XIV TRADITIONAL SCIENTIFIC CONFERENCE
NEW 2026 ECONOMY
New Horizons: Digital Economy and Responses to a Changing World

COLLECTION OF PAPERS
NEW ECONOMY
Volume 4, No. 1, 2026

CLOUD-ENABLED ACCESS MANAGEMENT IN SMART PORTS: A BUSINESS MODEL FRAMEWORK FOR SECURITY, EFFICIENCY AND GOVERNANCE

Maria Rosilene Sabino[1,2*], Marcela Castro[1,3,4], Shervin Shahidi[1], Ana Mendes[1,2], Tiago Pinho[1,2]

Received 07.03.2026. | Send to review 29.03.2026. | Accepted 04.08.2026.

Original Article

[1] Instituto Politécnico de Setúbal, Escola Superior de Ciências Empresariais, Campus do IPS - Setúbal, Portugal

[2] UNIDEMI, Department of Mechanical and Industrial Engineering, NOVA School of Science and Technology, Universidade NOVA de Lisboa, Portugal

[3] LASI - Laboratório Associado de Sistemas Inteligentes, Guimarães, Portugal

[4] NECE - Research Centre for Business Sciences, Department of Management and Economics, Faculty of Human and Social Sciences, Universidade da Beira Interior, Covilhã, Portugal

***Corresponding Author:**
Maria Sabino

Email:
mr.sabino@campus.fct.unl.pt

JEL Classification:
O31, O32, L86, L91, R40, M15

Doi: 10.61432/CPNE0401001s

UDK: 004.738.5:351.824.11

ABSTRACT

Smart ports increasingly rely on secure, interoperable, and scalable digital infrastructures to manage complex flows of cargo, vehicles, people, and information. Access management has therefore evolved from an operational security function into a strategic component of governance, cybersecurity, regulatory compliance, and logistics efficiency. This study proposes a cloud-enabled access management framework for smart port ecosystems. It adopts an exploratory, design-oriented methodology combining a Scopus-based literature review, benchmarking of 22 cloud-based access control systems, consultations with nine stakeholders, and value proposition analysis. The findings identify key technological, organizational, and regulatory requirements, including modular integration, multi-factor authentication, role- and zone-based access controls, interoperability with existing port systems, auditability, and compliance with data protection and information security standards. Stakeholder consultations further reveal recurring challenges, such as biometric reliability, entry delays, fragmented access control, high staff turnover, and continued reliance on manual procedures. The proposed framework links these challenges to value-creating mechanisms, including automated scheduling, remote management, API integration, alternative authentication methods, real-time monitoring, and non-compliance management. The study contributes to smart port research by conceptualizing cloud-enabled access management as both a governance and business model innovation capable of strengthening security, operational efficiency, and resilience across port ecosystems.

Keywords: *Smart ports, cloud-enabled access management, port governance, cybersecurity, business model innovation, maritime logistics, digital transformation, access control*

1. INTRODUCTION

Ports are undergoing a profound digital transformation. Once viewed primarily as physical interfaces between maritime and inland transport, they have evolved into complex cyber-physical ecosystems in which cargo flows, vehicle movements, personnel access, regulatory procedures, security requirements, and data infrastructures are closely interconnected. This transformation has increased the demand for secure, interoperable, and scalable systems that support both operational efficiency and infrastructure protection.

Access management is a critical yet underexplored component of this transition. In port environments, it extends beyond gate entry and credential verification to the governance of differentiated access rights across users, zones, schedules, operational roles, and security levels. Workers, contractors, drivers, inspectors, crews, passengers, technology providers, and public authorities may all require distinct combinations of physical and digital access. Access management therefore constitutes a strategic function for security, operational continuity, regulatory compliance, and logistics coordination.

Many legacy access control systems are poorly suited to these requirements. They often rely on static card-based mechanisms, fragmented databases, manual validation, and limited integration with wider port infrastructures. These limitations are particularly problematic in environments characterised by high personnel turnover, multiple access points, differentiated security zones, and the need for real-time visibility. Cloud-enabled access management offers a more flexible alternative through remote administration, multi-factor authentication, role- and zone-based permissions, modular integration, audit trails, dashboards, and interoperability with existing systems.

The empirical context of this study is a cloud-enabled access management prototype developed for port and logistics environments. The prototype provided a design-oriented basis for examining how access control, security, and surveillance functions can be integrated into a scalable digital architecture. The analysis considered anonymised requirements relating to physical and logical authentication, mobile and non-intrusive verification, entry and exit records, operational dashboards, failed authentication events, and integration with physical barriers and terminal devices. Broader issues, including service-based deployment, compatibility with logistics systems, and market acceptance, were also examined.

The study does not present the prototype as a commercial product or disclose operationally sensitive details. Instead, prototype-based evidence is used to develop a general analytical framework. The research question is therefore: How can cloud-enabled access management support the transition from legacy access systems to smart port governance in complex maritime logistics environments?

To address this question, the study adopts an exploratory, design-oriented approach combining a Scopus-based literature review, market benchmarking, stakeholder consultations, and value proposition analysis. The empirical design includes 61 scientific articles, 22 cloud-based access control systems, and nine consultation meetings involving six experts in port operations, security, logistics, and information technology. The paper contributes by conceptualising access management as a governance issue, linking cloud-based access control to cybersecurity, interoperability, and compliance, and proposing a framework that connects stakeholder challenges, technological enablers, and value-creation mechanisms.

