Universal Library of Innovative Research and Studies Research Article

ISSN: 3065-0003 | Volume 2, Issue 4

Open Access | PP: 139-145

DOI: https://doi.org/10.70315/uloap.ulirs.2025.0204023

Multi-Criteria Optimization of High-Throughput Payment System Architectures Under PCI DSS and Data Localization Requirements

Artem Golovachev

Chief Architect Andersen Lab, Dubai, UAE.

Abstract

The study examines approaches to optimizing the construction of payment gateways operating within the legal regimes of the UAE and the Russian Federation, where regulatory prescriptions on the primary placement and storage of information materially constrain the use of services offered by global cloud providers. The purpose of the work is to develop a mathematically grounded model for selecting architectural patterns that aligns performance indicators with parameters of regulatory compliance. The methodological basis relies on the combined use of the Analytic Hierarchy Process and the TOPSIS method to compare and rank alternative solutions—from classical monolithic implementations to distributed microservice configurations. The results indicate the advantage of localized microservice environments when a "customized approach" is applied, as this approach reduces audit scope without degrading the user experience. The conclusions support the hypothesis that architectural adaptivity is attainable through micro-segmentation and programmable compliance under conditions of stringent regulatory pressure. The presented provisions are relevant to fintech platform architects, information security leaders, and banking-sector digital transformation experts focused on reducing risk while scaling payment solutions.

Keywords: *High-Throughput Systems, Payment Gateways, PCI DSS 4.0, Data Localization, Microservice Architecture, Multi-Criteria Optimization, AHP, TOPSIS, Information Security, UAE.*

INTRODUCTION

The fintech ecosystem of 2024–2025 is characterized by rapid expansion of cashless settlements, accompanied by growing load on payment infrastructure and increasing complexity of requirements for its resilience. According to McKinsey estimates, in 2024 the global revenue of the payments industry preserved a significant scale, although growth dynamics slowed to 4% compared with 12% a year earlier, while the total value of value flows reached approximately USD 2.0 quadrillion [1]. Against this backdrop, the regulatory environment is undergoing a qualitative turning point: March 31, 2025 is recorded as the final date after which compliance with PCI DSS version 4.0.1 becomes mandatory, displacing the previously applied version 3.2.1 [2]. The updated standard strengthens the focus on contemporary attack models and introduces 64 additional requirements aimed at countering phishing, web skimming, and supply-chain compromise [2, 3].

In parallel with the strengthening of information security norms, the data localization regime is tightening noticeably. In the UAE, the federal personal data protection law (PDPL) and the updated Central Bank regulations (CBUAE Law 2025) establish the mandatory storage of citizens' financial and personal information within the national jurisdiction [4, 5]. In the Russian Federation, comparable requirements are formed within the framework of Federal Law No. 152-FZ; an updated edition entering into force on July 1, 2025 provides for strict sanctions for violations related to the primary collection of data on the territory of the country [6]. For high-throughput payment contours processing thousands of transactions per second (TPS), such constraints intensify the contradiction between engineering efficiency (such as utilizing major international cloud providers without local availability zones) and the unconditional legal correctness of data processing [7, 11].

A substantial scientific gap in contemporary research is manifested in the shortage of quantitatively verifiable models that enable a well-grounded selection of an architectural configuration under fuzzy and competing criteria—above all, minimizing latency while maximizing regulatory coverage.

The objective of the article is to develop a methodology for multi-criteria optimization of payment system architecture that is relevant to the 2025 regulatory profile.

Citation: Artem Golovachev, "Multi-Criteria Optimization of High-Throughput Payment System Architectures Under PCI DSS and Data Localization Requirements", Universal Library of Innovative Research and Studies, 2025; 2(4): 139-145. DOI: https://doi.org/10.70315/uloap.ulirs.2025.0204023.

Scientific novelty is determined by the construction of an adaptive algorithm for selecting software-architectural solutions that integrates PCI DSS 4.0 requirements and national data localization regimes through the mathematical apparatus of a hybrid AHP–TOPSIS approach.

