deploying honeypot microservices that mimic real payment endpoints but contain decoy data. Attackers engaging with these honeypots reveal tactics, giving defenders early warnings. Honeypot overhead is minimal if configured carefully, so it does not degrade legitimate user pathways.

3.6 Edge-Driven Encryption Key Management

A crucial aspect for latency reduction is local encryption key availability. If edge nodes must repeatedly fetch or verify keys from a central key management service, each transaction can suffer from WAN latencies. Solutions include local hardware security modules (HSMs) or secure enclaves that store short-lived session keys. Master keys or root certificates remain in a central vault, but derived keys periodically propagate to edge nodes using secure channels. This approach accelerates cryptographic operations for thousands of concurrent sessions. Still, carefully designed revocation or rotation policies remain necessary, ensuring that compromised or outdated keys cannot be misused at the edge.

3.7 Optimizing Overhead vs. Security Gains

Balancing robust security with minimal overhead is fundamental. Overly granular encryption or multi-layer scanning can offset the latency benefits of edge computing. E-commerce providers typically adopt risk-based approaches: high-value or suspicious transactions might undergo more comprehensive checks, while lower-risk ones receive a lighter security path. Load balancing at the edge can direct potentially fraudulent transactions to specialized scanning nodes with more compute resources. Meanwhile, routine transactions pass through streamlined encryption and tokenization microservices. This adaptiveness ensures that security measures stay proportional to risk, preserving end-user speed.

In sum, edge security capabilities revolve around cryptographic, zero-trust, and anomaly detection paradigms adapted for decentralized nodes. Implementing these in synergy with performance-focused design allows e-commerce operators to deliver near real-time payment authorizations without relinquishing data integrity or confidentiality. The subsequent section discusses how governance and compliance frameworks must evolve to accommodate these new distributed security models while aligning with PCI DSS and other regulations.

4. Governance, Compliance, and Regulatory Implications

Edge computing redefines data responsibilities, with multiple nodes spanning jurisdictions and hosted by different providers. Achieving compliance requires a coherent governance structure that addresses how data ownership, risk management, and privacy regulations apply in an environment featuring ephemeral containers and local caches of payment data.

4.1 PCI DSS in Distributed Payment Flows

PCI DSS mandates rigorous segmentation of the cardholder data environment (CDE). Extending the CDE to the edge means that every edge node processing or storing card data falls within scope. Retailers must demonstrate robust encryption, strict access controls, and vulnerability scanning for each node. Logging of authorized or denied attempts to handle cardholder data is essential, as is evidence of secure key management. Assessors may require proof that ephemeral containers do not store data beyond their lifetime or that memory is properly cleared upon termination. Frequent ephemeral operations can complicate change management documentation, a PCI requirement that tracks modifications in the CDE. Automated compliance scanning and configuration management thus become critical for adopting edge nodes at scale.

4.2 Data Privacy and Cross-Border Restrictions

E-commerce frequently crosses national boundaries, subjecting edge nodes to varying data residency laws. If an edge node in one region caches partial user details or personal data, it may inadvertently breach local rules. Privacy regulations (e.g., GDPR) require that personal data be stored and processed only under lawful conditions. Retailers must design location-aware orchestration so that user data from the European Union remains on nodes residing in EU territory, for instance. Meanwhile, logs or machine learning features that replicate data to other nodes must filter out personally identifiable information or rely on tokenization. Implementing robust identity and data classification policies helps ensure that local nodes exclusively handle data types legally permissible in their region.

4.3 Vendor Management and Third-Party Edge Providers

Some e-commerce companies rely on edge services from third-party platforms, such as telecom carriers or CDN vendors. Contracts must stipulate security obligations, specifying how these providers handle encryption, patch vulnerabilities, and store cryptographic keys. Retailers remain accountable to regulators and card issuers if a third-party breach exposes user data. Formal audits, certifications (e.g., SOC 2 Type II, ISO 27001), and breach notification protocols must be spelled out. Periodic risk reviews confirm that edge vendors update their firmware, maintain physical security at remote nodes, and align with relevant compliance needs. If a vendor’s node fails an audit, the retailer can reconfigure traffic routing to bypass that location until issues are remediated.

4.4 Incident Response in a Distributed Environment

Governance frameworks define how to detect, investigate, and contain breaches across edge nodes. Real-time telemetry from each node must feed a centralized security operations center (SOC). Anomalies discovered in one region might signal a large-scale campaign targeting multiple edges. Teams must coordinate access revocation, encryption key rotation, and node isolation quickly to limit damage. The ephemeral nature of edge containers can be an advantage: re-provisioning compromised containers with fresh images is fast and standardized. However, forensic data (logs, memory dumps) must be collected swiftly before ephemeral sessions vanish. Standard operating procedures detail how to preserve digital evidence across diverse geographic sites.

