Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure and Compliant Cloud Migration Strategies for E-Commerce Systems

Dilip Prakash Valanarasu
Alagappa University, Tamil Nadu, Karaikudi, India
dilipprakash@gmail.com

ARTICLE INFO

Received: 20 Jan 2024

Accepted: 28 Mar 2024

ABSTRACT

With the rapid pace of digital transformation across industries, e-commerce companies are increasingly compelled to adopt cloud technologies. This transition enables organizations to meet modern expectations for scalability, operational flexibility, and cost-efficiency. However, such a proposed change raises security and compliance issues with respect to guarding sensitive customer information and adhering to the laws and regulations, such as GDPR, PCI DSS, and data sovereignty-related legalities. This paper deals with secure methods for the migration of e-commerce to the cloud. Some of these aspects are cloud building blocks, deterrents, and remedies using zero trust concepts, encryption, and DevSecOps. The other areas discussed include relevant framework regulations, case studies on successful migrations, and, finally, actionable recommendations as to the businesses that need to be resilient and compliant in the future-ready cloud migration.

Keywords: Cloud Migration; E-Commerce Security; Regulatory Compliance; GDPR; DevSecOps

1. Introduction

The digitization across the global markets has eclipsed the e-commerce system in the usage of cloud infrastructure for it to be competitive, scalable, and agile. The traditional on-premise IT architecture is better in many respects, but fails to keep up with the swift evolution of customer demands and changing dynamics of e-commerce traffic. Hence, rearchitecting the modern e-commerce frameworks revolves around four pillars, with the cloud being one. On the other hand, cloud migration represents a multi-layered and complex transformation, particularly when examined through the lenses of security, regulatory compliance, and service-level requirements. Additionally, it may pose challenges from the perspective of maintaining customer trust and assurance. Cloud migration is no longer viewed as a trade-off between maintaining security and meeting regulatory compliance requirements. Instead, it has become an urgent necessity for e-commerce organizations. These businesses must protect sensitive customer data, ensure full legal compliance, and capitalize on the benefits of scalable and flexible computing resources [1][2][3]. The major concern with regard to this strategic need pertains to its extent with respect to the maturity or sophistication of cyber threats. Such attacks are exceedingly perilous to any e-commerce site because of the massive bulk of sensitive information involved-such as PII, financial details, or even data relating to user identifications. An insecure or non-compliant cloud migration inherently nurtures threats to security and thereby detracts from customer confidence, brand reputation, and compliance status. Compliance-related legislation, such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and various regional data protection laws, imposes strict and often challenging requirements on e-commerce platforms. These legal frameworks govern how data must be handled both at rest and in transit, and apply to data involved in both current and past cloud migration processes [4][5][6]. This article thus tries to explore secure and compliant cloud migration paradigms that are tailor-made for e-commerce systems. It begins with a brief discussion on the cloud computing environment in e-commerce and ends with the problem of cloud migration. Later, it proceeds to see the security, compliance, and case-based approaches to making the transition able to work seamlessly and securely.

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. The Role of Cloud Infrastructure in E-Commerce

