Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Cloud Security Challenges in Saudi E-commerce Platforms under Vision 2030

Salem Ba Abdullah
Master of Science in Information and Communication Technology, MEDIU, Malaysia
Corresponding Author: Salem Ba Abdullah, **E-mail**: sbaabdullah86@gmail.com

| ABSTRACT

Saudi Arabia's e-commerce sector has become one of the most rapidly expanding digital markets in the Middle East, propelled by the Kingdom's Vision 2030 agenda, high internet penetration, and a young, digitally engaged population. As e-commerce operators accelerate their migration to cloud-based infrastructure, they face a sophisticated and intensifying security landscape that threatens both operational continuity and the trust of millions of consumers. This study investigates the principal cloud security challenges confronting Saudi e-commerce platforms operating within the Vision 2030 context. Drawing on a systematic review of academic literature, industry and market research reports, and primary regulatory documents — including Saudi Arabia's Personal Data Protection Law (PDPL) and the National Cybersecurity Authority (NCA) cloud security frameworks — the study identifies and analyses seven distinct challenge domains: cloud misconfiguration and the shared responsibility gap; identity and access management weaknesses; regulatory compliance and data localization complexity; ransomware and distributed denial-of-service threats; third-party and supply chain risk; cybersecurity talent scarcity; and insider threats. The findings reveal a structural misalignment between the pace of cloud adoption and the maturity of security governance among Saudi e-commerce operators, particularly small and medium-sized enterprises. The paper concludes with evidence-based recommendations for platform operators, regulators, and policymakers to bridge this gap and build a cloud security posture commensurate with Vision 2030's ambitions for a trusted, resilient digital economy.

| KEYWORDS

Cloud Security, Saudi E-commerce, Vision 2030, PDPL, NCA, Cybersecurity, Data Sovereignty, Shared Responsibility Model, Digital Transformation

| ARTICLE INFORMATION

ACCEPTED: 01 June 2026 **PUBLISHED:** 13 July 2026 **DOI:** 10.32996/jcsts.2026.8.8.10

1. Introduction

The Kingdom of Saudi Arabia is undergoing one of the most consequential digital transformations in its modern history. Guided by Vision 2030, the Kingdom has committed to building a globally competitive, knowledge-driven digital economy, reducing dependence on hydrocarbon revenues, and positioning technology, e-commerce, and artificial intelligence as primary drivers of economic diversification and growth. This transformation has fundamentally reshaped how Saudi businesses operate, how consumers transact, and how digital infrastructure is conceptualized, financed, and governed.

At the center of this transformation is the e-commerce sector. Saudi Arabia's digital retail market was valued at approximately $5.15 billion in 2023, representing 6% of the Kingdom's $92.6 billion retail economy (Statista, 2024). Projections by global consultancy Deloitte estimate that the sector will reach $23.46 billion in market volume by 2027, supported by an anticipated 34.5 million e-commerce users by 2025. User penetration is expected to rise from 66.7% in 2023 to 74.7% by 2027, reflecting the Kingdom's exceptionally high smartphone adoption rates and rapidly expanding logistics infrastructure. Digital payments have grown in lockstep: the share of electronic transactions in retail exceeded 57% in 2021, placing the Kingdom well on its way to the Vision 2030 target of 70% cashless retail transactions by 2030.

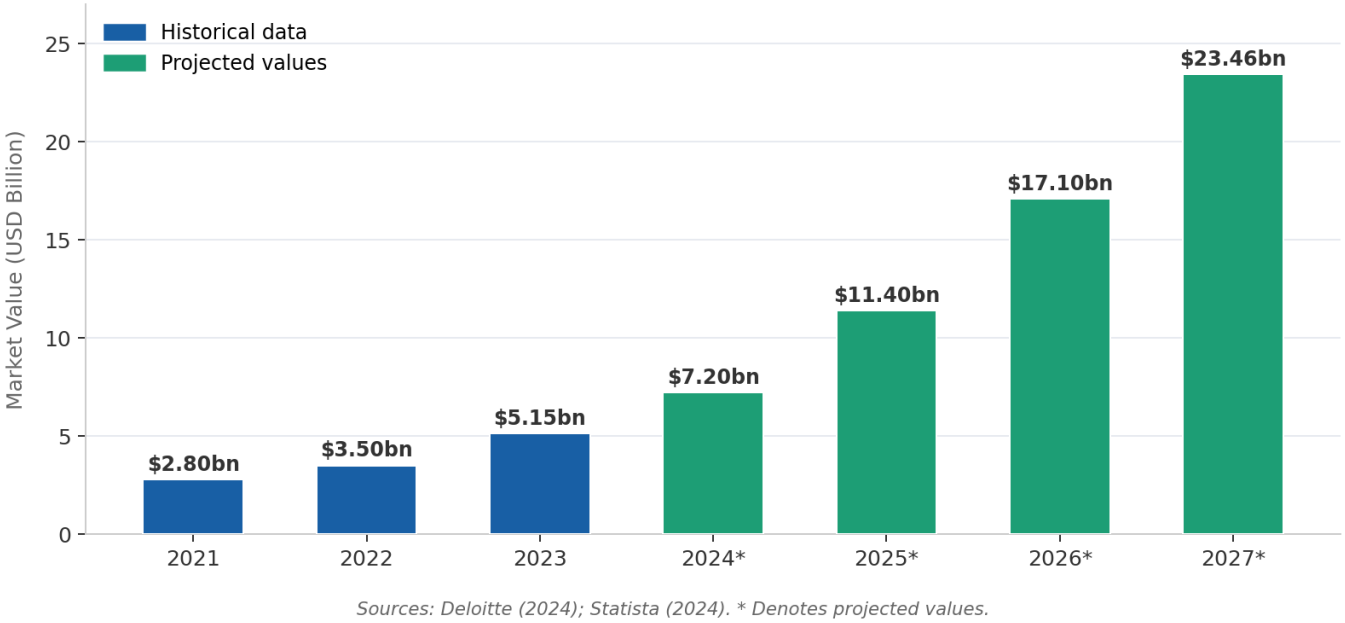

Figure 1: Saudi Arabia E-commerce Market Size, 2021–2027 (USD Billion)
Sources: Deloitte (2024); Statista (2024). Values for 2025–2027 are projections.

Cloud computing is the foundational layer upon which this e-commerce expansion rests. Saudi Arabia's annual spending on public cloud services surpassed $2.4 billion in 2024 and is forecast to reach $4.7 billion by 2027, at a compound annual growth rate of 25% (IDC, 2024). The Saudi government formalized its commitment to cloud infrastructure through the Cloud First Policy of 2019, which mandated that all government entities prioritize cloud-based solutions in their IT procurement. A Cloud Computing Special Economic Zone, launched in 2023, further institutionalized this direction and signaled the Kingdom's intent to attract hyperscale cloud providers to establish local infrastructure. Microsoft's Saudi Arabia datacenter region is expected to become operational in the fourth quarter of 2026, joining Google Cloud and STC Cloud among locally available hyperscaler options — a development with significant implications for data residency compliance.

Yet the pace and ambition of cloud adoption have introduced security challenges of commensurate scale and complexity. Cyber threats targeting Saudi digital infrastructure have intensified considerably. The cost of a cyberattack on a Saudi organization exceeds the global average by 69% (ResearchAndMarkets, 2025), and e-commerce platforms — which sit at the intersection of financial transactions, personal data repositories, and consumer trust — are among the most attractive and vulnerable targets for both financially motivated cybercriminals and state-affiliated advanced persistent threat actors. The Kingdom's cybersecurity market reached SAR 15.2 billion (approximately $4.05 billion) in 2024, growing at 14% year-over-year, reflecting the scale of investment required to meet this threat (NCA, 2025).