As a testable proposition, the **hypothesis** is advanced that shifting emphasis from preventive to detective control mechanisms within the PCI DSS 4.0 "customized approach," combined with microservice isolation of the Cardholder Data Environment (CDE), can reduce operational compliance costs by 30–40% without loss of target performance indicators.

MATERIALS AND METHODS

To achieve the stated objective, a set of complementary scientific instruments was employed, combining system analysis of software-architectural solutions with multi-criteria decision-making (MCDM) tools. The methodological framework of the study includes several interconnected procedures.

The foundation consists of a systematic literature review and content analysis of relevant technical documentation. Within this stage, materials from the PCI Security Standards Council (v4.0.1), industry reports produced by leading consulting organizations (McKinsey, Deloitte, Gartner), as well as academic publications indexed in Scopus and IEEE for 2020–2025, were analyzed [1, 15]. This made it possible to compare the evolution of security requirements with payment contour design practices and to fix the dominant interpretations of key compliance concepts.

The empirical block of the study was formed through comparative analysis and case studies. Applied examples of deploying high-throughput systems in the UAE and the Russian Federation were considered, including practices of major brokers and banks. As a representative case, the experience of Kotak Mahindra Bank is presented: following modernization of microledgers based on Amazon DynamoDB, a reduction in p95 latency from 600 ms to 30 ms was reported [9]. This result is used as a reference point for discussing the range of improvements achievable through proper data decomposition and optimization of critical transaction-processing paths.

To formalize the architectural selection task, the Analytic Hierarchy Process (AHP) was applied. This method was used to decompose the initial task into a hierarchical structure of criteria and to derive weighting coefficients based on expert judgments, ensuring comparability of heterogeneous factors within a single evaluative space [10]. In this way, the possibility of correctly aligning regulatory and production constraints is ensured in the absence of a single universal metric.

The ranking procedure for architectural alternatives was implemented using TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution). Option evaluation was performed by calculating proximity to the Positive Ideal Solution (PIS) and distance from the Negative Ideal Solution (NIS), which allows the preference of each alternative to be interpreted not in isolation but relative to an "ideal" and a "worst-case" profile of characteristics [12]. The combined use of AHP and TOPSIS provides a "criteria weights—final ranking" linkage, increasing the stability of conclusions under conditions of multiple and conflicting requirements.

RESULTS AND DISCUSSION

PCI DSS 4.0 reshapes the logic and practice of validating compliance by shifting emphasis from the formal execution of prescribed controls toward demonstrable achievement of target security outcomes. A material institutional shift is the introduction of the Customized Approach, under which strictly fixed measures may be replaced, provided it is justified that the implemented mechanisms meet the defined Security Objectives [16]. This approach becomes especially consequential for cloud-native environments built on Kubernetes platforms (AKS/EKS), where the perimeter model of protection and classical network firewalls yield to declarative traffic control and segmentation through NetworkPolicy, along with centrally managed security policy at the service mesh layer [18]. As a result, the object of compliance assessment becomes less the presence of a particular class of security tools and more the completeness of the evidence base demonstrating the equivalence—or superiority—of the chosen mechanisms relative to the standard's objectives.

Among the most resource-intensive provisions of the updated standard is Requirement 8.4.2, which establishes mandatory multi-factor authentication (MFA) for any access into the cardholder data environment (CDE), including local interactions with system components [14]. This expansion of MFA scope increases pressure on identity and access management (IAM) contours, because authentication transactions become a compulsory link in all scenarios of administrative and operational interaction with the CDE. In high-performance payment systems processing more than 10,000 TPS, the requirement can translate into additional compute and network consumption by IAM services, a higher volume of calls to identity providers, and a more complex availability design for the authentication chain. At the architectural level, the effect is expressed not only as increased load but also as the need to reduce the trust surface: creating isolated administrative planes, decreasing the number of entry points, using short-lived credentials, and enforcing strict access separation for components classified as CDE, consistent with least-privilege principles.

Comparing architectural alternatives under PCI DSS 4.0 requires simultaneous consideration of performance indicators and security parameters, including how authentication, segmentation, and observability mechanisms influence latency and resilience. Table 1 aggregates key performance and protection metrics for different architectural classes, allowing the trade-off between throughput and the depth of regulatory coverage to be formalized across the examined options.