The truth of the hidden message of cloud computing in e-commerce precedes the argument of the reason why one would construct safe and conforming migration procedures. The e-commerce business environment is highly dynamic and competitive, with real-time transactions, surges in traffic, and global coverage. Traditional on-premise solutions lack scalability, are costly, and do not generally provide the scalability required in digital retail. Compared to this, the cloud computing platform possesses scalable computing capabilities, fast deployment, global content delivery, and disaster recovery solutions that align with business models in e-commerce [7][8][9]. Moreover, the cloud services are on-demand, scalable, and they could help e-commerce sites to survive times of high traffic, such as Black Friday or Cyber Monday, without the performance deteriorating. Such solutions as content delivery networks (CDNs), serverless computing, container orchestration (e.g., Kubernetes), and microservices architecture have been added to the current e-commerce cloud environments [10][11][12]. However, while the technological benefits of cloud migration are clear, these advancements also bring an expansion of the attack surface. As e-commerce platforms adopt multi-cloud or hybrid cloud architectures, the complexity of managing security configurations, access controls, and regulatory requirements increases significantly. For instance, a single misconfigured storage bucket in a cloud environment can expose millions of customer records, leading to data breaches and compliance failures. Therefore, while cloud computing empowers e-commerce systems, it concurrently necessitates robust strategies for securing data, managing access, and ensuring compliance [13][14]. The transition from on-premise systems to cloud-hosted environments introduces a fundamental shift in the shared responsibility model. In a cloud setting, service providers such as AWS, Azure, or Google Cloud assume responsibility for infrastructure security, while customers are responsible for application-level and data-layer security. This demarcation requires that e-commerce companies actively manage encryption, identity and access management (IAM), logging, and incident response mechanisms within the cloud environment. Therefore, adopting cloud infrastructure does not diminish the responsibility of e-commerce firms to maintain security and compliance; rather, it intensifies the obligation to uphold these standards across increasingly complex environments [15][16]. As we transition into the next section, the challenges involved in cloud migration must be examined more deeply, especially those that pose significant security and compliance risks during the migration lifecycle.

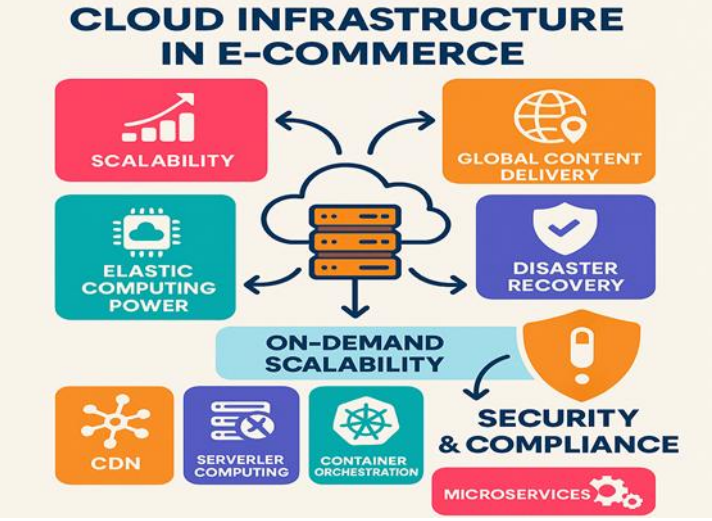

Figure 1: The figure illustrates the critical role of cloud infrastructure in e-commerce, highlighting features like scalability, global content delivery, elastic computing, and security compliance

3. Challenges in Secure Cloud Migration for E-Commerce

The challenges are not just technical but also strategic and regulatory, which have a significant effect on the success of the whole migration project. The stakes are particularly high concerning the case of e-commerce platforms, since the absence of stability, data breach, or non-observance may cause a revenue loss directly, legal penalties, and the loss of customer trust. Therefore, in order to remain in operational integrity and remain legal, it is important to undergo a

Research Article

process of cloud migration in a security-centric and compliance-friendly manner. The risk of transferring the data and the sensitivity is another one of the largest issues faced when migrating to the cloud. E-commerce websites contain immense data of personally identifiable information (PII), card details, shopping habits, and history. In case of migration, it will probably need to transfer data between on-premise systems and cloud servers, and in the majority of situations, it will be a public or semi-public network. Without end-to-end encryption and sophisticated authentication, data in transit can be intercepted, tampered or unauthorized access to the data can occur [17][18]. Moreover, the legacy systems may lack the existing encryption standard, and they may need a large amount of re-engineering to be capable of migrating the data safely.