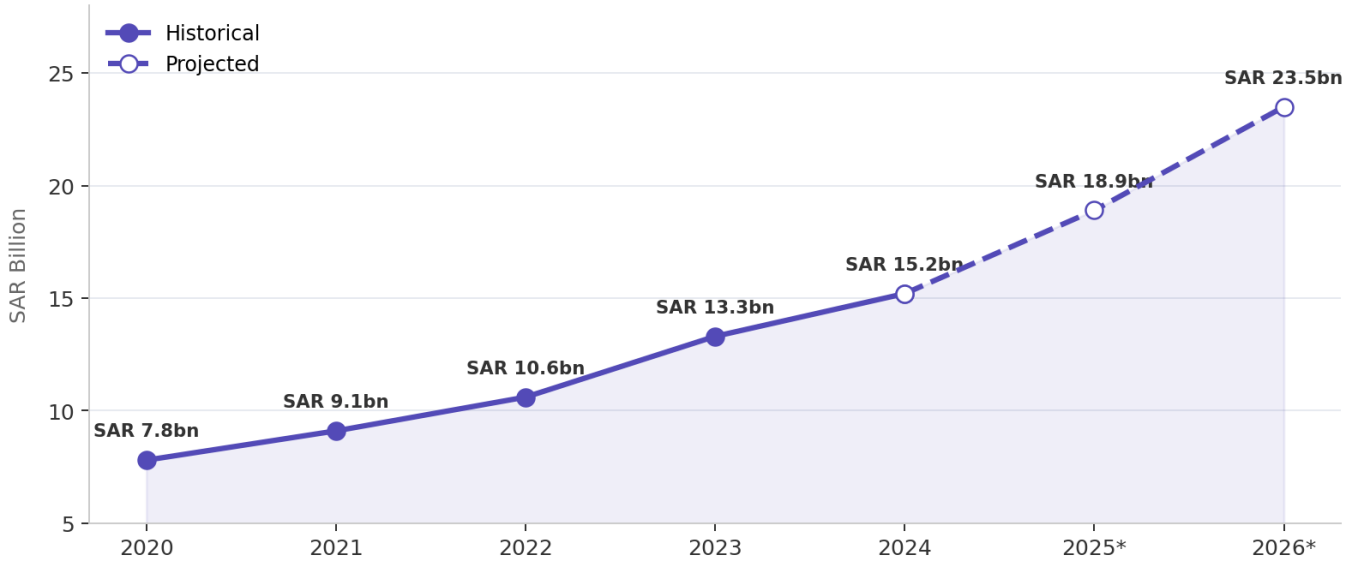

Figure 2: Saudi Arabia Cybersecurity Market Value, 2020–2026 (SAR Billion)
Sources: NCA (2025); Ken Research (2025); MarkSpark Solutions (2024).

Despite Saudi Arabia's notable national-level achievements in cybersecurity — including its ranking as second globally in the International Telecommunication Union's Global Cybersecurity Index (ITU, 2024) — the translation of that national ambition into platform-level security maturity among individual e-commerce operators remains uneven and, in many cases, inadequate. This paper investigates the specific cloud security challenges that define this gap, the regulatory and organizational factors that shape them, and the strategic responses required to close them within the Vision 2030 timeline.

2. Problem Statement

The central problem this study addresses is a structural misalignment between the pace and scale of cloud adoption in Saudi Arabia's e-commerce sector and the maturity of the cloud security frameworks that individual operators have deployed to protect the data, transactions, and digital assets they are entrusted to safeguard.

This misalignment has several dimensions. First, cloud adoption has in many cases been driven by commercial imperative — the need for scalability, cost reduction, and speed to market — rather than by a security-informed architecture strategy. Many e-commerce platforms, particularly small and medium-sized enterprises (SMEs), have migrated workloads to cloud environments without equivalent investment in the security controls, monitoring capabilities, and incident response procedures necessary to protect those environments. Alamri and Alzahrani (2024), in their peer-reviewed study of cloud computing adoption by Saudi SMEs in the e-commerce sector, documented significant gaps in security awareness, technical capability, and organizational readiness — and noted that "existing literature indicates significant gaps, including a general lack of comprehensive research focused on cloud computing adoption for SMEs and very limited research on the Kingdom of Saudi Arabia context."

Second, the regulatory environment governing cloud security in Saudi e-commerce has become substantially more demanding since 2021, creating new compliance obligations that many operators are not yet equipped to meet. The full enforcement of the Personal Data Protection Law (PDPL) on 14 September 2024, the concurrent strengthening of the National Cybersecurity Authority's cloud security controls, and the layered obligations imposed by the SAMA Cybersecurity Framework for payment-processing entities have collectively created a compliance landscape of considerable complexity. Non-compliance exposes operators to fines of and reputational damage that can be existential for smaller operators.

Third, the global cloud threat landscape has deteriorated sharply. Cloud intrusions rose 37% year-over-year in 2025 (CrowdStrike, 2025), ransomware incidents surged 126% in the first quarter of 2025 alone, and API exploitation now accounts for 31% of all cloud data breaches globally (SentinelOne, 2025). These trends affect Saudi e-commerce platforms directly, and the Kingdom's elevated threat profile — reflecting its economic significance, geopolitical position, and rapidly expanding digital footprint — amplifies the risk further.

The problem is therefore not merely technical but strategic: Saudi e-commerce operators are deploying increasingly powerful cloud infrastructure in an increasingly dangerous security environment, while the governance frameworks, technical capabilities, and human expertise needed to secure that infrastructure lag significantly behind. Under Vision 2030's ambitions for a trusted, competitive digital economy, this gap constitutes a material risk not only to individual platforms but to the broader national digital transformation agenda.

3. Research Questions

This study is structured around the following primary and secondary research questions:

RQ1: What are the principal cloud security challenges confronting Saudi e-commerce platforms operating within the Vision 2030 context, and how do they differ across operator types and scales?

RQ2: How does Saudi Arabia's regulatory framework — in particular the PDPL, NCA Cloud Cybersecurity Controls, and SAMA Cybersecurity Framework — shape the cloud security compliance obligations of e-commerce operators, and where do significant implementation gaps or regulatory tensions exist?

RQ3: To what extent does the shared responsibility model of cloud computing create organizational security gaps among Saudi e-commerce operators, and how are these gaps manifested in documented breach patterns and incident statistics?

RQ4: What strategic, technical, and organizational interventions are most effective in strengthening cloud security posture for Saudi e-commerce platforms, and how should these interventions be prioritized given the resource constraints of SME operators?

4. Study Objectives

The study pursues the following specific objectives:

1. To identify and classify the primary cloud security threat vectors affecting Saudi e-commerce platforms, drawing on both global empirical data and Saudi-specific evidence.
2. To examine the regulatory and compliance landscape governing cloud security in Saudi e-commerce under Vision 2030, including obligations arising from the PDPL, NCA frameworks, and sectoral regulations.
3. To analyze the organizational dimensions of cloud security challenges, encompassing the cybersecurity talent gap, shared responsibility misunderstandings, and third-party risk exposure.
4. To synthesize findings from across the academic and industry literature into a coherent, structured framework of cloud security challenges specific to the Saudi e-commerce context.
5. To formulate evidence-based recommendations for e-commerce operators, regulators, and national policymakers to address identified challenges in alignment with Vision 2030 objectives.

