2025

Cloud Security Risks in the Shipping Sector

RESEARCH METHODS AND PROFESSIONAL PRACTICE JULY 2025 B - LITERATURE REVIEW

TYRONE LIM

Abstract

Cloud computing has become integral to the digital transformation of the shipping industry, enabling efficiency, scalability, and resilience. Yet its adoption introduces new vectors of cyber risk, particularly in ports and terminals where operational technology (OT), information technology (IT), and diverse stakeholders converge. This literature review critically evaluates quantitative evidence on cloud security risks in the shipping sector, with a particular emphasis on the Caribbean context and compliance obligations under the Jamaica Data Protection Act (JDPA, 2020). Drawing on industry surveys, regulatory frameworks, and academic studies, the review identifies five primary risk categories: identity and access management (IAM) flaws, misconfiguration, unsecured Application Programming Interfaces (APIs), ransomware, and systemic concentration. It compares perspectives on cloud as a resilience facilitator vs a concentration risk, and criticizes the research foundation for its lack of quantitative, port-specific data. The analysis concluded that without quantitative indications such as incident frequency, downtime, identity ratios, and compliance standards, ports like Kingston Freeport Terminal Limited (KFTL) run the danger of making governance choices based on assumptions rather than facts.

Introduction

The shipping industry is undergoing rapid digital transformation, with cloud computing increasingly integrated into terminal operations, logistics management, and cybersecurity monitoring. For ports and terminals such as Kingston Freeport Terminal Limited (KFTL) in Jamaica, cloud services support mission-critical systems, including Terminal Operating Systems (TOS), Port Community Systems (PCS), and data-sharing platforms. While cloud adoption provides scalability, resilience, and efficiency, it also creates new dangers in situations where operational technology (OT), information technology (IT), and a variety of stakeholders interact.

The audience for this review includes two groups: academic examiners, who will assess the work as part of the MSc programme, and professional practitioners in the maritime sector, who must understand how cloud adoption intersects with operational resilience and legal compliance.

The aim is to critically evaluate existing literature on cloud security risks in the shipping sector, with an emphasis on the Caribbean port context and the obligations imposed by the Jamaica Data Protection Act (JDPA, 2020). The review will provide:

1. An overview of current knowledge and quantitative evidence on cloud security risks.
2. An analysis of sector-specific risks in shipping and ports.
3. A comparison of contrasting perspectives on cloud as a resilience enabler versus a concentration risk.
4. A critique of research designs and identification of methodological gaps, particularly the absence of quantitative, port-level studies.
5. A conclusion that synthesizes findings and argues for metrics-driven governance approaches in Caribbean terminals.

Roadmap. The review proceeds in five parts. Section 2 examines general cloud security risks supported by quantitative industry data. Section 3 explores shipping-specific risks with reference to TOS, PCS, OT/IT convergence, and JDPA compliance. Section 4 contrasts optimistic and critical perspectives in the literature. Section 5 evaluates the research designs used in existing studies, highlighting strengths, limitations, and discrepancies. Section 6 concludes by identifying gaps and proposing a quantitative research agenda for KFTL and other regional ports.

General Cloud Security Risks

- Identity & access risk. Cloud identities, particularly non-human identities (NHIs), are increasing quickly. Microsoft (2023) reports that workload identities now outnumber human identities at a ratio of 10:1, while CyberArk (2025) estimates over 80:1 in some enterprises. Poorly managed tokens and service accounts increase breach risk (Microsoft, 2023; CyberArk, 2025).
- Misconfiguration & multi-cloud complexity. ENISA (2023) highlights that misconfiguration accounts for nearly half of reported cloud incidents. Multi-cloud adoption magnifies configuration drift, creating governance challenges.
- Insecure APIs. OWASP (2023) identifies broken object-level authorization (BOLA), misconfigured authentication, and unsafe API consumption as critical risks. Gartner predicts API abuses will soon be the leading cause of cloud breaches.
- Ransomware and disruption. Sophos (2024) reports that 59% of organizations suffered ransomware in the prior year, with USD 2.73M median recovery costs and 56% of encrypted victims paying ransom. IBM (2023) finds ransomware breaches cost on average USD 5.13M, higher than the global average of USD 4.45M (IBM, 2023; Sophos, 2024).
- Compliance and sovereignty. Standards such as ISO/IEC 27017 and the CSA Cloud Controls Matrix v4 clarify shared responsibility. Yet Pearson and Benameur (2019) argue compliance often lags behind technological change.