In addition to data transit vulnerabilities, another significant challenge is system downtime and service disruption. Unlike other industries, e-commerce cannot afford prolonged service interruptions. Downtime directly correlates with lost sales opportunities, negative customer experience, and reputational damage. Migrating to the cloud involves transferring databases, reconfiguring applications, and testing new deployments, all of which must be executed with precision and often within constrained time windows. Techniques such as live migration, blue-green deployments, and hybrid architectures are often employed to minimize disruption, but their implementation adds complexity and introduces further security considerations [19][20]. Furthermore, compliance with legal and industry regulations becomes particularly complicated during and after migration. Regulations such as GDPR, HIPAA, CCPA, and PCI DSS impose strict requirements on how data is stored, processed, and transferred across jurisdictions. For example, the General Data Protection Regulation (GDPR) stipulates that the personal data of European Union (EU) citizens must not be transferred to countries or regions that lack adequate data protection measures. Such transfers are only permitted if the data subject has given explicit consent, or if appropriate safeguards such as standard contractual clauses or binding corporate rules are implemented. E-commerce firms operating across borders must ensure that their cloud providers offer data residency options and comply with international standards for data protection [21][22]. Failure to do so may result in hefty penalties and permanent reputational harm.

Another critical challenge lies in identity and access management (IAM) within the new cloud environment. Unlike centralized, on-premise systems, cloud platforms rely on distributed access controls, often managed through role-based access control (RBAC) and federated identities. Improper configuration of IAM policies can lead to privilege escalation, unauthorized access, and lateral movement within the cloud infrastructure. To effectively mitigate these risks, it is essential for organizations to adopt key security strategies such as the principle of least privilege, continuous monitoring, and the zero-trust security model. However, the successful implementation of these approaches demands a comprehensive understanding of both cloud-native infrastructure and pre-existing identity and access management systems [23][24]. In addition to IAM, configuration management emerges as a significant concern. Misconfigured cloud resources such as storage buckets, API gateways, and security groups are among the most common causes of cloud security breaches. Misconfigurations often occur due to human error, lack of cloud expertise, or failure to enforce security baselines. E-commerce companies undergoing cloud migration must adopt advanced automation practices to maintain infrastructure consistency and compliance. This includes the use of automated configuration management tools, the implementation of Infrastructure as Code (IaC), and the integration of compliance-as-code techniques. Together, these tools help ensure that infrastructure remains secure, standardized, and aligned with regulatory requirements throughout its entire lifecycle [25][26].

Security monitoring and incident response also face challenges in cloud environments. Traditional intrusion detection and prevention systems (IDPS) may not function effectively in dynamic, containerized, or serverless environments. E-commerce platforms must adapt their security operations to integrate with cloud-native monitoring tools, establish centralized logging systems, and ensure real-time alerting for anomalous behavior. Moreover, incident response plans must be revised to incorporate the cloud provider's role, SLAs, and specific response procedures for multi-tenant environments [25][26]. An often-underestimated challenge is vendor lock-in. Many cloud service providers offer proprietary tools, APIs, and development environments that may not be compatible with other platforms. While these tools can accelerate migration and development, they also bind the organization to a specific provider, making future migrations costly and complex. For e-commerce companies, vendor lock-in not only limits flexibility but also raises concerns about compliance portability, data sovereignty, and long-term cost management. Employing containerization,

Research Article

open source, and setting the stage, the paper looks at the security frameworks and techniques to help secure the migration.

4. Security Strategies for Cloud Migration in E-Commerce

Beginning with challenges in cloud migration, e-commerce security calls for embedding the security principle at the design stage instead of seeing it as an afterthought. Given how sensitive customer data is, along with concerns about transactional integrity and trust, a layered security approach is needed. Zero Trust Architecture (ZTA) forms the base wherein no implicit trust exists for any user or device-anything must be verified all along. Given the numerous external users and partners, ZTA provides security via multifactor authentication, micro-segmentation, dynamic access controls, and continuous monitoring [1][2]. To enhance data protection, encryption must be applied both at rest and during transit. This is particularly critical for securing sensitive information such as payment details, personal data, and user credentials. Recommended encryption standards include Advanced Encryption Standard (AES) with 256-bit keys for data at rest, and Transport Layer Security (TLS) for data in transit. Additionally, following key management best practices such as the use of customer-managed encryption keys further strengthens the overall security posture [3][4]. Furthermore, Identity and Access Management (IAM) plays a critical role in enhancing cloud security by enforcing the principle of least privilege. This is achieved through the implementation of Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and federated identity solutions. In addition, the logging and auditing of IAM-related activities are essential for detecting unusual or unauthorized behaviors. These practices contribute significantly to ensuring a secure, compliant, and reliable cloud migration process for e-commerce organizations [15][16].