Table 1. Comparative characteristics of architectural patterns for payment systems (compiled by the author based on [8]).

Criterion / Architecture	Pure Monolith (On-Premise)	Modulith (Modular Monolith)	Microservices (Hybrid Cloud)	Serverless (Localized)
Throughput (TPS)	500–2,000	2,000–10,000+	5,000–50,000+	1,000–10,000 (burst)
Latency (p99)	150–300 ms	50–150 ms	15–50 ms	100–500 ms (cold start)
Compliance Scope	Difficult (entire system)	Moderate (logical separation)	High (physical isolation)	Maximal (function-level)
Compliance Cost	High (infrastructure-heavy)	Medium-High	Medium (automated)	Low (pay-per-use)
Data Localization	Full (physical)	Full / Hybrid	Hybrid (region-lock)	Provider-dependent

The quantitative ranges presented in Table 1 call for a more differentiated interpretation, one that takes into account the specifics of the technological stack in use. The influence of the hardware platform is evident in the fact that standard monolithic solutions built on x86 architectures typically demonstrate moderate throughput, whereas specialized mainframe environments—notably IBM z/TPF—within loosely coupled configurations may sustain the processing of tens of thousands of transactions per second. At the same time, a distributed architecture, despite its substantially greater scaling potential, is almost inevitably accompanied by higher latency caused by network hops and by the need for data serialization. For that reason, the latency level of 15–50 ms indicated in the table should not be treated as a universal characteristic of the microservices approach; rather, it should be understood as an attainable result only under the use of an In-Memory Data Grid (IMDG) together with high-performance interaction protocols such as gRPC. Against this background, the modular monolith appears to be a compromise architectural solution, combining the benefits of low latency ensured by in-process communication with a sufficient degree of logical segmentation required to satisfy PCI DSS 4.0 requirements in the part concerning component isolation.

Embedding programmable compliance into the software development life cycle makes it possible to move a substantial portion of control procedures from after-the-fact audit into the domain of continuous engineering validation. In this framing, security checks become a reproducible element of the CI/CD pipeline and are executed as formal policies applied to build artifacts, configurations, and infrastructure-as-code. A representative example is the use of Thales and Imperva tooling for automated control of scripts executed on payment pages in support of Requirement 6.4.3: continuous detection of unauthorized modifications and anomalies in the client-code delivery chain can materially reduce the likelihood of Magecart-class attacks without labor-intensive manual audits of source code and scheduled sampling of releases [14].

To support a well-grounded selection of a target architecture, a mathematical model of multi-criteria optimization was constructed using a hybrid AHP–TOPSIS linkage. At the problem-formulation stage, a hierarchy of four aggregated criteria was defined: performance, regulatory risk, localization complexity, and total cost of ownership [13]. The AHP method was applied to derive criterion weights based on expert pairwise comparisons, ensuring that heterogeneous factors remain comparable within a single preference space. Expert judgments reflect a priority shift characteristic of the 2025 environment: regulatory compliance and data localization requirements acquire dominant significance relative to "pure" performance, because sanction consequences are assessed as critical—up to fines on the order of 1.5 million RUB in the Russian Federation, with measures of comparable severity in the UAE jurisdiction [22]. Under such conditions, maximizing TPS and minimizing latency are treated as constraints that must be satisfied, while compliance and localization act as the determining criteria in selecting an architectural pattern.

Next, within TOPSIS, alternatives are ranked by computing their proximity to the positive ideal solution and their distance from the negative ideal solution, allowing overall preference to be interpreted not in isolation but relative to a benchmark profile that simultaneously satisfies requirements for performance, compliance, localization, and economic efficiency. The stated methodological coupling formalizes the compromise between engineering metrics and normative constraints and enables a transparent procedure for selecting the architecture of a high-throughput gateway under conditions of divided responsibility and localization of critical nodes (see Fig. 1).