5. Study Significance

This study makes contributions at multiple levels that distinguish it from prior work in the field.

Academic contribution: The study addresses a demonstrably understudied intersection of topics. As Alamri and Alzahrani (2024) confirmed in their published review, comprehensive academic research on cloud security in the Saudi e-commerce sector is sparse, with existing literature focused predominantly on adoption patterns rather than security-specific challenges and governance frameworks. This paper provides a structured analysis of the security dimension, offering a foundation for future empirical research.

Practical contribution: The study provides Saudi e-commerce operators — from large multi-category platforms to SME merchants — with a structured, evidence-grounded understanding of the specific cloud security challenges they face and actionable guidance for addressing them. At a time when PDPL enforcement is active and NCA scrutiny of cloud practices is intensifying, this guidance carries immediate commercial relevance. Operators that fail to address these challenges face regulatory penalties, operational disruptions, and loss of consumer trust.

Policy contribution: The study informs regulatory design and national cybersecurity strategy at a moment when both the PDPL implementing framework and the NCA's cloud security controls are likely to undergo revision. Research that maps the on-the-ground challenges of e-commerce operators provides essential grounding for evidence-based policymaking, helping regulators distinguish between aspirational standards and practically achievable compliance targets.

Social and economic contribution: E-commerce platforms are trusted custodians of the personal, financial, and behavioral data of tens of millions of Saudi consumers. Strengthening cloud security in this sector is a matter of public interest that extends well beyond the commercial concerns of individual operators. It underpins consumer confidence in the digital economy, protects citizens from fraud and identity theft, and supports the broader Vision 2030 goal of an inclusive, trusted digital society.

6. Limitations of the Study

This study is subject to a number of limitations that must be considered when interpreting and applying its findings.

Methodological scope: As a systematic literature review and qualitative secondary data analysis, this study does not draw on primary data collected directly from Saudi e-commerce operators, security practitioners, or regulators. The lived experiences, contextual judgments, and operational constraints of those working within specific platform environments are therefore not directly captured. Future research should complement these findings with quantitative surveys measuring security posture across operator segments, and qualitative case studies of specific breach incidents and remediation experiences.

Temporal dynamics: The cloud security landscape, the threat environment, and the regulatory framework in Saudi Arabia are all evolving rapidly. Data, statistics, and regulatory provisions cited in this study reflect the best available evidence as of April 2026 but will require periodic revision. In particular, the expected launch of Microsoft's Saudi datacenter region in Q4 2026 and anticipated updates to PDPL implementing regulations may alter the data residency and compliance dynamics described herein.

Sector heterogeneity: Saudi e-commerce encompasses operators of vastly different scales and sophistication — from Noon and Amazon.sa operating large, technically capable platforms, to hundreds of thousands of SMEs and micro-merchants transacting primarily through social commerce channels. Cloud security challenges differ substantially across these segments. This study addresses challenges common to the sector as a whole, and its findings may not accurately represent the experience of any particular subsegment.

Data availability: Granular empirical data on cloud security incidents affecting Saudi e-commerce platforms specifically is limited. Organizations are understandably reluctant to disclose breach details, and Saudi-specific incident classification data at the sector level is not publicly available from the NCA or other authorities. This study relies on regional and global proxy data where Saudi-specific evidence is unavailable, which may introduce imprecision in magnitude estimates.

Literature gap: The thinness of Saudi-specific academic literature in this domain, acknowledged by prior researchers, means this study draws substantially on industry reports and regulatory documents rather than peer-reviewed empirical findings specific to the Saudi e-commerce cloud security context. The quality and rigor of industry research varies, and the findings of commercial research houses may reflect commercial interests.

7. Literature Review

7.1 Cloud Computing in E-commerce: Foundational Concepts

Cloud computing has restructured the technical and economic foundations of e-commerce since the mid-2000s. Buyya et al. (2009) established the canonical definition of cloud computing as the delivery of computing as a metered, on-demand utility — a model that enables the scalability, flexibility, and cost efficiency that modern e-commerce requires. Subsequent scholarship by Zhang et al. (2010) documented the rapid evolution of cloud deployment models and their growing relevance to commercial digital operations. Al-Jaberi, Mohamed, and Al-Jaroodi (2015) addressed the specific intersection of cloud computing and e-commerce directly, cataloguing both the operational benefits and the security and governance challenges that cloud adoption introduces into digital commerce environments.

The security challenges associated with cloud adoption in e-commerce have been a consistent theme in the literature. Rad, Diaby, and Rana (2017), in a targeted review of cloud adoption barriers, found that security and data privacy concerns were the most frequently cited obstacles across organizational contexts. Badotra and Sundas (2021) extended this analysis with a systematic review of e-commerce system security, identifying authentication weaknesses, insecure API implementations, and misconfigured access control systems as the dominant vulnerability categories. These findings have been consistently reinforced by practitioner research: by 2026, approximately 82% of all data breaches involve cloud-stored data (SentinelOne, 2025), and cloud intrusions have accelerated for three consecutive years.

7.2 The Shared Responsibility Model

A foundational concept in cloud security that recurs throughout both academic and practitioner literature is the shared responsibility model — the contractual and technical division of security obligations between cloud service providers (CSPs) and their customers. Cloud providers secure the underlying physical and virtual infrastructure; customers are responsible for securing everything deployed on top of it, including application configurations, data, user identities, and access controls.

Trend Micro (2021) documented empirically how this model is consistently misunderstood, with customers systematically underestimating the scope of their own security responsibilities. Gartner's widely cited projection — that 99% of cloud security failures will be the customer's fault, primarily due to misconfigurations and inadequate security implementations — is now supported by multiple years of breach data. IBM's 2025 Cost of Data Breach Report attributes 26% of all breaches to human error, the category under which most cloud misconfigurations fall. In 2026, misconfigurations account for approximately 23% of all cloud security incidents globally (Exabeam, 2025), and the average time to detect a misconfiguration-driven breach is 186 days, with containment requiring a further 65 days.