The remainder of the paper is organised as follows. Section 2 presents the theoretical background. Section 3 describes the methodology. Section 4 reports the findings from the literature review, market benchmarking, stakeholder analysis, and framework development. Section 5 discusses the theoretical and practical implications, while Section 6 concludes with the main contributions, limitations, and directions for future research.

2. THEORETICAL BACKGROUND

2.1. SMART PORTS, DIGITAL TRANSFORMATION AND PORT OPERATIONAL GOVERNANCE

Ports are increasingly understood as digitally enabled, interconnected, and multi-actor systems rather than purely physical infrastructures for cargo handling. The transition towards smart ports reflects the wider digital transformation of maritime logistics, char-

acterised by the integration of data infrastructures, automation, the Internet of Things, cloud computing, artificial intelligence, and cyber-physical systems (Barasti et al., 2021; Nguyen et al., 2023; Pham, 2023). This transformation affects not only terminal productivity and cargo flows, but also security, stakeholder coordination, regulatory compliance, and operational governance.

Smart ports use advanced digital technologies to improve efficiency, transparency, sustainability, and connectivity across port ecosystems (Sarabia-Jacome et al., 2020; Tijan et al., 2021; Nguyen et al., 2026). However, smart port development extends beyond technology adoption and requires the reconfiguration of organisational processes, governance structures, and stakeholder relationships. Port Community Systems and logistics single windows illustrate this shift by enabling information exchange and coordinating port and hinterland operations (Carlan et al., 2016).

This governance dimension is particularly important because no single actor controls all flows of people, cargo, vehicles, information, and regulatory procedures within a port. Port authorities provide strategic direction and oversight, while terminal operators, logistics companies, security providers, technology vendors, and public agencies manage interdependent operational processes. Access management therefore forms part of a broader governance architecture. It involves defining who may access specific zones, systems, resources, and procedures, under which conditions, and with what degree of traceability (de Langen et al., 2020; Tijan et al., 2021).

Digitalisation also creates new vulnerabilities by increasingly linking physical and digital security (Marjohan et al., 2026). Cyber incidents may disrupt cargo handling, gate operations, identity verification, surveillance, customs procedures, and logistics coordination (Dimakopoulou & Rantos, 2024; Mileski et al., 2018; Senarak, 2021). Cloud-enabled access management can thus support smart port governance, but its effectiveness depends on interoperability, cybersecurity, data protection, stakeholder acceptance, and alignment with operational requirements, rather than on remote administration and real-time monitoring alone (Hu et al., 2020; Parkinson & Khan, 2023).

2.2. CLOUD-BASED ACCESS CONTROL AND CYBERSECURITY IN CRITICAL INFRASTRUCTURES

Access control is a foundational element of security management in critical infrastructures. In digitally connected environments, it increasingly combines physical security, identity management, authentication, authorisation, monitoring, data protection and auditability (Ferrari, 2010; Mohamed et al., 2022; Parkinson & Khan, 2023). This evolution is particularly important in ports, where operational spaces bring together employees, contractors, truck drivers, customs officers, ship crews, passengers, security personnel, and service providers.

Legacy access control systems often rely on static credentials, local databases, fixed permissions and hardware-dependent configurations. Such systems are less suited to port ecosystems characterised by temporary access needs, multiple entry points, differentiated security zones and changing operational schedules (Aksentijevic et al., 2021; Garzia et al., 2009; Koliousis, 2020). Cloud-based access control systems respond by shifting part of the infrastructure from local, hardware-bound environments to cloud-enabled platforms that support centralised oversight, scalable user management, automated backups, remote configuration and integration with mobile or web-based interfaces (Dubey & Rai, 2021; Hu et al., 2020).

Cybersecurity is central to the transition towards cloud-enabled access management. Although cloud-based systems can improve visibility, scalability, and responsiveness, they

also introduce risks related to data privacy, unauthorised access, insecure APIs, credential compromise, vendor dependence, cloud misconfiguration, and cyber-physical vulnerabilities (Chauhan & Shiaeles, 2023; Sun, 2019). Their design should therefore follow core security principles, including least privilege, multi-factor authentication, encryption, timely access revocation, continuous monitoring, incident response, and compliance with recognised information security standards (El Kafhali et al., 2022; Hu et al., 2020).

Attribute-Based Access Control enables permissions to be assigned according to user characteristics, roles, location, time, context, and operational requirements (Hu et al., 2020; Mohamed et al., 2022). This is particularly relevant in ports, where access rights vary across professional functions, security zones, schedules, and operational conditions. Attribute-based encryption and fine-grained access controls can further protect sensitive cloud-based data (Ding et al., 2020; Namasudra, 2019). Blockchain and distributed ledger technologies may also enhance auditability, tamper resistance, and decentralised verification, although their use is most appropriate where distributed trust or verifiable records are required (Agyekum et al., 2022; Yang et al., 2020).

Biometric authentication, mobile credentials, and multi-factor authentication provide additional security layers. However, biometric systems also raise concerns regarding reliability, privacy, data protection, and user acceptance (Parkinson & Khan, 2023; Sun, 2019). Port access management should therefore be treated as a cyber-physical governance challenge involving technologies, rules, responsibilities, data flows, permissions, and accountability mechanisms.