Security monitoring and threat detection have to be implemented alongside the security architecture, and that is of equal importance. On-prem tools for security are generally unsuitable, given that a cloud environment is dynamic and constantly renewed. The cloud provider comes with its own set of tools, such as AWS GuardDuty, Azure Security Center, and Google Cloud Security Command Center, to detect threats in real time, send anomaly alerts, and assess vulnerabilities. These tools must be woven into an e-commerce company's Security Operations Center (SOC), along with automated incident-recovery workflows able to address threats before escalation [7][8]. Furthermore, a secure migration also requires infrastructure as code (IaC), along with security-as-code conventions. These methodologies involve codifying infrastructure configurations (e.g., network topologies, access policies, firewall rules) using scripts that can be version-controlled, tested, and automatically deployed. Tools such as Terraform, AWS CloudFormation, and Ansible support this approach and help ensure that every infrastructure change is secure by design. By incorporating security controls directly into the codebase, organizations reduce the risk of human error and enforce policy consistency across environments [13][15].

Another critical security strategy is the implementation of container security and orchestration. Many modern e-commerce systems are built using containerized microservices deployed through orchestration platforms such as Kubernetes. These containers must be scanned for vulnerabilities, continuously monitored for runtime anomalies, and protected using network segmentation and admission controls. Runtime protection tools and Kubernetes-native policies such as PodSecurityPolicies (PSPs) or Open Policy Agent (OPA) can enforce secure behaviors at scale. Regular image scanning and the use of trusted image registries further ensure that only verified and secure code enters production [11][12]. For companies adopting a hybrid or multi-cloud approach, secure connectivity and network segmentation are fundamental. E-commerce systems often span multiple regions and cloud zones, making secure communication channels vital. Virtual Private Clouds (VPCs), private endpoints, transit gateways, and VPNs ensure encrypted and isolated traffic between services. Network segmentation limits lateral movement within the environment, minimizing the blast radius in the event of a breach. Security groups and network access control lists (NACLs) must be tightly configured and continuously monitored [13][14].

Security governance and policy enforcement must be instituted from the top down. A well-defined security governance model outlines who is responsible for what within the cloud environment, defines acceptable usage policies, and establishes incident response protocols. Compliance with standards such as ISO 27001, SOC 2, and NIST SP 800-53 should be part of the organizational security posture, and these standards must be enforced using automated compliance tools provided by cloud platforms or third-party vendors [15][16]. It is equally important to integrate DevSecOps

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

practices into the development lifecycle. Security must shift left, meaning it should be integrated into development workflows from the very beginning rather than being applied post-deployment. To maintain a secure development lifecycle, it is essential to integrate security measures at every stage of the software delivery process. This includes implementing Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to identify vulnerabilities in both source code and running applications. Additionally, secret scanning and dependency management must be enforced to detect hardcoded credentials and insecure third-party libraries. Continuous Integration (CI) pipelines should also be equipped with security gates that automatically block the deployment of vulnerable code into production environments. For e-commerce platforms that deploy changes rapidly, this shift-left approach ensures that new features do not introduce security flaws [17][18].

Finally, constant training and awareness on security are non-technical but must be present for any successful security strategy [19][20]. E-commerce businesses must avoid relying on a single control or solution but instead weave an interlocking set of strategies working together to minimize risk, maintain data confidentiality and integrity, and guarantee continuous compliance. Our next discussion will explore the linkage between regulatory compliance frameworks-general as well as industry-type-and cloud security strategies in guiding the safe migration of e-commerce.

Figure 2: Infographic highlighting key security strategies for cloud migration in e-commerce

To complement the discussed security frameworks, it is valuable to examine how different cloud-native security features map to specific e-commerce needs. The table below outlines key cloud-native security tools across major providers and their relevance to securing e-commerce environments.