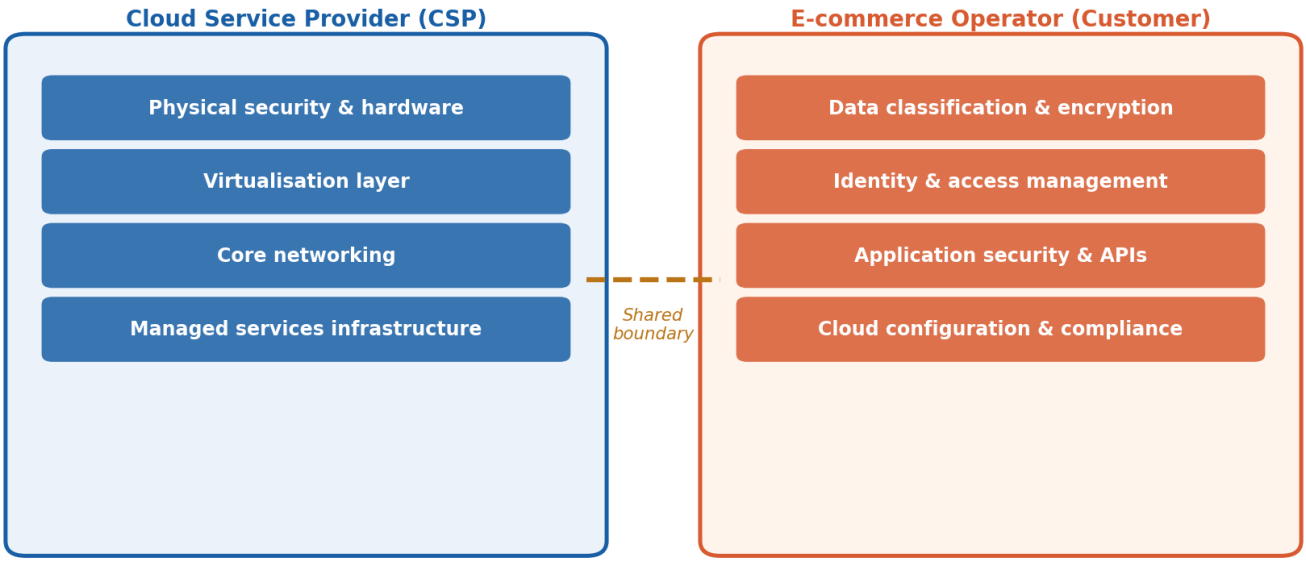

Figure 3: Cloud Shared Responsibility Model — CSP vs. E-commerce Operator Obligations

The shared responsibility gap may be more evident among e-commerce operators in emerging digital economies, where rapid cloud adoption is not always accompanied by corresponding investments in cloud security expertise.

7.3 Cybersecurity in Saudi Arabia: National Context

Saudi Arabia's national cybersecurity posture has attracted considerable academic and policy attention over the past decade. Alelyani and Kumar (2018) provided an early empirical overview of cyberattacks targeting Saudi organizations, documenting the dominance of government, energy, and financial sector targets — a profile that has since expanded to include e-commerce as the sector's economic weight has grown. Alzubaidi (2021) examined cybersecurity awareness levels among Saudi individuals and organizations, finding significant gaps in security knowledge and behavior that create exploitable vulnerabilities at both the consumer and operator levels.

Research published on ResearchGate (2021) analyzing Saudi Arabia's cybersecurity journey from 2017 to 2024 identified the NCA's centralized governance model, substantial investment commitments, and international cooperation frameworks as the primary drivers of the Kingdom's rise to second place globally in the ITU Global Cybersecurity Index. The NCA's Essential Cybersecurity Controls, Cloud Cybersecurity Controls (2020), and Cybersecurity Guidelines for E-Commerce Service Providers (2019) represent the primary regulatory instruments shaping platform-level security obligations in the sector.

Fallatah (2021) examined the adequacy of legal protections for e-commerce transactions in Saudi Arabia, identifying weaknesses in enforcement and implementation that, while focused on a different dimension of governance, reflected a broader pattern of regulatory frameworks outpacing implementation capacity. This observation is directly relevant to the PDPL compliance challenge analyzed in this study.

7.4 Cloud Adoption by Saudi SMEs in E-commerce

The most directly relevant recent academic contribution is that of Alamri and Alzahrani (2024), who employed the Technology-Organization-Environment (TOE) framework to analyze cloud computing adoption by SMEs in Saudi Arabia's e-commerce sector. Published in Engineering, Technology & Applied Science Research (Vol. 14, No. 6), their study found that while cloud adoption was broadly perceived as beneficial, implementation was consistently hampered by limited technical expertise, inadequate security awareness, regulatory complexity, and cost constraints. Their documentation of a significant academic literature gap in this domain provides a key justification for the present study.

Alqahtani, Beloff, and White (2023) proposed a tailored cloud adoption model (ACCM-SME) for the Saudi context, finding that organizational readiness — encompassing management commitment, IT capability maturity, and security governance — was the strongest predictor of both successful adoption and secure cloud operation. Al-Dosari and Fetais (2023) extended this analysis through a meta-study of risk management frameworks for SMEs, confirming that implementation gaps in regulatory compliance were significantly larger in smaller organizations, a finding with direct implications for the e-commerce SME segment.

7.5 Regulatory Frameworks and Data Governance

Saudi Arabia's data governance landscape has undergone a fundamental transformation since 2021. The PDPL, enacted under Royal Decree M/19 and brought to full enforcement in September 2024, introduced the Kingdom's first comprehensive data privacy regulation (CMS Law, 2025; ICLG, 2025). Modeled in part on the EU General Data Protection Regulation (GDPR), the PDPL imposes substantive obligations on all organizations processing the personal data of Saudi residents — including e-commerce platforms of all sizes operating cloud-based services.

Fonseca-Herrera, Rojas, and Florez (2021) examined ISO/IEC 27001-based information security management systems, finding that alignment with international standards provided a robust and portable foundation for meeting regulatory requirements across multiple jurisdictions. For Saudi e-commerce platforms, compliance with both international standards (ISO 27001 for information security management; ISO 27017 for cloud security controls) and Saudi-specific NCA requirements constitutes the baseline of defensible cloud security governance.

SGS (2025), in a comprehensive analysis of cloud security across the Middle East, documented that cloud security now accounts for approximately one-third of total cybersecurity spending in the region, making it the primary security investment priority for many organizations. This investment pattern reflects the combined pressure of regulatory enforcement and escalating threat activity.

8. Methodology

This study employs a **systematic literature review and qualitative secondary data analysis** design, synthesizing evidence across three categories of sources to develop a comprehensive, structured analysis of cloud security challenges in Saudi e-commerce under Vision 2030.

Academic literature was identified through systematic searches of Google Scholar, IEEE Xplore, ResearchGate, and the ICLG database, using the search terms: "cloud security Saudi Arabia," "e-commerce cybersecurity Saudi Arabia," "PDPL cloud compliance," "cloud misconfiguration e-commerce," "NCA cybersecurity controls," "cloud adoption Saudi SME," and related combinations. Inclusion criteria required that sources be published between 2017 and 2026, address cloud security, e-commerce security, or cybersecurity in the Saudi Arabian or GCC context, or provide foundational theoretical contributions to the shared responsibility or cloud adoption literatures. Sources older than 2017 were included only where they provided foundational conceptual contributions that have not been superseded.

Industry and market research reports were obtained from IDC, Gartner, CrowdStrike, SentinelOne, IBM Security, Fortinet, MarkSpark Solutions, Ken Research, Grand View Research, ResearchAndMarkets, the SGS Group, and the World Economic Forum. These sources provided quantitative data on cloud security incident rates, breach costs, market size, talent availability, and organizational security posture metrics, which were used to ground the analysis in empirical reality where academic primary data was absent.

Regulatory and policy documents consulted include the Saudi Personal Data Protection Law (Royal Decree M/19, as amended by M/148), the PDPL Implementing Regulations issued by SDAIA, the NCA Essential Cybersecurity Controls, the NCA Cloud Cybersecurity Controls (2020), the NCA Cybersecurity Guidelines for E-Commerce Service Providers (2019), the SAMA Cybersecurity Framework, and the NCA Key Economic Indicators in the Cybersecurity Sector Report (2025).

Analytical approach: The study employs thematic synthesis across all three source categories. Recurring themes were identified, coded, and organized into a structured framework of seven challenge domains. Where quantitative data from multiple sources addressed the same phenomenon, data triangulation was applied to produce the most defensible empirical estimates. Where Saudi-specific data was absent, regional GCC data and global analogues were used with explicit acknowledgment of their limitations as proxies.