2.3. BUSINESS MODEL INNOVATION AND VALUE PROPOSITION DESIGN IN PORT ECOSYSTEMS

The adoption of cloud-enabled access management in ports represents not only a technological advancement but also a business model innovation. Unlike traditional hardware-intensive access control systems, cloud-based solutions support Software-as-a-Service (SaaS), subscription models, modular deployment, remote maintenance, scalable user management, and integration-based value creation (Chauhan & Shiaeles, 2023; Hu et al., 2020; Marinov & Lisenyi, 2024).

This innovation is particularly relevant in port ecosystems, where value is co-created by multiple stakeholders. Cloud-enabled access management can improve governance and compliance for port authorities, workforce management for terminal operators, operational efficiency for logistics providers, and traceability for regulators. Such a multi-stakeholder perspective aligns with ecosystem-based approaches to maritime value creation, in which performance depends on coordination rather than on isolated organisational decisions (De Martino, 2021; Tsvetkova & Hellström, 2022; Mussina et al., 2026).

Value Proposition Design provides a useful framework for linking stakeholder needs with technological capabilities (Osterwalder et al., 2014). Common challenges in port access management include entry delays, fragmented access controls, unreliable biometric authentication, high staff turnover, manual authorisation procedures, limited interoperability, and the management of temporary users. These challenges translate into requirements such as API integration, automated scheduling, continuous operation, role-based access, reduced manual intervention, and alternative authentication methods.

Regulatory compliance constitutes a further element of the value proposition. Because ports process sensitive personal, operational, and commercial data, cloud-based access management must comply with data protection and information security standards, including the GDPR and ISO/IEC 27001, 27017, and 27018. Compliance not only satisfies legal requirements but also strengthens trust among port authorities, service providers, regulators, and users.

Accordingly, cloud-enabled access management should be viewed as a socio-technical governance innovation that integrates technological capabilities, stakeholder requirements, regulatory compliance, and operational processes. This perspective underpins the analytical framework developed in the following sections, where cloud-enabled access management is examined through three complementary dimensions: technological infrastructure, governance, and business model design.

3. METHODOLOGICAL APPROACH

This study adopts an exploratory, design-oriented approach to develop a cloud-enabled access management framework for smart port ecosystems. The research addresses the intersection of smart port transformation, cloud-based access control, cybersecurity, operational governance, and business model innovation. Given the emerging and multidisciplinary nature of the topic, the study integrates multiple sources of evidence rather than testing predefined hypotheses.

The methodology comprises four stages: literature review, market benchmarking, stakeholder consultation, and value proposition and framework development. Exploratory research is appropriate for examining emerging phenomena, synthesising heterogeneous evidence, and developing frameworks for subsequent empirical validation (Creswell, 2009; Saunders et al., 2023). The design-oriented component draws on research traditions that develop artefacts, models, and frameworks in response to practical problems while also contributing to theoretical knowledge (Hevner et al., 2004; Peffers et al., 2007).

The empirical basis includes project documentation and prototype-oriented design materials generated within a port innovation context. These materials were used to identify requirements, stakeholder concerns, and design relationships. Because some contain operational, consortium-related, or commercially sensitive information, they are not cited directly. Findings derived from them are therefore presented in aggregated and anonymised form.

The methodological design and the role of each evidence source are summarised in Table 1.

Table 1. Research design and evidence integration

Methodological stage	Evidence source	Procedure	Analytical purpose	Output
Literature review	Scopus and selected academic literature	Broad search, refined query, citation-based selection and contextual searches	Identify conceptual foundations and research gaps	Final analytical corpus of 61 articles
Market benchmarking	22 cloud-based access control systems	Comparative analysis across six functional dimensions	Identify technological, deployment and business model patterns	Market-informed system requirements
Stakeholder consultations	Six stakeholders across nine meetings	Semi-structured consultations, online and in-person meetings, and recorded sessions	Capture operational pain points, expectations and implementation constraints	Stakeholder requirements and value-creating mechanisms
Value proposition development	Integrated stakeholder and market evidence	Pain-point/gain mapping, mind maps and Business Model Canvas	Connect operational needs with system capabilities	Structured value proposition
Framework development	Integrated multi-source evidence	Cross-source synthesis and BPMN-oriented process modelling	Relate drivers, enablers and governance outcomes	Three-layer analytical framework

Source: Authors' elaboration

3.1. LITERATURE REVIEW

The first stage consisted of an exploratory literature review designed to identify conceptual foundations, relevant research streams and application-oriented evidence related to cloud-enabled access management in smart port environments. Literature reviews are appropriate for organising fragmented knowledge, identifying conceptual patterns and clarifying emerging research domains (Snyder, 2019; Tranfield et al., 2003). The review focused on the intersection of cloud computing, access control, cybersecurity, smart ports, port digitalisation, business model innovation and maritime logistics.

The review began with a broad exploratory search in the Scopus database using combinations of terms related to *cloud* and *access control*. The initial search, covering the period from 1988 to 2025, retrieved approximately 7,800 documents. This broad search was used to assess the field's scale and evolution and to identify the need for a more focused search strategy.