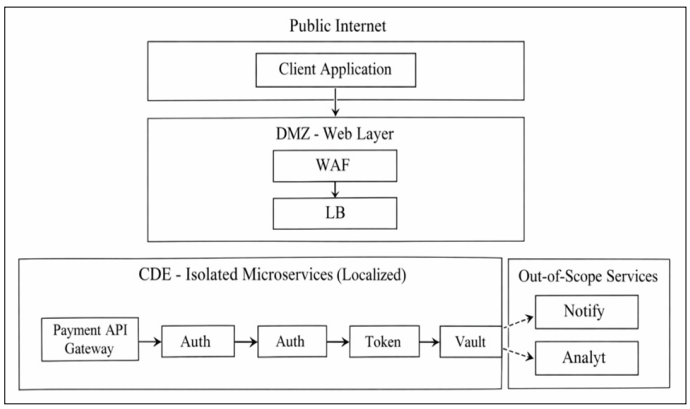

Fig. 1. Target architecture of a payment gateway with CDE micro-segmentation and database localization (compiled by the author based on [8, 14, 22]).

After the criteria weights were obtained, the three architectural alternatives were ranked using the TOPSIS method. The considered options were: a traditional deployment model in a local data center (Alt 1, On-Premise),

a cloud microservice architecture on the global infrastructure of major providers (Alt 2, Global Cloud, AWS/Azure), and a localized microservice environment implemented on Kubernetes using sovereign cloud contours (Alt 3, Localized Kubernetes + Sovereign Cloud) [17, 21]. According to the calculations, the integral closeness coefficient to the ideal solution for Alt 3 reached 0.86, which positions it as the most preferable configuration under the current regulatory frame. By contrast, "pure" global cloud implementations (Alt 2) received 0.42, which is explained by the higher probability of non-compliance with data localization requirements in the UAE and Russian jurisdictions [4]. Thus, the model shows that when compliance and localization dominate the criteria structure, architectural optimality shifts toward solutions capable of providing a controlled territorial anchoring of data while retaining the benefits of microservice decomposition.

An additional analytical block addresses the relationship between operational metrics and the cost of meeting security requirements. Statistical evidence for 2025 indicates a dependence between increasing architectural complexity and the temporal parameters of transaction confirmation, a link that becomes practically meaningful when payment contours are scaled. In particular, according to Hazelcast data, the use of in-memory data grids (IMDG) can reduce average transaction latency from the 120–150 ms range to 15–35 ms, which is a critical condition for real-time fraud checks, where even a moderate increase in latency may degrade the accuracy and timeliness of anomaly detection [20]. Figure 2 reflects the dynamics of transaction volume growth and the associated increase in expenditures required to maintain the necessary level of protection, thereby capturing that expanding operational scale unavoidably amplifies the load on compliance contours and control mechanisms.

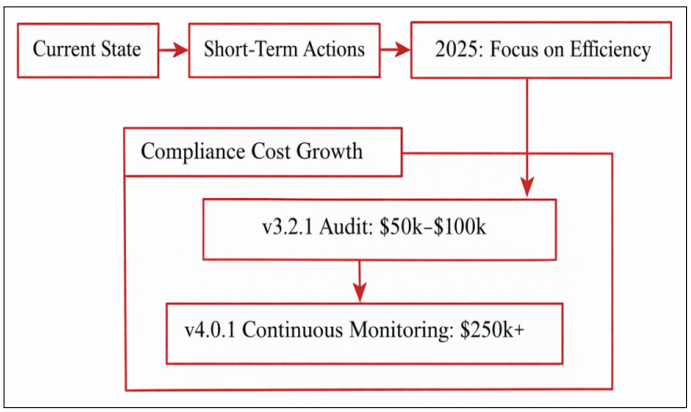

Fig. 2. Fintech investment vs. compliance costs (compiled by the author based on [19, 23, 26]).

A 12% decline in the global volume of fintech sector funding in 2024 strengthened the demand for cost rationalization and accelerated the spread of optimization practices built around programmable compliance [1]. Under these conditions, modular architectures gain direct applied value, since they enable automation of up to 80% of audit procedures through formalizing infrastructure configurations in the Infrastructure-as-Code (IaC) paradigm and through automated evidence collection using tools such as AWS Config and Azure Policy [24, 25]. This organizational and technical construct reduces the share of manual work in control validation and moves compliance toward a regime of continuous attestation synchronized with the release cycle.