9. Results

9.1 Market Context and the Scale of Cloud Security Risk

The empirical evidence confirms that cloud security risk for Saudi e-commerce operators is material, growing, and disproportionately consequential relative to global benchmarks. Saudi Arabia's cybersecurity market reached SAR 15.2 billion in 2024, growing 14% year-over-year, with the cybersecurity sector's total contribution to GDP — including indirect and induced effects — estimated at SAR 15.6 billion (NCA, 2025). Cloud security is the fastest-growing segment within this market, with a projected CAGR of 14.5% through 2030 (P&S Intelligence, 2024), reflecting both the pace of cloud adoption and the escalating cost of securing cloud environments.

The threat environment is shaped by several converging pressures: cloud intrusions rose 37% globally in 2025 (CrowdStrike, 2025), organizations now face an average of 1,925 cyberattacks per week — a 47% increase since 2024 (SentinelOne, 2025) —

and the average cost of a data breach reached $4.44 million globally. E-commerce platforms, which process continuous high-value financial transactions and store extensive consumer personal data, face particular exposure within this environment.

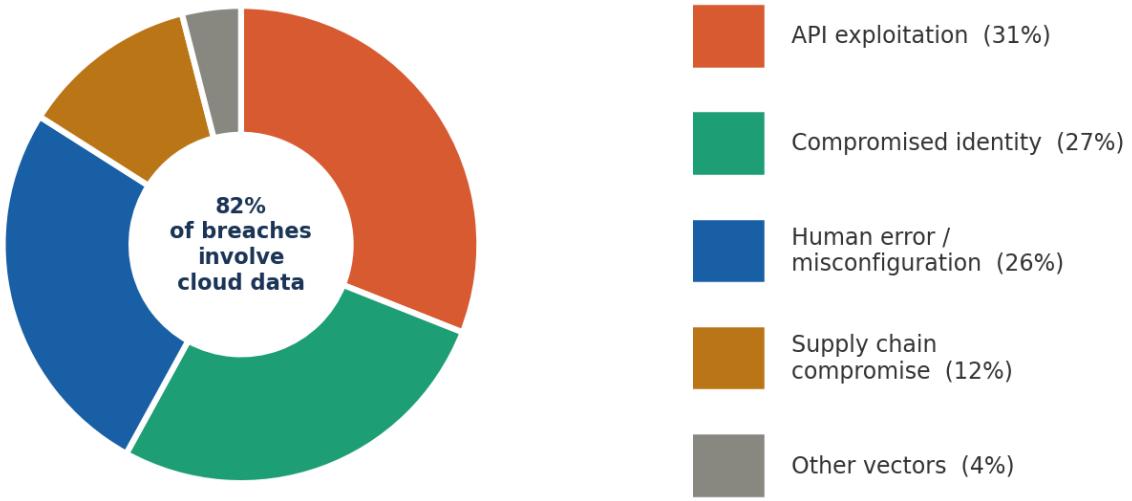

Figure 4: Root Causes of Global Cloud Data Breaches (2025)
Sources: SentinelOne (2025); Exabeam (2025.

9.2 Challenge Domain 1: Cloud Misconfiguration and the Shared Responsibility Gap

The most prevalent and consequential cloud security challenge for Saudi e-commerce platforms is the misconfiguration of cloud environments — the incorrect setting of storage permissions, access control lists, API configurations, database exposure rules, and network security groups. Globally, misconfigurations account for 23% of all cloud security incidents and are present in 15% of all data breaches (Verizon DBIR, 2024). Gartner's projection that 99% of cloud security failures will be attributable to customer error — rather than provider vulnerability — has been borne out by successive breach data cycles.

The root cause is structural. The shared responsibility model assigns security obligations for applications, data, identities, and configurations to the customer, while the cloud provider secures underlying infrastructure. Many Saudi e-commerce operators, particularly SMEs, either misunderstand this division or lack the technical capability to fulfill their obligations under it. The result is preventable exposure: an average of 43 misconfigurations per public cloud account (SentinelOne, 2025), and an average of 186 days to detect a configuration-driven breach before containment begins.

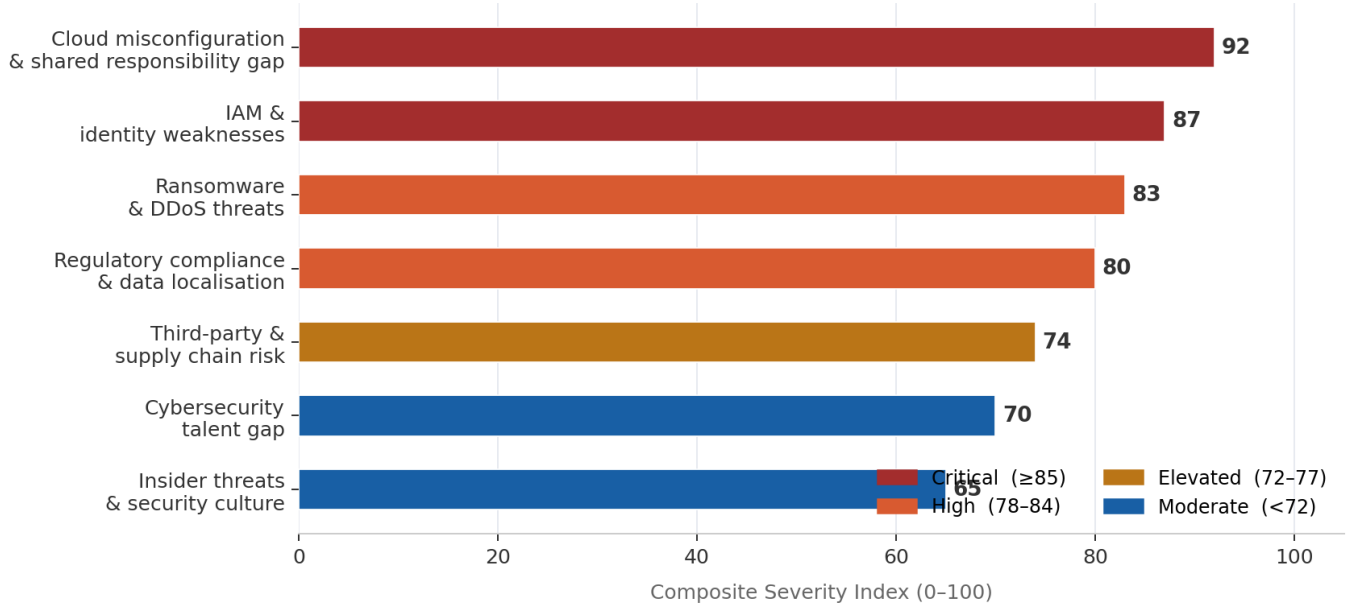

Figure 5: Severity Index of Seven Cloud Security Challenge Domains in Saudi E-commerce Platforms
Composite severity index derived from global breach data (IBM, 2025; SentinelOne, 2025; Verizon DBIR, 2024) weighted against Saudi-specific threat intelligence (NCA, 2025)

For Saudi e-commerce platforms operating across multiple cloud providers — a pattern increasingly common as operators combine AWS, Azure, Google Cloud, and STC Cloud for different functions — the configuration surface multiplies in proportion to cloud diversity, while the expertise required to manage it remains scarce. Organizations that implemented AI-assisted cloud security posture management achieved an average $2.2 million reduction in breach costs compared to those without such tooling (IBM, 2025), illustrating the measurable return on investment available from addressing this challenge.