The search was subsequently refined using the expression: TITLE-ABS-KEY("cloud computing" AND "access control" AND "Security"), with restrictions applied by publication period, document type and subject area. The refined search produced 1,701 documents. From this set, the 50 most-cited publications were used as an initial analytical core to capture influential contributions to cloud computing, access control and security.

To explore innovation at the nexus of business models and ports, two additional searches were carried out:

- TITLE-ABS-KEY("cloud computing" AND "access control" AND "Security") AND TITLE-ABS-KEY("BUSINESS MODEL")
- TITLE-ABS-KEY("cloud computing" AND "access control" AND "Security") AND TITLE-ABS-KEY("SEAPORT" OR "PORT" OR "MARITIME" OR "SHIP")

The initial analytical core and the supplementary searches were consolidated into a final corpus of 61 articles considered relevant to the study's analytical scope. The literature was subsequently examined comparatively to identify recurring conceptual and application-oriented themes relevant to cloud-enabled access management. These themes informed the interpretation of access security, privacy and data governance, connected infrastructures, auditability, interoperability and cloud governance, and were later compared with evidence from market benchmarking and stakeholder consultation.

3.2. MARKET BENCHMARKING

The second stage consisted of market benchmarking of cloud-based access control systems. The purpose was to identify technological trends, deployment models, authentication mechanisms, integration requirements, operability features and business model patterns relevant to logistics and port environments.

An initial screening identified 22 systems with potential relevance to the research problem. Rather than comparing or ranking individual suppliers, the analysis extracted functional and strategic characteristics that could inform the proposed cloud-enabled access management framework.

The evidence was organised around six dimensions: use type, authentication, deployment, access and management, features and operability, and pricing. These parameters were used to identify requirements such as multi-factor authentication, mobile credentials, QR codes, RFID, biometric options, cloud and hybrid deployment, browser and mobile access, remote permissions, CCTV, real-time alarms, automatic backups, interoperability, lockdown functions, freemium models, volume-based pricing and flexible subscription options.

The benchmarking evidence was analysed comparatively to identify recurring requirements rather than vendor-specific advantages. Attention was given to modularity, interoperability, scalability, remote management, compatibility with legacy infrastructures and the implications of alternative deployment and pricing models. These findings were subsequently compared with stakeholder evidence and used to support the value proposition and the development of the framework.

3.3. STAKEHOLDER CONSULTATIONS

The third stage involved semi-structured stakeholder consultations designed to identify operational requirements, implementation constraints, and system expectations not fully captured by the literature review or market benchmarking. A purposive sampling approach was used to involve participants with direct expertise in port operations, access security, logistics, and information technology.

Six participants contributed: one Information Systems and Business Support Manager from the Port of Sines, two representatives associated with Port Facility Security Officer functions, one logistics or terminal operator representative, and two IT specialists. Their roles provided complementary perspectives on access procedures, security requirements, systems integration, and technological implementation.

Data were collected through nine consultation meetings. Six meetings with the IT specialists were conducted online via Microsoft Teams and recorded. Two meetings with Port of Sines representatives were held in person, while one meeting with the logistics or terminal operator representative was conducted online. Repeated consultations with the IT specialists supported the progressive clarification of technical requirements, authentication options, integration constraints, system architecture, and cloud, on-premises, and hybrid configurations.

A semi-structured interview guide was used with port and terminal stakeholders. It covered user categories, access authorisation volumes, communication channels, authentication methods, control points, hardware configurations, validation systems, biometric technologies, and access to sensitive data. The format ensured consistency across core topics while allowing participants to elaborate on context-specific issues.

The consultation evidence included recordings, transcripts, meeting notes, mind maps, and structured technical premises. These materials were organised around recurring themes, including authentication reliability, biometric limitations, access delays, workforce variability, differentiated access zones, interoperability, remote management, credential lifecycle management, and non-compliance monitoring.

The data were analysed through iterative thematic synthesis. First, recurring operational problems and requirements were identified. Second, related issues were grouped into three categories: stakeholder pain points, system requirements, and value-creating mechanisms (Chenail, 2016; Miles et al., 2013). Finally, these categories were compared with the findings from the literature review and market benchmarking. The aim was analytical integration rather than statistical generalisation, supporting the development of the proposed design-oriented framework.

3.4. VALUE PROPOSITION AND FRAMEWORK DEVELOPMENT

The fourth stage translated evidence from the literature review, market benchmarking, and stakeholder consultations into a structured value proposition and analytical framework. Value Proposition Design was used to link stakeholder pain points with expected gains, system requirements, and value-creating mechanisms (Osterwalder et al., 2014).

The synthesis followed three steps. First, recurring operational challenges were identified, including biometric reliability issues, access delays, high workforce turnover, fragmented credential management, differentiated access requirements across port zones, and limited interoperability. Second, these challenges were matched with potential system responses derived from market benchmarking and technical consultations, such as multimodal authentication, remote permission management, API integration, automated scheduling, credential lifecycle management, dashboards, and alternatives to biometric verification.

Third, the resulting relationships were organised through visual and process-oriented tools. Mind maps consolidated stakeholder concerns and expected outcomes, while the Business Model Canvas supported the integration of value propositions, user requirements, service configuration, and business model considerations. BPMN-based process modelling, supported by draw.io, was used to represent the activity flows for user registration, identity validation, authentication, access authorisation, permission management, exception handling, and access logging.