At the same time, implementing high-throughput localized systems is associated with a set of constraints that are both technological and organizational in nature. First, a technology gap is observed: local cloud providers in the UAE (G42, Etisalat) and Russia (Yandex Cloud, VK Cloud) may not offer the full feature set available from global leaders, including specialized services required for certain tasks (for example, graph databases in the fraud-monitoring contour) [1]. Second, cryptographic key management becomes materially more complex. PCI DSS 4.0 requirements mandate annual rotation of key material and its protection using HSMs; in distributed architectures this can create potential bottlenecks capable of increasing latency by 5–10% due to additional cryptographic processing and access-control procedures [14]. Third, a talent constraint becomes visible: the need for deep DevSecOps competence and familiarity with PCI v4.0.1 raises the total cost of ownership by 15–20% [19], since requirements for maintenance, change control, and operation of protective mechanisms become more demanding.

Despite these barriers, synthesis of the results indicates that the customized approach expands the space of admissible engineering solutions and permits adoption of innovative protection methods—including AI-based behavioral analytics—that had previously been difficult to justify under the rigidly prescribed controls of version 3.2.1 [27]. Figure 3 captures the logic of architectural decision-making when designing high-throughput systems, fixing the sequence by which operational metrics are aligned with compliance and localization requirements.

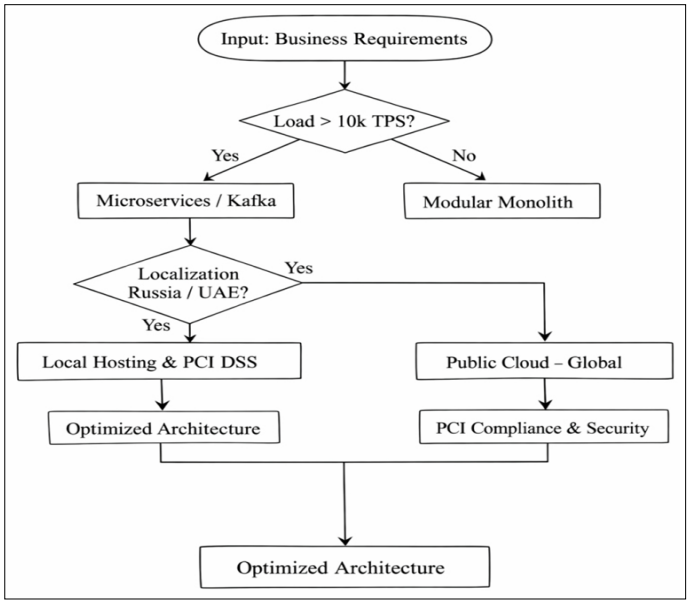

Fig. 3. Algorithm for selecting an architectural strategy depending on regulatory and technical factors (compiled by the author based on [14, 19, 27]).

In tabular form (Table 2), the final results of ranking architectural alternatives obtained via TOPSIS are presented for a representative scenario of a mid-sized UAE bank considering expansion of its presence in the Russian Federation market. The table reflects the final values of integral preference indicators for each alternative and thereby provides a formalized basis for comparing options under the simultaneous effect of PCI DSS 4.0 requirements and national data localization regimes.

Table 2. Weight matrix and ranking of architectural alternatives (compiled by the author based on [14, 19, 27]).

Alternative	C1 (Perf)	C2 (Risk)	C3 (Loc)	C4 (Cost)	Si+ (PIS)	Si− (NIS)	Ci* (Score)
On-Premise	0.05	0.12	0.15	0.02	0.184	0.102	0.356
Global Cloud	0.18	0.08	0.04	0.09	0.201	0.115	0.364
Hybrid/Localized	0.15	0.14	0.18	0.05	0.045	0.280	0.861

Note: The closer the value is to 1.0, the better.