Table 1: Cloud-Native Security Tools and Their E-Commerce Applications

Cloud Provider	**Security Tool**	**Purpose in E-Commerce**	**Notable Features**
AWS	**AWS GuardDuty**	Threat detection and anomaly monitoring	Detects malicious IPs, compromised EC2 instances
AWS	**AWS Macie**	Data classification and PII protection	Identifies and protects sensitive customer data

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cloud Provider	Security Tool	Purpose in E-Commerce	Notable Features
Azure	**Microsoft Defender for Cloud**	Unified cloud security posture management	Threat protection, compliance score tracking
Azure	**Azure Key Vault**	Secure key and secret management	Centralized management of encryption keys
Google Cloud	**Security Command Center (SCC)**	Risk analysis and threat visualization	Asset inventory, misconfiguration detection
Google Cloud	**Cloud Identity-Aware Proxy (IAP)**	Identity-based access control to applications	Enforces least privilege and contextual access

5. Regulatory Alignment in E-Commerce Cloud Migration

The cloud migration for these e-commerce firms entails several security considerations and possibilities of legal, operational, or reputational risks. Under the shared responsibility model, there is a necessity for a clear distinction of responsibilities between the cloud providers and the organizations. Compliance packs GDPR, PCI DSS, and U.S. privacy acts such as CCPA/CPRA within it, whereas some data sovereignty laws of countries like India, China, or Brazil demand local storage and processing. International standards like ISO/IEC 27001 and NIST will give the strongest conditions. Recommended practices include creating audit trails, breach notifications, and continuous monitoring using cloud-native tools. Table 2 previews the key frameworks with their implications.

Table 2: Regulatory Requirements in E-Commerce Cloud Migration

Framework / Regulation	Scope & Applicability	Key Requirements	E-Commerce Cloud Implications	References
GDPR (EU)	Applies to organizations handling EU citizens' data	Data portability, erasure, explicit consent, 72-hour breach notification, restrictions on third-country transfers	Enforce encryption, consent management, and DPIAs, and ensure CSPs support GDPR-ready services	[1][2][3][4]
PCI DSS	Global standard for payment card data	Secure cardholder data storage, transmission, access control, network segmentation, and audit logging	Tight IAM, micro-segmentation, encryption, shared responsibility with CSPs, regular audits	[5][6][7]

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CCPA / CPRA (U.S.)	Consumer data protection laws in California	Transparency, opt-outs, right to know/delete, restrictions on data sale	Configure consent management, enforce ABAC/RBAC, and adjust services for consumer data rights	[8][9]
Data Sovereignty Laws (India, China, Brazil, etc.)	Mandates local storage/processing of citizen data	Geo-fencing, regional cloud deployment, and restricted cross-border transfer	Regional data center selection, compliance-driven CSP choice, localized backups	[10][11]
ISO/IEC 27001	International ISMS standard	Establishing security controls, vendor risk management, and audit readiness	Helps standardize compliance practices, improves regulatory preparedness	[12][13]
NIST SP 800-53 & 800-171	U.S.-centric but globally referenced frameworks	Control baselines for cloud security, incident response, and access control	Adoptable by private e-commerce firms for structured security implementation	[14][15]
Breach Notification Laws	Vary by jurisdiction (e.g., GDPR's 72-hour rule)	Timely reporting, incident response protocols	Cloud-native alerting, jurisdiction-specific response plans	[18][19]
Operational Tools & CASBs	Cloud-native compliance enforcement	Centralized logging, audit trails, shadow IT detection, and continuous monitoring	Use AWS Config, Azure Policy, Google Compliance Reports, and CASBs for enforcement	[16][17][20] [21][22][23]

5.1 Cloud Migration Methodologies for E-Commerce

Before examining case-specific approaches, it is essential to understand the principal methodologies available for migrating e-commerce systems to the cloud. The choice of method depends on several factors, including system

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

complexity, desired modernization level, budget, and regulatory requirements. Each methodology offers a different balance between speed, cost, and long-term flexibility.