These analytical artefacts helped integrate heterogeneous evidence and clarify the relationships among operational challenges, technological capabilities, governance requirements, and business model implications. The resulting three-layer framework comprises: adoption drivers, including security, efficiency, scalability, and compliance; cloud-enabled capabilities, including APIs, interoperability, multi-factor authentication, fallback mechanisms, auditability, dashboards, and monitoring; and governance outcomes, including traceability, zone-based access, reduced manual control, interoperability, and operational resilience.

The framework is presented as a design-oriented analytical contribution rather than a universally validated model. It is intended to support future empirical testing, pilot implementation, and comparative assessment across different port environments.

3.5. METHODOLOGICAL SCOPE AND LIMITATIONS

The methodological approach has several limitations that should be considered when interpreting the findings.

First, the study is exploratory and design-oriented. It develops a framework by integrating evidence from the literature review, market benchmarking, stakeholder consultations, and prototype-oriented material, but it does not provide a longitudinal evaluation of a fully deployed cloud-enabled access management system.

Second, the literature review was designed to support conceptual integration and framework development rather than to function as a fully systematic review or meta-analysis. The initial selection of highly cited studies strengthened coverage of influential contributions, but it may also favour established research over emerging work. Supplementary contextual searches were therefore used to broaden the corpus towards business model and maritime-port applications.

Third, the market benchmarking was used to identify recurring capabilities, deployment patterns and business model characteristics rather than to compare or rank commercial providers. The findings should therefore be interpreted as market-informed requirements rather than as evidence of relative supplier performance.

Fourth, the stakeholder evidence is based on a purposively selected group of six participants across nine consultation meetings. Although these participants provided complementary expertise in port operations, security, logistics and information technology, the sample is not statistically representative of the wider population of port actors. The findings should therefore be interpreted as analytically useful evidence for framework development rather than as generalisable quantitative results.

Finally, the proposed framework emerged from a specific port-innovation context and the integration of multiple evidence sources. Although this strengthens its practical relevance, its transferability to other ports depends on factors such as port scale, governance model, technological maturity, regulatory context and existing infrastructure. Future research should therefore test and refine the framework through comparative case studies, pilot implementations and longitudinal evaluation.

4. RESULTS

4.1. LITERATURE-BASED ANALYTICAL THEMES

The literature review showed that cloud-enabled access management is positioned at the intersection of several interconnected research domains, including cloud computing, access control, cybersecurity, privacy, Internet of Things technologies, fine-grained authorisation, auditability and digital governance. Across the reviewed studies, five recurring analytical themes were particularly relevant to the development of the proposed framework (Hu et al., 2020; Sun, 2019).

The first theme concerns cloud security and access management. Research in this area emphasises the need for scalable identity management, secure authorisation and context-sensitive access decisions in distributed digital environments. Cloud-based access systems can support centralised oversight, remote administration, and flexible permission management, but they also raise concerns about cloud misconfiguration, credential compromise, insecure APIs, and shared responsibility (Chauhan & Shiaeles, 2023; Hu et al., 2020; Sun, 2019). In port environments, these issues are particularly relevant because access decisions may involve heterogeneous users, multiple security zones and operationally critical infrastructures.

The second theme concerns privacy and data governance. Access management systems process identities, credentials, access histories and, in some cases, biometric data. The literature therefore emphasises privacy protection, data minimisation, secure processing, accountability, and controlled access to sensitive information (Ding et al., 2020; Namasudra, 2019; Sun, 2019). For smart ports, this theme is important because personal and operational data may circulate across organisational boundaries involving port authorities, terminal operators, logistics firms, technology providers and public agencies.

The third theme concerns IoT and cyber-physical integration. Smart port environments increasingly connect gates, sensors, mobile devices, surveillance systems and operational platforms. This integration creates opportunities for real-time visibility and coordinated access management, but also expands the attack surface and increases the complexity of identity, permission and device governance (Nguyen et al., 2023; Sarabia-Jacome et al., 2020). Access management should therefore be understood as part of a broader cyber-physical infrastructure rather than as an isolated gate-control function.

The fourth theme concerns auditability and distributed verification. The literature identifies growing interest in secure logging, traceable permission changes, verifiable records and, in specific contexts, blockchain-based mechanisms for distributed trust and tamper-resistant audit trails (Agyekum et al., 2022; Appleyard & Yuthas, 2022; C. Yang et al., 2020). However, blockchain is not treated in this study as a universal solution. Its relevance depends on whether the governance context requires cross-organisational verification, distributed trust or enhanced resistance to record manipulation.

The fifth theme concerns interoperability and cloud governance. Secure cloud adoption requires more than authentication mechanisms. It also involves integration with existing systems, allocation of responsibilities, incident response, risk management, data-sharing rules and compatibility with legacy infrastructures (Chauhan & Shiaeles, 2023; Dimako-

poulou & Rantos, 2024; Senarak, 2021). In port ecosystems, interoperability is especially important because access management may need to interact with Port Community Systems, logistics platforms, human resource databases, contractor systems and surveillance infrastructures.

The literature-based themes are summarised in Table 2.