9.3 Challenge Domain 2: Identity and Access Management Weaknesses

Identity and access management (IAM) represent the second critical challenge domain. Globally, 77% of organizations identify IAM as their primary cloud-native security risk, and 70% of cloud breaches stem from compromised identities (SentinelOne, 2025). Phishing — the exploitation of human factors to steal cloud credentials — was the most prevalent cloud breach vector in 2024, affecting 73% of organizations. In 2025, adversaries have expanded their use of generative AI to create personalized, highly convincing phishing campaigns that defeat standard email filtering, targeting the cloud platform credentials of operations, finance, and development teams.

Saudi e-commerce platforms manage complex identity ecosystems: developers, warehouse and operations staff, marketing teams, finance personnel, third-party logistics providers, and payment processor integrations all require differentiated access to cloud resources. Without strict least-privilege access policies, regular access reviews, and mandatory multi-factor authentication for privileged accounts, over-permissioned accounts accumulate — creating wide lateral movement paths for attackers who succeed in obtaining a single valid credential set.

Middle Eastern organizations report higher-than-average concern about account compromise via phishing and credential theft relative to global peers (SGS, 2025), a finding consistent with the relatively lower maturity of security awareness programs in the region's commercial sector. The NCA's ECC mandates MFA for privileged cloud accounts, but implementation compliance across the e-commerce sector — particularly among smaller operators — remains patchy.

9.4 Challenge Domain 3: Regulatory Compliance and Data Localization Complexity

The regulatory landscape governing cloud security in Saudi e-commerce under Vision 2030 has grown substantially more demanding, creating a complex compliance environment that many operators are ill-prepared to navigate. The PDPL, in full enforcement since September 2024, imposes the following obligations directly relevant to cloud architecture:

Data localization requirements: Transfers of personal data outside the Kingdom are restricted unless the receiving country provides an adequate level of data protection, explicit data subject consent is obtained, or specific approved safeguards — such as standard contractual clauses issued by SDAIA — are in place. For e-commerce platforms relying on global cloud regions for

data processing, this may require significant re-architecture of data flows. SAMA and NCA regulations further mandate that banking and regulated-sector data be resident within the Kingdom, a requirement that constrains the use of non-local cloud regions for payment transaction data.

Security obligations: Article 19 of the PDPL requires controllers to implement appropriate organizational, administrative, and technical security measures for all personal data — including during transfer. This obligation maps directly onto cloud encryption standards, access management requirements, and security monitoring practices. Controllers must adopt cybersecurity standards issued by the NCA, creating an explicit regulatory link between the PDPL and the NCA's cloud security controls.

Breach notification: Organizations are required to notify the NCA of cybersecurity incidents, share threat intelligence, breach indicators, and incident reports. This obligation demands mature Security Operations Center (SOC) capabilities and documented incident response procedures that most Saudi e-commerce SMEs currently lack.

Penalties: Non-compliance carries significant consequences. The PDPL imposes fines of up to SAR 3 million for the unauthorized disclosure of sensitive data, with imprisonment of up to two years possible for serious violations. Violations related to cross-border data transfers may result in fines of approximately USD 267,000, imprisonment for up to one year, or both (CMS Law, 2025).

Achieving coherent compliance across the PDPL, NCA ECC and Cloud Cybersecurity Controls, the Anti-Cyber Crime Law (2007), and — for payment-processing operators — the SAMA Cybersecurity Framework, demands legal counsel, technical expertise, and organizational commitment that the majority of Saudi e-commerce SMEs have not yet mobilized. As compliance professionals have noted, PDPL consent and localization requirements are in several respects stricter than the EU GDPR, meaning GDPR compliance, while a useful foundation, does not guarantee PDPL compliance (upGrowth Digital, 2026).

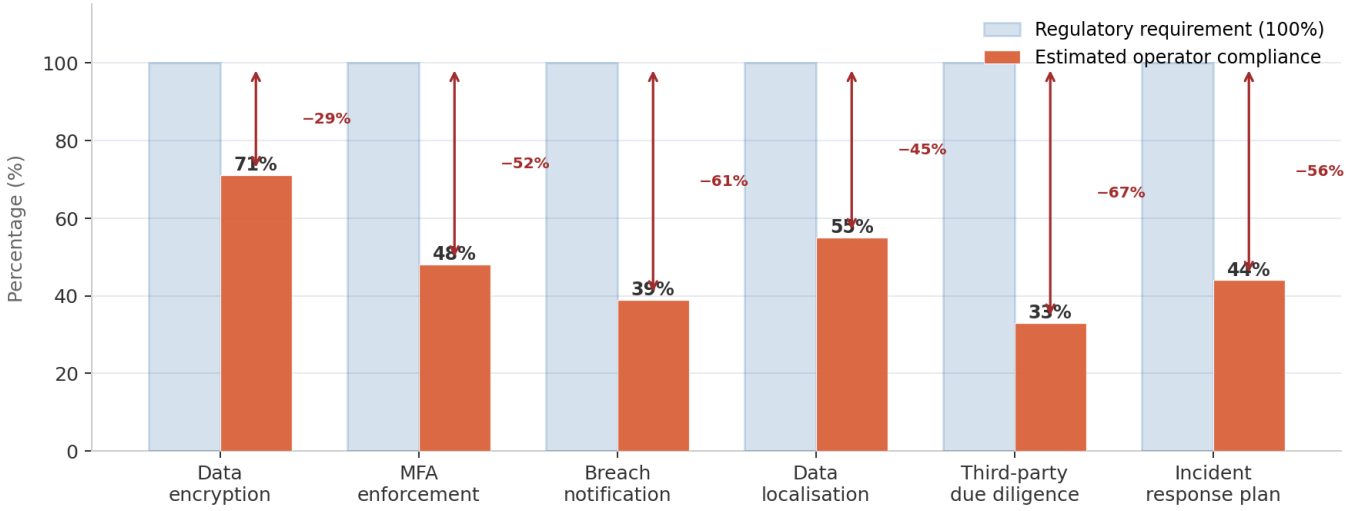

Figure 6: PDPL and NCA Compliance Gap — Saudi E-commerce Operators: Regulatory Requirement vs. Estimated Implementation Rate

Compliance estimates derived from Alamri & Alzahrani (2024); NCA (2025); SGS (2025). Figures represent best-available proxy estimates for the SME segment; large-platform compliance levels are higher.

9.5 Challenge Domain 4: Ransomware, DDoS, and Escalating Threat Activity

Saudi e-commerce platforms face a persistent and elevated threat from ransomware and distributed denial-of-service (DDoS) attacks. Ransomware incidents surged 126% globally in the first quarter of 2025, and 78% of organizations were hit by ransomware in the past year (SentinelOne, 2025). E-commerce platforms — which require continuous service availability to process orders and payments and face acute revenue losses during downtime at peak commercial events such as Ramadan, National Day promotions, and seasonal sales — represent high-value ransomware targets. The incentive to pay ransom demands is structurally strong, which in turn reinforces the attractiveness of e-commerce operators as repeat targets.