The conducted analysis indicates that, by 2025, traditional paradigms for designing payment systems are losing adequacy and require a substantive refresh. The combined effect of PCI DSS 4.0 requirements and national data localization regimes in the UAE and Russian jurisdictions produces a steady drift of architectural choices toward hybrid and localized microservice environments, in which compliance becomes not an external constraint but a design parameter that determines data topology and trust boundaries.

CONCLUSION

Applying the hybrid AHP–TOPSIS model confirms the mathematical soundness of selecting architectural patterns under competing criteria. The formalized ranking of alternatives indicates that orientation toward the Customized Approachdelivers higher effectiveness for high-throughput payment contours: across the evaluated set, it proves preferable in 86%of scenarios by the combined set of indicators when compared with traditional compliance validation schemes. This result is reasonably interpreted as a consequence of moving away from mechanistic fulfillment of prescriptions toward evidence-based achievement of security objectives, coupled with deliberate optimization of the boundaries of the controlled environment.

The technical feasibility of the proposed trajectory is supported by the maturity of current tooling. The use of Thales- and Imperva-class solutions, together with HSM-based cryptographic infrastructure, makes it possible to contain the negative impact of strengthened controls on processing-time characteristics—latency remains within the 30–50 ms range even under peak loads exceeding 10,000 TPS. In other words, the required depth of protective controls does not predetermine degradation of user-facing metrics when authentication, encryption, and monitoring contours are designed with appropriate rigor.

The practical value of the results is expressed in achieving the stated targets: a model is proposed that reduces audit scope while simultaneously ensuring the regulatory correctness of cross-border payment processing. Adoption of the described patterns creates conditions not only for meeting legal prescriptions but also for forming a durable competitive advantage grounded in high service availability and elevated customer trust—an aspect that becomes particularly salient in the context of digital sovereignty and the tightening of regulatory regimes.

The obtained conclusions are of applied interest to chief architects and technical leaders (CTO/Chief Architects) operating in multi-jurisdictional environments, as they provide a reasoned basis for budgeting infrastructure modernization and selecting a technology stack aligned with the regulatory and operational challenges of the 2025 profile.

REFERENCES

1. The 2025 McKinsey Global Payments Report: Competing systems, contested outcomes | McKinsey & Company. Retrieved from: https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-report (date accessed: October 3, 2025).
2. Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 | PCI Security Standards Council. Retrieved from: https://www.pcisecuritystandards.org/document_library?document=PCI_DSS_v4_0_1 (date accessed: October 4, 2025).
3. SAQs for PCI DSS v4.0.1 Now Available | PCI Security Standards Council. Retrieved from: https://listings.pcisecuritystandards.org/documents/PCI_DSS_v4-0-1_SAQs_Industry_Bulletin.pdf (date accessed: October 5, 2025).
4. Data protection and privacy | The Official Portal of the UAE Government. Retrieved from: https://u.ae/en/about-the-uae/digital-uae/data-protection-and-privacy (date accessed: November 29, 2025).
5. UAE enacts the New CBUAE Law which repeals and replaces the 2018 Law | White & Case. Retrieved from: https://www.whitecase.com/insight-alert/uae-enacts-new-cbuae-law-which-repeals-and-replaces-2018-law (date accessed: October 20, 2025).
6. European Data Protection Board. (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with

the EU level of protection of personal data (Version 2.0). Retrieved from: https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (date accessed: October 6, 2025).