Table 2. Main analytical themes identified in the literature and their relevance for cloud-enabled access management in ports

Analytical theme	Main concepts	Interpretation	Relevance for smart ports
Cloud security and access management	Cloud computing; access control; authentication; authorisation	Focuses on secure and scalable management of identities and permissions	Supports flexible and context-sensitive access decisions
Privacy and data governance	Data privacy; secure processing; data minimisation; accountability	Highlights protection and governance of sensitive personal and operational data	Relevant for identity, credential and biometric data
IoT and cyber-physical integration	IoT; connected devices; sensors; surveillance; mobile systems	Addresses integration and security across connected physical and digital infrastructures	Relevant for gates, devices, mobile credentials and real-time monitoring
Auditability and distributed verification	Logging; traceability; blockchain; verifiable records	Focuses on accountability, secure records and conditional distributed trust	May support multi-actor verification and incident investigation

Source: Authors' elaboration based on the reviewed literature

Taken together, these themes indicate that access management is evolving from a predominantly technical concern with authentication and authorisation towards a broader discussion involving cybersecurity, data governance, connected infrastructures, interoperability and organisational responsibility. From a smart port perspective, this suggests that access management should be understood as part of port digital governance rather than as an isolated security subsystem.

The literature also reveals a continuing fragmentation between highly technical research on cloud security and access control and more application-oriented studies on smart ports and port digitalisation. The specific intersection between cloud-enabled access management, port governance, business model innovation and stakeholder value creation remains comparatively underdeveloped. This gap provides the rationale for complementing the literature review with evidence from market benchmarking and stakeholder consultations in the following sections.

4.2. MARKET BENCHMARKING OF CLOUD-BASED ACCESS CONTROL SYSTEMS

The market benchmarking complemented the literature review by examining how cloud-based access control capabilities are configured in practice. The analysis showed that market offerings differ not only in technical features, but also in deployment architecture, management logic, interoperability, and business model design. These dimensions are particularly relevant to smart ports, where access systems must accommodate heterogeneous users, critical infrastructure, and legacy digital environments.

Six benchmarking dimensions were identified: use type, authentication, deployment, access and management, features and operability, and pricing and business model configuration.

The first dimension, use type, distinguishes systems designed for domestic, office, industrial, or application-specific contexts. Port environments require more complex configurations because they combine critical infrastructure protection, logistics operations, workforce and contractor access, ship-related activities, and public–private coordination. Access systems must therefore support multiple user groups, security levels, and physical zones (Pham, 2023; Sarabia-Jacome et al., 2020; Tijan et al., 2021).

The second dimension concerns authentication. The benchmarked systems supported combinations of PIN codes, multi-factor authentication, mobile credentials, QR codes, RFID, smart devices, and biometrics. This diversity suggests that smart ports require configurable, multimodal authentication adapted to different user categories and operational conditions (Bast & Yeh, 2024; Parkinson & Khan, 2023).

The third dimension relates to deployment architecture. On-premises, cloud-based, and hybrid configurations were identified. While cloud deployment offers scalability and remote administration, hybrid solutions may be necessary to ensure compatibility with legacy infrastructure and operational continuity. The findings therefore support a gradual transformation pathway based on interoperability, governance, and risk management (Chauhan & Shiaeles, 2023; Sun, 2019).

The fourth dimension covers access and management capabilities, including browser, desktop, and mobile access, guest permissions, customised restrictions, and remote administration. These functions are important in ports, where authorisation may depend on role, location, time, task, and security level. Remote management is especially valuable for temporary credentials, operational changes, and exceptional access requests.

The fifth dimension concerns features and operability. Relevant capabilities included CCTV integration, real-time alarms, mass notifications, automatic backups, lockdown functions, interoperability, and hardware integration. These features indicate that access control is evolving from isolated entry management towards integrated security and operational platforms linked to surveillance, incident response, compliance, and continuity planning (Dimakopoulou & Rantos, 2024; Senarak, 2021).

The sixth dimension addresses pricing and business model configuration. The systems employed subscription, freemium, volume-based, modular, and trial-based models. Although these approaches may reduce initial investment and improve scalability, they also raise concerns regarding cost predictability, service continuity, cybersecurity responsibilities, and vendor dependence (Marinov & Lisenyi, 2024; Osterwalder et al., 2014).

Across these dimensions, five capabilities emerged as particularly relevant to smart ports: multimodal authentication, modular deployment, configurable remote management, interoperability, and flexible service models. However, technological functionality alone does not guarantee successful adoption. Operational value also depends on compatibility with existing infrastructure, regulatory requirements, organisational routines, and stakeholder expectations. The benchmarking findings were therefore treated as market-informed inputs to the proposed framework rather than as evidence of technological determinism.

The benchmarking dimensions and their relevance to smart port access management are presented in Table 3.

Table 3. Market benchmarking criteria and relevance for smart port access management

Benchmarking criterion	Main elements identified	Relevance for smart ports
Use type	Domestic, office, industrial and application-specific settings	Highlights the need for configurations adapted to critical infrastructure and multi-actor port operations
Authentication	PIN, multi-factor authentication, mobile credentials, QR codes, RFID, smart cards and biometrics	Supports differentiated access procedures across heterogeneous user groups
Deployment	On-premises, cloud-based and hybrid configurations	Enables progressive transition from legacy systems while preserving continuity and compatibility
Access and management	Browser, desktop and mobile applications, guest access, customised permissions and remote administration	Supports role-, zone-, time- and task-based access management
Features and operability	CCTV, video/audio, alarms, notifications, backups, lockdown and interoperability	Connects access control with surveillance, incident response and operational continuity
Pricing and business model	Trials, freemium, subscriptions, volume-based and modular arrangements	Supports alternative service models while raising cost, dependency and governance considerations

Source: Authors' elaboration

The market benchmarking, therefore, confirms that cloud-enabled access management should be evaluated against both technological and organisational criteria. In smart port ecosystems, the value of access management systems depends not only on authentication and surveillance features, but also on interoperability, progressive deployment, governance compatibility and the capacity to adapt to heterogeneous operational requirements. This finding provides the basis for the stakeholder analysis in the next section, where market capabilities are compared with operational pain points and user expectations.