Table 3: Migration Methodologies Explained

Method	Description	Pros	Cons
Lift and Shift	Move the existing application (ATG or similar platforms) to the cloud with minimal or no modification.	Quick transition, minimal disruption.	Limited optimization; may not leverage cloud-native features.
Re-platforming	Make selective upgrades (e.g., operating system or database modernization) while migrating.	Balances migration speed with efficiency and modest modernization.	Some limited rework and testing are required.
Incremental / Strangler	Gradually migrate services through an API gateway or intermediary layer, replacing legacy components over time.	Reduced downtime and better risk management.	Requires API synchronization and detailed migration planning.
Full Re-architecture	Redesign the system into cloud-native microservices or MACH (Microservices, API-first, Cloud-native, Headless) architecture.	Maximizes scalability, agility, and future-proofing.	Highest complexity and longest implementation time.

These methodologies enable e-commerce organizations to align their migration strategy with both business objectives and compliance priorities. While Lift and Shift approaches are suitable for rapid cloud adoption with minimal upfront cost, they often fail to utilize advanced cloud capabilities. Re-platforming represents a balanced path, introducing partial modernization while maintaining operational stability. Incremental or Strangler strategies are ideal when downtime must be minimized, enabling controlled migration of components while maintaining existing services. Finally, full re-architecture, though time-consuming, is the most transformative, offering scalability, resilience, and integration with modern frameworks such as microservices and serverless functions. Selecting the right methodology requires evaluating not only technical readiness but also governance maturity and the capacity to maintain compliance throughout the migration lifecycle. This structured understanding provides the foundation for the case studies that follow, which illustrate how organizations have applied these methodologies in real-world e-commerce contexts.

6. Case Studies

Having established the foundational concepts of secure cloud migration, real-world cases offer practical insight into how e-commerce businesses are implementing these strategies. These examples illustrate the diverse approaches, challenges, and solutions applied across varying organizational sizes and technological maturity. One notable case involves a mid-sized e-commerce firm transitioning from a legacy on-premise monolith to a cloud-native microservices architecture. Adopting a phased migration strategy, the company started with non-sensitive components before moving to critical data systems. By using Kubernetes and containerization, they achieved workload isolation and improved compliance, enforcing encryption with customer-managed keys and aligning early with GDPR through DPIAs and strict API access controls [1][12].

Hybrid cloud environments are increasingly being used to support secure and compliant operations across various industries. For example, a global fashion retailer may choose to host customer-facing applications in the public cloud to

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

enhance scalability and performance, while retaining its enterprise resource planning (ERP) system on-premises for greater control and data governance. In such scenarios, Virtual Private Networks (VPNs) are used to establish secure connections between cloud and on-premise systems. Additionally, the organization may implement security frameworks such as the NIST Special Publication 800-53 controls to ensure compliance with cybersecurity best practices. A Cloud Access Security Broker (CASB) can also be deployed to enforce unified security policies and manage GDPR-related consent across both cloud and local environments [3][4]. A grocery delivery startup leverages FaaS serverless scalability with identity federation, SIEM logging, PCI DSS compliance, tokenization, and workload isolation [5][6]. An international e-commerce firm's Cloud Center of Excellence governs large-scale migration, using compliance-as-code via ISO 27001 and SOC 2 templates [7][8]. Key lessons are integrating security from the outset, automating compliance, and training teams, supported by CI/CD scanning tools, compliance dashboards, and identity platforms [9][10].

7. Recommendations and Future Directions

The secure and certified cloud migration in e-commerce is an ongoing, multi-tier endeavor requiring technical, organizational, and legal orchestration to achieve regulatory compliance and operational long-term security. Therefore, security and compliance have to be embedded all through from its inception, starting with the identification of regulated data, such as data regulated under GDPR or PCI DSS, through to the application of controls like encryption and auditability, and consent management [1][2]. It is advisable to adopt a phased, risk-based migration approach, starting with low-risk workloads so that teams may gain experience before transitioning to sensitive systems, with security and compliance validations in place throughout [3][4]. Centralized governance frameworks based on NIST or ISO/IEC 27001 provide guidelines for access control, patches, monitoring, and encryption to be implemented by AWS Organizations or Azure Policy [5][6]. In this regard, strong identity and access management (IAM) practices, including RBAC/ABAC, credential protection, use of multi-factor authentication, and continuous monitoring, should be established to eliminate the risk of unauthorized access [7][8].