4.5 Cross-Functional Training and Accountability

Edge governance extends beyond pure IT concerns. Payment, legal, and compliance teams must collaborate with DevOps and security engineers to manage how data flows between edge nodes and central systems. Training ensures local staff at edge facilities recognize physical tampering risks, such as suspicious attachments to network cables. Payment experts clarify how partial transaction data or user attributes must be masked to satisfy privacy mandates. Regular tabletop exercises test the readiness of cross-functional teams to handle edge-based intrusions, shaping a culture of collective responsibility for data protection.

4.6 Auditing and Continuous Compliance Verification

Edge computing's distributed nature complicates periodic audits. Traditional manual checklists are time-consuming when dozens or hundreds of nodes are involved. Automated compliance verification tools become mandatory, scanning node configurations, verifying cryptographic libraries, and ensuring patch levels match enterprise baselines. Summaries of compliance metrics then feed into executive dashboards, enabling swift detection of drift. External auditors or regulators might request remote access to these monitoring systems to confirm that security standards remain constant across all edge locations. Well-documented processes, version-controlled infrastructure definitions, and robust logging prove continuity of compliance in the dynamic edge environment.

Effectively governing an edge-based payment system thus requires a structured approach, ensuring each node abides by consistent encryption, logging, and vulnerability management. Achieving PCI DSS and privacy compliance in this decentralized model depends on advanced policy automation, vendor oversight, and cross-functional alignment. In the final section, we look ahead to new trends in edge security solutions and provide strategic recommendations for e-commerce leaders seeking to balance speed with robust data protection.

5. Future Developments and Strategic Recommendations

Edge computing is poised to continue reshaping e-commerce payment networks by delivering sub-second transaction times and personalized experiences. Security remains the deciding factor that determines whether these benefits align with consumer trust and regulatory compliance. As the technology evolves, retailers can adopt new techniques and refine best practices for secure, low-latency operations.

5.1 AI-Enhanced Edge Intelligence

While machine learning inference at the edge is already common for fraud detection, future approaches may integrate streaming data from multiple nodes to build a consensus view of suspicious activities. Federated learning can update global fraud models without sharing raw user data between nodes, bolstering privacy. Real-time correlation across nodes will spot multi-region attacks more rapidly. This AI-based synergy optimizes local decisions—approvals, declines, or friction-based authentication—while feeding advanced analytics pipelines for continuous improvement.

5.2 Software-Defined Perimeters and Service Mesh at the Edge

Service mesh architectures, already popular for container-based applications, will extend to edge nodes. This shift means each transaction hop will pass through a service mesh layer, which applies uniform encryption, identity validation, and rate-limiting. Closer integration with software-defined perimeters (SDP) ensures that only authenticated devices and users can communicate with the mesh. This framework can dynamically scale security rules based on user risk scores or traffic anomalies, preventing one compromised node from escalating privileges across the entire network.

5.3 Confidential Virtualization for Edge Nodes

Advances in confidential computing are lowering the overhead of memory encryption and TEE usage. Future hardware solutions may allow entire edge nodes to operate in confidential mode, where hypervisor or bare-metal OS cannot access the memory or code of e-commerce microservices. This approach effectively black-boxes payment logic from even local administrators, mitigating insider threats. For remote or physically untrusted edge sites, confidential virtualization greatly reduces the risk of hardware tampering or extended physical access.

5.4 Quantum-Safe Cryptography and Post-Quantum Readiness

Although quantum computing is not yet a mainstream threat, forward-looking e-commerce providers may begin transitioning to quantum-safe cryptographic algorithms at edge nodes. If ephemeral card tokens or TLS certificates are vulnerable to future decryption, adversaries who record traffic today could decipher it post-hoc. Rolling out post-quantum algorithms at resource-constrained edges demands efficient implementations that do not balloon CPU usage or hamper response times. Experimenting with hybrid key exchange models, mixing classical and post-quantum schemes, allows for a phased approach without sacrificing immediate security.

5.5 Greener Edge Deployments and Efficiency Gains

Global concerns about energy consumption pressure e-commerce operations to adopt sustainable technology. Edge nodes that use specialized low-power hardware may reduce operational costs and environmental footprint. Meanwhile, advanced scheduling algorithms could shift workloads to nodes powered by renewable energy or at off-peak times. Security microservices must remain active even during power-saving modes—leading to innovations in efficient cryptography and lightweight intrusion monitoring. Balancing performance, security, and carbon impact becomes a priority in the design of next-generation edge networks [8], [9].