4.3. STAKEHOLDER PAIN POINTS AND SYSTEM REQUIREMENTS

The stakeholder consultation process identified key operational concerns not fully addressed by the literature review or market benchmarking. Participants in nine meetings highlighted that the shift from legacy access control to cloud-based management is primarily motivated by the need to resolve ongoing issues such as authentication reliability, access delays, workforce variability, fragmented permissions, and system interoperability.

The first group of concerns involved identity verification and the reliability of authentication. Participants noted challenges with biometric recognition, card readers, and reliance on single authentication methods. Biometric systems can be affected by device issues, environmental factors, and changes in user appearance, while physical cards may be lost or poorly tracked. The evidence suggests a need for multimodal authentication that combines various methods, such as physical and mobile credentials, multi-factor authentication, biometric verification, and fallback procedures, highlighting the importance of diverse and context-sensitive access mechanisms in complex environments (Bast & Yeh, 2024; Parkinson & Khan, 2023).

The second group concerns operational delays and fragmented validation procedures. Participants highlighted scenarios in which manual checks, redundant registration processes, distinct validation systems, and generic credentials can create bottlenecks at access points. In port environments, such delays extend beyond mere administrative inconveniences, as these access points are intrinsically linked to workforce movements,

vehicle flows, and logistics coordination. Consequently, the consultation findings indicated a need for solutions such as automated scheduling, remote permission management, pre-registration, self-service procedures, and digital records to reduce the need for repeated manual intervention.

The third group was concerned with workforce variability and credential lifecycle management. Port and logistics environments often involve temporary workers, subcontractors, and external service providers, resulting in rapidly changing access rights. This creates an operational burden in managing credentials across various systems. Therefore, automated user lifecycle management, quick permission updates, expiration controls, and traceable revocation procedures are crucial. Cloud-enabled access management can deliver value by facilitating flexible administration of diverse, time-sensitive user profiles.

A fourth group of concerns related to differentiated access across roles, zones, and operational conditions. The consultations showed that port access cannot be reduced to a binary entry decision. Permissions may depend on professional role, organisational affiliation, security clearance, access zone, time period, operational task, document validity, and specific authorisation conditions. Participants therefore emphasised the need for configurable and granular access rules, consistent with Attribute-Based Access Control and fine-grained authorisation models (Hu et al., 2020; Mohamed et al., 2022).

A fifth concern involved limited interoperability with existing systems. Ports typically operate multiple platforms, devices, databases, and operational procedures, requiring access management to interact with Port Community Systems, logistics platforms, contractor databases, human resource systems, surveillance technologies, and legacy access-control infrastructure. The findings therefore highlight the importance of API-based integration, legacy-system compatibility, and hybrid deployment. Rather than complete system replacement, participants generally favoured gradual integration that preserves operational continuity.

The consultations also stressed the importance of monitoring, non-compliance management, and auditability. Key requirements included detecting suspicious behaviour, recording failed authentication attempts, monitoring access events, and maintaining traceable permission histories. These concerns translated into demands for real-time alerts, dashboards, non-compliance modules, and audit trails, particularly in environments where physical security, cybersecurity, and operational continuity are closely interconnected (Dimakopoulou & Rantos, 2024; Senarak, 2021).

Finally, the consultation process revealed that data governance and privacy are integral to access management design. Discussions on biometric data, personal information and external system integration raised questions about data storage, access authorisation, permission management, and the distribution of responsibilities among port organisations, technology providers, and users. This emphasises the importance of integrating data minimisation, role clarity, access logging, and privacy-oriented governance into cloud-enabled architectures from the outset, rather than as afterthoughts.

A synthesis of the main pain points, their operational interpretation and the corresponding system requirements is presented in Table 4.

Table 4. Stakeholder pain points and cloud-enabled system requirements

Stakeholder pain point	Operational interpretation	Cloud-enabled system requirement	Expected value creation
Biometric reliability issues	Authentication may be affected by device, environmental or user-related conditions	Multi-modal authentication; biometric alternatives; fallback procedures	Improves continuity and reliability of access decisions
Card reader issues and non-personalised cards	Physical credentials may be lost, shared or insufficiently traceable	Individualised credentials; mobile credentials; digital access records	Strengthens accountability and traceability
Entry delays and fragmented validation	Manual and repeated procedures create bottlenecks	Automated scheduling; self-service registration; remote permissions	Reduces congestion and administrative burden
High staff turnover and temporary users	Credentials require frequent creation, modification and revocation	Automated lifecycle management; rapid updates; expiration and revocation controls	Supports flexible workforce management and reduces security gaps
Role and zone complexity	Permissions vary by function, location, time and operational purpose	Role-, zone-, time- and attribute-based access rules	Enables granular and context-sensitive access management
Multiple systems and limited interoperability	Fragmented platforms and legacy infrastructure constrain coordination	API integration; hybrid deployment; compatibility with existing systems	Improves data flow, scalability and progressive transformation
Suspicious behaviour and non-compliance	Limited visibility reduces detection and accountability	Real-time monitoring; non-compliance modules; audit trails	Enhances prevention and traceability
Data governance and privacy concerns	Personal and biometric data involve multiple actors and responsibilities	Role-based data access; logging; consent and permission management; privacy-oriented controls	Strengthens trust, accountability and regulatory alignment