Security is embedded into DevSecOps pipelines to find vulnerabilities via static code analysis and automated compliance-as-code frameworks using OPA or AWS Config Rules [9][12]. The e-commerce system proceeds with cloud-native incident response and disaster recovery with centralized logging, real-time alerting, and backup validation exercises and tests performed by red-team and tabletop drills [13][14]. Employing cloud-native security platforms such as AWS GuardDuty, Azure Defender, and GCP Security Command Center helps enhance threat detection, operational visibility, and regulatory alignment [15][16]. Organizational alignment is vital for effective cloud adoption, and Cloud Centers of Excellence (CCoE) play a central role in this process. They guide cloud strategy, enforce policy, and deliver organizational training [17][18]. At the same time, emerging technologies are enhancing cloud resilience. Confidential computing allows data to be processed securely in encrypted form, AI-based fraud detection strengthens threat response, and post-quantum cryptography prepares infrastructure for future quantum-era risks [23][26].

Table 3: Comparison of Key Data Compliance Frameworks

Regulation	Jurisdiction	Key Data Rights	Enforcement Penalties	Data Localization Requirement
GDPR	European Union	Right to access, erasure, and portability	Up to €20 million or 4% of global turnover	Conditional (adequacy decisions, SCCs)
CCPA/CPRA	California, USA	Opt-out of sale, data deletion rights	$2,500–$7,500 per violation	No, but limitations on third-party sharing
LGPD	Brazil	Consent, data correction, transparency	Up to 2% of revenue or BRL 50 million cap	No mandatory localization
PDPB (India)	India (pending)	Consent, data minimization	Up to ₹250 crore (approx. $30 million)	Yes (for critical/sensitive data)

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Regulation	Jurisdiction	Key Data Rights	Enforcement Penalties	Data Localization Requirement
PCI DSS	Global (industry)	Cardholder data protection	Fines, audit failures, and merchant blacklisting	Not tied to geography, but to systems

8. Conclusion

E-commerce cloud migration goes beyond mere technology change; it needs a secure, compliant, and customer-driven approach. Yet, there is literature available on the problems and solutions of migrating e-commerce systems, emphasizing how security and compliance need to be embedded throughout the lifecycle. Effective risk mitigation in cloud environments involves implementing Zero Trust Architecture, encryption, Identity and Access Management (IAM), and Infrastructure as Code (IaC). These are supported by Compliance-as-Code, continuous monitoring, and DevSecOps practices. Together, these measures ensure alignment with regulatory standards such as GDPR, PCI DSS, CCPA, and ISO 27001. Through case studies, it was demonstrated how, through automation, governance, and training, startups and multinationals performed secure migrations. Human factors and especially cross-functional collaboration with Cloud Center of Excellence (CCoE) practices emerged as important enablers for success. On the horizon are confidential computing, AI-powered compliance, and post-quantum cryptography as paradigms of future security, accompanied by new regulations such as DSA and DMA. Nevertheless, cloud migration is a continuous journey requiring foresight coupled with technical rigor and dispositions to adapt emerging e-commerce landscape.