Summary. Quantitative evidence confirms that identity sprawl, misconfigurations, APIs, ransomware, and sovereignty issues remain persistent, measurable cloud risks.

Cloud Security Risks in the Shipping Sector

- SaaS vendor dependency. TOS vendors such as Navis N4 increasingly offer cloud-hosted models. In June 2025, CISA issued ICSA-25-175-01, warning of vulnerabilities in Navis N4 and recommending TLS enforcement and DDoS protections (CISA, 2025). Such advisories show how SaaS risks cascade to terminals. For KFTL, vendor reliance also raises JDPA accountability questions.
- OT/IT convergence. Cranes, gate control, and yard equipment now integrate with cloud analytics and vendor-managed remote access. If cloud identity tokens are compromised, physical operations could be disrupted.
- Compliance under JDPA. The JDPA (2020) requires Data Protection Impact Assessments (DPIAs), breach notifications, and controls for cross-border data transfers. Ports like KFTL remain legally responsible even if foreign SaaS vendors process the data.
- Case study: Maersk (NotPetya, 2017). While not cloud-specific, this incident cost USD 300M and disrupted TOS globally (Clavijo-Mesa et al., 2024). It underscores systemic risk when centralized digital systems fail.
- Ransomware and DDoS in ports. Ports remain prime ransomware targets (e.g., Port of Shahid Rajaee, 2020). Cloud exposure increases attack surface. Even short SaaS outages could paralyze KFTL's transshipment flows.
- Ecosystem and supply-chain risks. PCS involve carriers, truckers, customs, and freight forwarders. Breaches in any partner's cloud service could expose port or trade data.
- Concentration risks. Most maritime SaaS vendors run on one of the major *hyperscalers,* which large global cloud providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), whose massive, globally distributed

infrastructures deliver compute and storage at scale. While these platforms offer strong resilience, their dominance creates systemic fragility. Outages or vulnerabilities at a hyperscaler could simultaneously disrupt multiple ports, a disproportionate threat for small economies like Jamaica.

Critical Comparison of Perspectives

- Cloud as resilience enabler. ENISA (2023) and industry reports highlight how hyperscalers deliver redundancy, advanced DDoS defenses, and faster disaster recovery. Ports with constrained IT budgets (e.g., in the Caribbean) can benefit from access to enterprise-grade controls.
- Cloud as concentration risk. Conversely, CSA (2024) and CISA advisories emphasize persistent misconfigurations and SaaS vulnerabilities. Accountability remains with the customer under the shared responsibility model. Critics also highlight systemic fragility from hyperscaler dominance.
- Regulatory frameworks. IMO (2025) and BIMCO (2024) provide broad guidance, but lack cloud-specific metrics. CSA CCM and ISO/IEC 27017 offer more detailed controls. Ports must reconcile these layers with JDPA requirements.
- Evaluation. The optimistic view values cloud resilience benefits, while the critical view warns of systemic exposure. A balanced interpretation is that outcomes depend on measurable governance maturity and port-specific risk metrics.

Research Design & Gaps

Strengths of existing literature.

- Strong quantitative evidence on breach costs, ransomware prevalence, and insider threats (IBM, 2023; Sophos, 2024).
- Well-established control frameworks (CSA CCM v4, ISO/IEC 27017).

Limitations.

- Lack of shipping-specific, quantitative studies linking cloud incidents to operational KPIs.
- Compliance research dominated by GDPR/EU; minimal analysis of JDPA.
- Over-reliance on global surveys; Caribbean contexts underrepresented.