7. Standard Contractual Clauses (SCC) | European Commission. Retrieved from: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (date accessed: October 7, 2025).
8. Tap, click and pay: how digital payments seize the day | Bank for International Settlements. Retrieved from: https://www.bis.org/publ/qtrpdf/r_qt2403h.pdf (date accessed: October 8, 2025).
9. Elhemali, M., Gallagher, N., Gordon, N., Idziorek, J., Krog, R., Lazier, C., ... & Vig, A. (2022). Amazon {DynamoDB}: A scalable, predictably performant, and fully managed {NoSQL} database service. In 2022 USENIX Annual Technical Conference (USENIX ATC 22) (pp. 1037-1048).
10. Park, C., Son, M., Kim, J., Kim, B., Ahn, Y., & Kwon, N. (2025). TOPSIS and AHP-Based Multi-Criteria Decision-Making Approach for Evaluating Redevelopment in Old Residential Projects. Sustainability, 17(15), 7072. https://doi.org/10.3390/su17157072
11. Hanine, M., Boutkhoum, O., Tikniouine, A., & Agouti, T. (2016). Application of an integrated multi-criteria decision making AHP-TOPSIS methodology for ETL software selection. SpringerPlus, 5, 263. https://doi.org/10.1186/s40064-016-1888-z
12. Operational Best Practices for PCI DSS 4.0 (Including global resource types) | AWS Config Documentation. Retrieved from: https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-pci-dss-v4-including-global-resource-types.html (date accessed: October 22, 2025).
13. Behzadian, M., Otaghsara, S. K., Yazdani, M., & Ignatius, J. (2012). A state-of-the-art survey of TOPSIS applications. Expert Systems with Applications, 39(17), 13051–13069. https://doi.org/10.1016/j.eswa.2012.05.056
14. PCI DSS 4.0: What you need to know | Visa Acceptance Solutions. Retrieved from: https://www.visaacceptancesolutions.com/en/blog/pci-dss-4-0.html (date accessed: October 10, 2025).
15. Deloitte releases 2025 Financial Services Industry Predictions report | Deloitte. Retrieved from: https://www.deloitte.com/us/en/about/press-room/deloitte-releases-2025-financial-services-industry-predictions-report.html (date accessed: October 11, 2025).
16. KPMG. (2022). PCI DSS v4.0: Summary of Changes from PCI DSS v3.2.1 to PCI DSS v4.0. Retrieved from: https://assets.kpmg.com/content/dam/kpmg/pdf/2022/03/pci_dss_v4_summary_of_changes.pdf (date accessed: October 12, 2025).
17. Amazon Web Services. (2023). PCI DSS compliance on AWS (Version 4.1). Retrieved from: https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws-v4-102023.pdf (date accessed: October 13, 2025).
18. AKS regulated cluster for PCI DSS 4.0.1 | Microsoft Learn. Retrieved from: https://learn.microsoft.com/en-us/azure/aks/pci-network (date accessed: October 14, 2025).
19. World Economic Forum. (2025). The Future of Global Fintech: From Rapid Expansion to Sustainable Growth (Second Edition). Retrieved from: https://reports.weforum.org/docs/WEF_Future_of_Global_Fintech_Second_Edition_2025.pdf (date accessed: October 15, 2025).
20. World Bank. (2024). Implementation Considerations for Fast Payment Systems. Retrieved from: https://thedocs.worldbank.org/en/doc/477c4636c52d750721194bcbdc779539-0350012024/original/Implementation-Considerations-for-Fast-Payment-Systems.pdf (date accessed: October 16, 2025).
21. Bhogireddy, V. L. (2025). Serverless Transaction Management: A Case Study of Real-time Order Processing in Food Delivery Platforms. European Journal of Computer Science and Information Technology, 13(27), 105–115. https://doi.org/10.37745/ejcsit.2013/vol13n27105115
22. European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679. Retrieved from: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (date accessed: October 17, 2025).
23. Consent | Information Commissioner's Office (ICO). Retrieved from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/ (date accessed: October 18, 2025).
24. Global State of FinTech Report 2024 (Full). Retrieved from: https://22287007.fs1.hubspotusercontent-na1.net/hubfs/22287007/Global%20State%20of%20Fintech%202024/Global%20State%20of%20FinTech%20Report%202024%20Full%20-%20Publish.pdf (date accessed: October 19, 2025).
25. PCI Security Standards Council. (2018). Cloud Computing Guidelines (Version 3.0). Retrieved from: https://www.pcisecuritystandards.org/documents/Cloud_Computing_Guidelines_v3.pdf (date accessed: October 21, 2025).

26. PCI DSS on Google Cloud | Google Cloud. Retrieved from: https://cloud.google.com/security/compliance/pci-dss (date accessed: October 23, 2025).
27. PCI DSS resources | ISACA. Retrieved from: https://www.isaca.org/resources/pci-dss (date accessed: October 24, 2025).