DDoS attacks are consistently directed at Saudi e-commerce portals, banking interfaces, and government websites, often during commercially sensitive periods (ITButler, 2025). The GCC region experienced multiple ransomware attacks on logistics networks and commercial infrastructure in 2024 alone, with Saudi operators among the primary targets. The emergence of AI-assisted attack tooling is amplifying these threats: CrowdStrike (2025) documents an 89% year-over-year increase in AI-driven adversary

operations, enabling adversaries to automate credential stuffing, exploit known cloud vulnerabilities at scale, and craft personalized social engineering campaigns with minimal human investment.

Many Saudi e-commerce platforms, particularly those outside the large-platform tier, rely on reactive security postures — responding to attacks after detection rather than maintaining continuous real-time threat monitoring. As ITButler (2025) observes, "By the time they realize they're under attack... the damage is already done." Transitioning from reactive to proactive, intelligence-led security is a critical but resource-intensive requirement.

9.6 Challenge Domain 5: Third-Party and Supply Chain Risk

Modern Saudi e-commerce platforms operate as ecosystems of integrated cloud services rather than monolithic systems. Payment gateways (Mada, Visa, Mastercard, Apple Pay, STC Pay), logistics APIs, marketing analytics platforms, customer relationship management systems, fulfilment management tools, and an expanding suite of cloud-native SaaS applications all interact continuously with core platform infrastructure. Each integration constitutes a potential entry vector for adversaries who cannot breach the primary platform directly.

Globally, 54% of organizations cite the supply chain as a significant barrier to cyber resilience (WEF, 2025), and API exploitation — the primary mechanism of third-party attack — causes 31% of all cloud data breaches (SentinelOne, 2025). For Saudi e-commerce platforms, this challenge is amplified by the rapid adoption of microservices architectures, which distribute security responsibility across dozens of vendors and service providers, creating a governance challenge that is difficult to manage without dedicated third-party risk management programs.

PDPL compliance obligations extend expressly into the third-party domain. Implementing Regulations require e-commerce operators to conduct due diligence on all third-party data processors, assess their compliance with PDPL requirements on an ongoing basis, and maintain comprehensive records of all processing activities throughout the supply chain. This third-party compliance burden is substantial and poorly understood by many operators, particularly those that rely on global SaaS platforms whose PDPL compliance posture has not been independently verified.

9.7 Challenge Domain 6: The Cybersecurity Talent Gap

The talent gap has a pronounced cloud-specific dimension. Multi-cloud security management, cloud-native threat detection, DevSecOps practices, cloud compliance architecture, and Security Operations Center operations all require specialized skills that command premium compensation globally and are in particularly short supply in Saudi Arabia's commercial sector. Globally, 45% of organizations lack qualified staff to manage multi-cloud environments (Exabeam, 2025) — and the problem is more acute in the Saudi e-commerce SME segment, where compensation structures and career development pathways lag those available in the government and financial services sectors.

The Saudi government's commitment of $1.2 billion to train approximately 100,000 cybersecurity professionals, and the 32% female participation rate in the cybersecurity workforce — which exceeds global averages — represent encouraging signals for long-term capacity building (NCA, 2025). However, these programs will not close the gap within the near-term Vision 2030 window. In the interim, e-commerce operators must rely on external managed security service providers, cloud security tooling that automates routine detection and response tasks, and strategic partnerships with regional security specialists.

9.8 Challenge Domain 7: Insider Threats and Security Culture Deficits

The final challenge domain is the human factor internal to the organization. IBM's 2025 Cost of Data Breach Report attributes 26% of breaches to human error — the category covering inadvertent misconfigurations, accidental data exposure, and successful social engineering of internal employees. Saudi businesses face a specific version of this challenge: employees across operations, customer service, marketing, and finance teams increasingly interact directly with cloud platforms, SaaS tools, and data pipelines, expanding the surface area of human error in proportion to cloud adoption.

Insider threats range from malicious actors — employees who steal customer data for financial gain or competitive advantage — to well-intentioned staff who inadvertently expose sensitive information through misconfigured sharing permissions or responses to sophisticated phishing campaigns. In cloud environments, where activity is distributed across dozens of services and platforms, detecting insider anomalies requires behavioral analytics and continuous monitoring capabilities that most Saudi e-commerce operators have not yet deployed.

ITButler (2025) notes that "some of the most damaging breaches occur from malicious or simply careless behavior," and that Saudi businesses face growing challenges from employees falling for phishing scams or misconfiguring systems — a challenge compounded by the rapid pace of cloud tool adoption that outpaces formal training programs. Building a security-aware

organizational culture, in which every employee understands their role in protecting cloud-hosted data, is a necessary but slow-building complement to technical security investments.

10. Conclusion

This study has identified and analyzed seven interconnected cloud security challenge domains confronting Saudi e-commerce platforms operating under Vision 2030: cloud misconfiguration and the shared responsibility gap; identity and access management weaknesses; regulatory compliance and data localization complexity; ransomware and DDoS threats; third-party and supply chain risk; the cybersecurity talent gap; and insider threats and organizational security culture deficits. Together, these challenges constitute a structural security deficit that, if unaddressed, threatens the competitive ambitions of Saudi Arabia's e-commerce sector within the Vision 2030 framework.

The implications of these findings are clear and actionable across three audiences.

For e-commerce operators, the most urgent priorities are: deploying Cloud Security Posture Management (CSPM) tooling to continuously scan for misconfigurations and policy violations; implementing Zero Trust architecture and enforcing multi-factor authentication for all privileged cloud accounts; establishing a structured PDPL compliance program with qualified legal counsel and a Data Protection Officer where required; formalizing third-party risk management processes that include vendor PDPL compliance assessments; and investing in continuous employee security awareness training. Operators that cannot staff these capabilities internally should engage qualified Managed Security Service Providers as an interim measure.

For regulators and policymakers, several interventions would materially reduce the compliance burden and security gap. The NCA and SDAIA should develop implementation guidance specifically tailored to e-commerce SMEs — practical, step-by-step toolkits that translate the principles of the NCA ECC, Cloud Cybersecurity Controls, and PDPL into concrete actions for resource-constrained operators. Regulatory sandbox programs, subsidized security assessments, and compliance self-assessment tools would reduce barriers to compliance for smaller operators. As the Microsoft Saudi datacenter region and other local cloud facilities come online, clear guidance on which data categories satisfy PDPL localization requirements when processed within those facilities will be essential to enabling compliant architecture decisions.

For the academic community, this study has confirmed the thinness of the primary research literature on cloud security in Saudi e-commerce and has proposed a structured framework of seven challenge domains as a foundation for future empirical work. Priority areas for future research include quantitative surveys measuring cloud security posture and PDPL compliance readiness across operator segments; qualitative case studies of incident experiences and remediation strategies; and longitudinal studies tracking security maturity development in relation to Vision 2030 milestones.

Saudi Arabia's ranking as second globally in the ITU's Global Cybersecurity Index is a genuine national achievement and a reflection of the extraordinary investment and governance effort the Kingdom has directed toward cybersecurity since the establishment of the NCA in 2017. Sustaining and extending that achievement, however, requires that the security excellence visible at the national policy level be translated into security maturity at the platform level — where millions of Saudi consumers conduct their digital transactions, share their personal data, and place their trust.