Discrepancies.

- ENISA (2023) emphasizes misconfigurations, while CSA (2024) prioritizes identity risk.
- Some maritime case studies stress operational resilience, others highlight systemic fragility (e.g., Maersk vs. Port of LA CRC).

Future quantitative agenda.

- Incident frequency baselines for PCS/TOS cloud disruptions.
- Resilience modelling (Monte Carlo simulation of downtime).
- Identity sprawl metrics (ratio of human: NHI accounts, rotation intervals).
- JDPA compliance benchmarking (DPIA adoption, breach notification times).
- Cost-impact regressions linking cloud incidents to shipping delays, demurrage, and reputational loss.

Conclusion

Quantitative evidence shows that identity sprawl, misconfigurations, ransomware, and SaaS dependency remain the most pressing risks, with misconfigurations accounting for nearly half of incidents (ENISA, 2023), ransomware recovery costs averaging USD 2.73M (Sophos, 2024), and non-human identities outnumbering human accounts by 10–80:1 (Microsoft, 2023; CyberArk, 2025).

For the shipping sector, these risks are magnified by SaaS reliance, OT/IT convergence, and ecosystem dependencies. The JDPA (2020) imposes compliance obligations that ports like KFTL must quantify through metrics such as DPIA adoption rates and breach response times.

The research differs: some see cloud as a resilience enabler (reducing downtime, offering enterprise-grade protection), others stress systemic concentration risks and governance gaps. Both perspectives are valid, but the absence of port-level, quantitative studies limits their applicability to contexts like KFTL.

Argument. Without quantitative measurement of incidents, KPIs, and compliance, port operators risk making governance decisions on assumption rather than evidence. Closing this gap requires adopting metrics-driven programs (e.g., tracking identity ratios, configuration drift, compliance benchmarks) aligned with CSA CCM v4, ISO/IEC 27017, and JDPA obligations.

To summarize, cloud adoption is both unavoidable and helpful for shipping, but it must be controlled using evidence-based, quantitative governance to assure resilience, compliance, and operational continuity.

References

BIMCO, ICS, INTERCARGO, & INTERTANKO. (2024). *The Guidelines on Cyber Security Onboard Ships* (Version 5). BIMCO.

CISA. (2025, June 24). *ICSA-25-175-01: Kaleris Navis N4 Terminal Operating System*. Cybersecurity and Infrastructure Security Agency.

Cloud Security Alliance. (2024). *Top Threats to Cloud Computing 2024*. Cloud Security Alliance.

Cloud Security Alliance. (2025). *Cloud Controls Matrix (CCM) v4*. Cloud Security Alliance.

CyberArk. (2025, April 23). *Machine Identities Outnumber Humans by More Than 80 to 1*. CyberArk.

ENISA. (2023). *ENISA Threat Landscape 2023: Cloud Security*. European Union Agency for Cybersecurity.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Security.

International Maritime Organization. (2025, April 4). *MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management*. IMO.

ISO/IEC. (2015). *ISO/IEC 27017:2015 — Code of practice for information security controls for cloud services*. International Organization for Standardization.

Jamaica Parliament. (2020). *The Data Protection Act, 2020 (Act No. 7 of 2020)*. Jamaica Gazette.

Microsoft. (2023, June 29). *Workload identities now outnumber human identities 10:1*. Microsoft Tech Community.

OWASP. (2023). *OWASP Top 10 API Security Risks – 2023*. OWASP Foundation.

Pearson, S., & Benameur, A. (2019). Privacy, security and trust in cloud computing. *Future Generation Computer Systems, 29*(2), 146–158. https://doi.org/10.1016/j.future.2011.12.006

Ponemon Institute. (2023). *Cost of Insider Threats 2023*. Ponemon Institute.

Sophos. (2024). *The State of Ransomware 2024*. Sophos.

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information*, *15*(11), 710. https://doi.org/10.3390/info15110710