5.6 Strategic Recommendations for Retailers

1. **Adopt Risk-Based Segmentation**: Partition edge-located services by transaction risk. High-value or suspicious transactions may pass through more rigorous checks, while routine purchases use streamlined flows.

2. **Invest in Hardware Security**: Evaluate devices that provide TEEs or memory encryption to shield sensitive code from local compromise. Ensure consistent updates to firmware or microcode.

3. **Automate Compliance and Monitoring**: Leverage policy-as-code for edge resources, implementing continuous scanning for PCI DSS controls. Integrate logs into a unified SIEM to detect multi-regional attack patterns.

4. **Orchestrate Secure DevOps**: Embed security testing in container building pipelines. Mandate signed images, minimal base layers, and robust identity management. Keep ephemeral containers ephemeral—no stored state or leftover credentials.

5. **Extend Zero-Trust End-to-End**: From user devices to edge nodes and back-end systems, enforce mutual TLS, short-lived certificates, and dynamic access policies. Simplify configurations to reduce overhead on real-time transactions.

6. **Plan for Edge Node Lifecycle**: Regularly rotate or rebuild node images, applying patches promptly. Conduct supply chain due diligence on third-party providers. Maintain a swift incident response strategy, including offline backups of encryption keys.

Retailers can confidently deploy edge computing architectures that slash payment latency without undermining data security [10], [11]. As hardware, software, and regulatory landscapes shift, a proactive stance centered on standardization, continuous improvement, and cross-functional cooperation ensures that edge nodes deliver frictionless shopping experiences and robust defense against adversaries. E-commerce stands at the cusp of an edge-driven revolution, where the synergy of low-latency architecture and embedded security can amplify both business outcomes and consumer trust.

References

[1] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, “Artificial intelligence for securing IoT services in edge computing: A survey,” *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, Sep. 2020.

[2] Y. Liu, T. Wang, S. Zhang, X. Liu, and X. Liu, “Artificial intelligence aware and security-enhanced traceback technique in mobile edge computing,” *Comput. Commun.*, vol. 161, pp. 375–386, Sep. 2020.

[3] R. Khurana, “Fraud Detection in eCommerce Payment Systems: The Role of Predictive AI in Real-Time Transaction Security and Risk Management,” *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 10, no. 6, pp. 1–32, 2020.

[4] R.-H. Hsu *et al.*, “A privacy-preserving federated learning system for android malware detection based on edge computing,” in *2020 15th Asia Joint Conference on Information Security (AsiaJCIS)*, Taipei, Taiwan, 2020.

[5] A. Velayutham, “AI-driven Storage Optimization for Sustainable Cloud Data Centers: Reducing Energy Consumption through Predictive Analytics, Dynamic Storage Scaling, and

Proactive Resource Allocation," *Sage Science Review of Applied Machine Learning*, vol. 2, no. 2, pp. 57–71, 2019.

[6] Z. Zhu, Y. Tian, F. Li, H. Yang, Z. Ma, and G. Rong, "Research on edge intelligence-based security analysis method for power operation system," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, New York, NY, USA, 2020.

[7] D. Kaul, "Optimizing Resource Allocation in Multi-Cloud Environments with Artificial Intelligence: Balancing Cost, Performance, and Security," *Journal of Big-Data Analytics and Cloud Computing*, vol. 4, no. 5, pp. 26–50, 2019.

[8] P. Marcer, X. Masip, E. Marin, and A. Jurnet, "Scaling edge computing security with blockchain technologies," in *Blockchain-enabled Fog and Edge Computing*, CRC Press, 2020, pp. 187–215.

[9] I. Ameli, N. Benamar, and A. S. Hafid, "Security and privacy issues of blockchain-enabled fog and edge computing," in *Blockchain-enabled Fog and Edge Computing*, CRC Press, 2020, pp. 155–185.

[10] S. Shekhar, "An In-Depth Analysis of Intelligent Data Migration Strategies from Oracle Relational Databases to Hadoop Ecosystems: Opportunities and Challenges," *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 10, no. 2, pp. 1–24, 2020.

[11] M. Qiu, S.-Y. Kung, and K. Gai, "Intelligent security and optimization in Edge/Fog Computing," *Future Gener. Comput. Syst.*, vol. 107, pp. 1140–1142, Jun. 2020.