Vision 2030 envisions Saudi Arabia as a leading digital economy — not merely a large one. In a digital economy, trust is the foundational currency. The e-commerce platforms that will define the Kingdom's digital future are not simply those with the largest market shares or the most seamless user experiences. They are those that have earned, protected, and sustained the trust of their customers through rigorous, intelligent, and continuously improving cloud security governance. Achieving that standard is not a compliance exercise. It is a strategic imperative.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflicts of interest.
ORCID ID: https://orcid.org/0009-0002-9217-3429

References

[1] Alamri, N., & Alzahrani, S. (2024). Navigating the clouds: An exploratory research of cloud computing adoption in Saudi Arabia's small and medium enterprises. *Engineering, Technology & Applied Science Research*, 14(6), 17859–17869. https://doi.org/10.48084/etasr.8435

[2] Al-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics*, 12(17), Article 3629. https://doi.org/10.3390/electronics12173629

[3] Aleid, F., Rogerson, S., & Fairweather, B. (2009). Factors affecting consumers' adoption of e-commerce in Saudi Arabia from a consumers' perspective. *Proceedings of the IADIS International Conference e-Commerce*, 11–18. IADIS Press.

[4] Alelyani, S., & Kumar, G. R. H. (2018). Overview of cyberattack on Saudi organizations. *Journal of Information Security and Cybercrimes Research*, 1(1), 32–39. https://doi.org/10.26735/16587790.2018.004

[5] Al-Jaberi, M., Mohamed, N., & Al-Jaroodi, J. (2015). E-commerce cloud: Opportunities and challenges. *International Conference on Industrial Engineering and Operations Management (IEOM)* (pp. 1–6). Dubai, UAE. https://doi.org/10.1109/IEOM.2015.7093867

[6] Alqahtani, M., Beloff, N., & White, M. (2023). A new adoption of cloud computing model for Saudi Arabian SMEs (ACCM-SME). In *Intelligent Systems and Applications* (pp. 192–210). Springer. https://doi.org/10.1007/978-3-031-16072-1_15

[7] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), Article E06016. https://doi.org/10.1016/j.heliyon.2021.e06016

[8] Badotra, S., & Sundas, A. (2021). A systematic review on security of e-commerce systems. *International Journal of Applied Engineering Research*, 16(3), 200–210.

[9] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

[10] CMS Law. (2025). *Data protection and cybersecurity laws in Saudi Arabia*. CMS Expert Guide to Data Protection and Cyber Security Laws. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/saudi-arabia

[11] CrowdStrike. (2025). *2025 global threat report*. CrowdStrike Inc.

[12] Deloitte. (2024). *Saudi Arabia e-commerce market outlook and projections*. Deloitte & Touche Middle East.

[13] Exabeam. (2025). *61 cloud security statistics you must know in 2025*. Exabeam Inc. https://www.exabeam.com/explainers/cloud-security/61-cloud-security-statistics-you-must-know-in-2025/

[14] Fallatah, H. I. (2021). The efficiency of current measures to protect intellectual property rights in e-commerce in Saudi Arabia. *Journal of the Iraqi University*, 50(2), 518–525. https://iasj.net/iasj/article/225048

[15] Fidelis Security. (2025). *Cloud misconfiguration: The #1 cause of data breaches 2025*. https://fidelissecurity.com/threatgeek/threat-detection-response/cloud-misconfigurations-causing-data-breaches/

[16] Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science*, 48(2), 213–222.

[17] Grand View Research. (2025). *Saudi Arabia cybersecurity market size and outlook 2030*. Grand View Research Inc. https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/saudi-arabia

[18] IBM Security. (2025). *Cost of a data breach report 2025*. IBM Corporation.

[19] International Data Corporation (IDC). (2024). *Saudi Arabia cloud computing market data and digital economy forecast*. IDC.

[20] International Telecommunication Union (ITU). (2024). *Global cybersecurity index 2024*. ITU Publications.

[21] International Comparative Legal Guides (ICLG). (2025). *Data protection laws and regulations report 2025–2026: Saudi Arabia*. https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia

[22] ITButler. (2025). *Top 10 cybersecurity threats for Saudi businesses in 2025*. https://itbutler.sa/blog/top-10-cybersecurity-threats-for-saudi-businesses-in-2025/

[23] Ken Research. (2025). *Saudi Arabia cybersecurity market 2019–2030: Size, share, growth, and forecast*. Ken Research Private Limited. https://www.kenresearch.com/saudi-arabia-cybersecurity-and-critical-infra-market

[24] MarkSpark Solutions. (2024). *Saudi Arabia cyber security market: Size, share, and forecast 2024–2030*. https://marksparksolutions.com/reports/saudi-arabia-cyber-security-market

[25] National Cybersecurity Authority (NCA). (2019). *Cybersecurity guidelines for e-commerce service providers*. Kingdom of Saudi Arabia.

[26] National Cybersecurity Authority (NCA). (2020). *Cloud cybersecurity controls*. Kingdom of Saudi Arabia.

[27] National Cybersecurity Authority (NCA). (2025). *Key economic indicators in the cybersecurity sector 2025*. Kingdom of Saudi Arabia. https://nca.gov.sa/en/studies-and-reports/

[28] Personal Data Protection Law (PDPL). (2021). Royal Decree M/19 of 9/2/1443H (16 September 2021), as amended by Royal Decree M/148 dated 5/9/1444H (27 March 2023). Kingdom of Saudi Arabia.

[29] P&S Intelligence. (2024). *Saudi Arabia cybersecurity market analysis: Insights from 2019 to 2030*. https://www.psmarketresearch.com/market-analysis/saudi-arabia-cybersecurity-market

[30] Rad, B. B., Diaby, T., & Rana, M. E. (2017). Cloud computing adoption: A short review of issues and challenges. *Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, Turku, Finland, 51–55. https://doi.org/10.1145/3108421.3108426

[31] ResearchAndMarkets / BusinessWire. (2025). *Growth opportunities in Saudi Arabia's cybersecurity market 2025–2034: Ranked second globally in cybersecurity*. https://www.businesswire.com/news/home/20251126016084/en/

[32] Saudi Data and Artificial Intelligence Authority (SDAIA). (2023). *Implementing regulations of the PDPL and regulations on personal data transfers outside the Kingdom*. SDAIA, Kingdom of Saudi Arabia.
[33] SentinelOne. (2025). *Cloud security statistics 2026: Key data and trends*. https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/
[34] SGS Group. (2025). *Strengthening cloud security in the Middle East: Challenges and best practices*. https://www.sgs.com/en-ae/news/2025/11/strengthening-cloud-security-in-the-middle-east-challenges-and-best-practices
[35] Sprinto. (2025). *60+ cloud security statistics: Quick facts for 2025*. https://sprinto.com/blog/cloud-security-statistics/
[36] Statista. (2024). *Saudi Arabia e-commerce market statistics and user forecast 2023–2027*. Statista GmbH.
[37] Trend Micro. (2021). *The most common cloud misconfigurations that could lead to security breaches*. Trend Micro Incorporated. https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches
[38] U.S. International Trade Administration. (2024). *Saudi Arabia digital economy country commercial guide*. U.S. Department of Commerce. https://www.trade.gov/country-commercial-guides/saudi-arabia-digital-economy-0
[39] upGrowth Digital. (2026, April). *Saudi SaaS compliance checklist [PDPL 2026]*. https://upgrowth.in/saudi-saas-compliance-checklist/
[40] Verizon. (2024). *2024 data breach investigations report*. Verizon Communications Inc.
[41] World Economic Forum (WEF). (2025). *Global cybersecurity outlook 2025*. World Economic Forum.
[42] Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud computing research and development trend. *2010 Second International Conference on Future Networks*, Sanya, China, 93–97. https://doi.org/10.1109/ICFN.2010.58