Reference

[1] Gorelik, E. (2013). *Cloud computing models* (Doctoral dissertation, Massachusetts Institute of Technology).
[2] Duncan, B. (2018). Can the EU General Data Protection Regulation compliance be achieved when using cloud computing?. *Cloud computing*, *2018*, 11.
[3] Balalaie, A., Heydarnoori, A., Jamshidi, P., Tamburri, D. A., & Lynn, T. (2018). Microservices migration patterns. *Software: Practice and Experience*, *48*(11), 2019-2042.
[4] Parvatha, N. (2021). Resilient cybersecurity frameworks for multi-cloud environment: Innovations in securing distributed systems against emerging threats. *International Journal of Science and Research Archive*, *3*(1), 266-275.
[5] Cameron, A., & Williamson, G. (2020). Introduction to IAM Architecture (v2). *IDPro Body of Knowledge*, *1*(6).
[6] Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and software technology*, *141*, 106700.
[7] Olajide, P. (2013). PCI DSS compliance validation of different levels of merchants in a multi-tenant private cloud.
[8] Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3-4), 40-71.
[9] Aldawsari, H., & Kouchay, S. A. (2023). Integrating AI and Machine Learning Algorithms in Cloud Security Frameworks for Enhanced Proactive Threat Detection and Mitigation. *Journal of Emerging Threat Management*.
[10] Sardar, M. U., & Fetzer, C. (2023). Confidential computing and related technologies: a critical review. *Cybersecurity*, *6*(1), 10.
[11] Gopireddy, S. R. (2020). Automated Compliance as Code for Multi-Jurisdictional Cloud Deployments. *European Journal of Advances in Engineering and Technology*, *7*(11), 104-108.
[12] Marin, E., Perino, D., & Di Pietro, R. (2022). Serverless computing: a security perspective. *Journal of Cloud Computing*, *11*(1), 69.
[13] Fitria, N. (2021). Comparing Software-Defined Perimeter and Zero-Trust Architectures for Secure, Cloud-Native Online Retail Infrastructures. *International Journal of Applied Business Intelligence*, *1*(12), 12-22.
[14] Harishchandra Patel Impedance Control in HDI and Substrate-Like PCBs for AI Hardware Applications. (2024). Journal of Electrical Systems, 20(11s), 5109-5115.
[15] Raghava-Raju, A. (2017). Predicting Fraud in Electronic Commerce: Fraud Detection Techniques in E-Commerce. *International Journal of Computer Applications*, *171*(2), 18-22.

Journal of Information Systems Engineering and Management
2024, 9(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[16] Spanaki, K., Gürgüç, Z., Mulligan, C., & Lupu, E. (2019). Organizational cloud security and control: a proactive approach. *Information Technology & People*, *32*(3), 516-537.
[17] Rong, C., Geng, J., Hacker, T. J., Bryhni, H., & Jaatun, M. G. (2022). OpenIaC: open infrastructure as code-the network is my computer. *Journal of Cloud Computing*, *11*(1), 12.
[18] Cheikhrouhou, O., Koubâa, A., & Zarrad, A. (2020). A cloud-based disaster management system. *Journal of sensor and actuator networks*, *9*(1), 6.
[19] Alharthi, D. N. (2023, March). Secure cloud migration strategy (SCMS): A safe journey to the cloud. In *International Conference on Cyber Warfare and Security* (pp. 1-6). Academic Conferences International Limited.
[20] Oduri, S. (2021). AI-Powered threat detection in cloud environments. *International Journal on Recent and Innovation Trends in Computing and Communication*, *9*(12), 57-62.
[21] Hesamifard, E., Takabi, H., Ghasemi, M., & Jones, C. (2017, November). Privacy-preserving machine learning in cloud. In *Proceedings of the 2017 on cloud computing security workshop* (pp. 39-43).
[22] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237-243.
[23] Jacob, I., Lawson, R., & Smith, R. (2021). Future-Proofing AI and Cloud Systems: The Intersection of Quantum and Cybersecurity.
[24] Montagnani, M. L., & Cavallo, M. (2021). Liability and emerging digital technologies: an EU perspective. *Notre Dame J. Int'l Comp. L.*, *11*, 208.
[25] Akram, E., & Basit, F. (2023). AI-Powered Information Security: Innovations in Cyber Defense for Cloud and Network Infrastructure.
[26] Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys (CSUR)*, *46*(1), 1-30.
[27] Enjam, G. R. (2023). AI Governance in Regulated Cloud-Native Insurance Platforms. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 102-111.