Source: Authors' elaboration

The consultation findings highlight that the value of cloud-enabled access management goes beyond advanced technology. Features like authentication, interoperability, and data governance are only valuable when they address specific operational issues. This underscores the importance of using Value Proposition Design to link stakeholder challenges with system capabilities and expected outcomes (Osterwalder et al., 2014).

Furthermore, access control is a technical function, while access management is a governance capability. Concerns identified in the consultations extend beyond physical barriers; they include identities, permissions, user categories, data responsibilities, and accountability within a multi-actor ecosystem. This distinction forms the basis for the three-layer framework outlined in the next section.

4.4. CLOUD-ENABLED ACCESS MANAGEMENT FRAMEWORK

This section presents a cloud-enabled access management framework for smart port ecosystems, drawing on evidence from the literature review, market benchmarking, and stakeholder consultation. The framework integrates findings into three interdependent layers: adoption drivers, technology enablers, and governance outcomes.

This structure reflects the study's design-oriented logic. It posits that cloud-enabled access management generates value not just through technology adoption, but by aligning

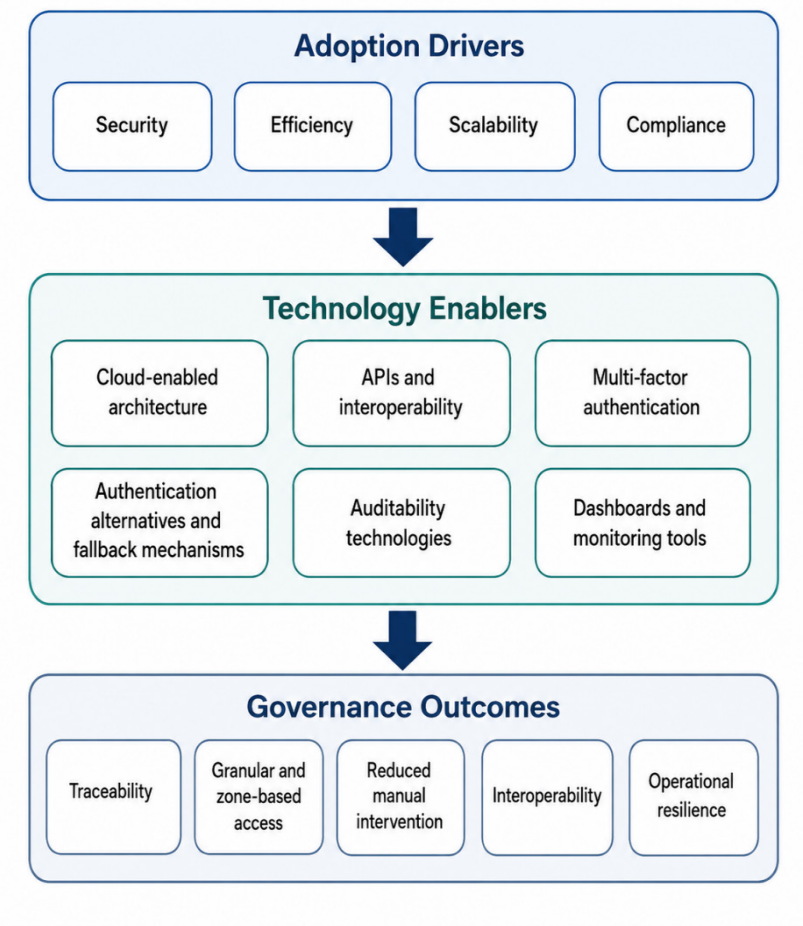
specific operational and governance needs with appropriate technological capabilities. This alignment leads to improved port coordination, security, and resilience.

The first layer concerns adoption drivers: security, efficiency, scalability and compliance. Security is the primary driver, as ports are critical infrastructures where access decisions involve people, vehicles, and restricted zones. Concerns about biometric reliability, suspicious behaviour, and limited traceability highlight the need for secure authorisation and real-time monitoring (Dimakopoulou & Rantos, 2024; Hu et al., 2020; Senarak, 2021). Efficiency is the second driver. Stakeholder feedback indicated that access delays and manual validation create administrative burdens and operational bottlenecks, affecting workforce mobility and vehicle flows. Cloud solutions can help streamline processes through pre-registration, remote permission management, and automated scheduling (Sarabia-Jacome et al., 2020; Tijan et al., 2021). Scalability matters because port environments involve heterogeneous users and variable access needs. High turnover and frequent credential updates can be challenging. Cloud-based systems offer modular deployment and configurable permissions, allowing for adaptability to evolving operational needs (Chauhan & Shiaeles, 2023; Hu et al., 2020). Compliance involves managing personal data and access records securely. It is essential to adhere to regulations such as the GDPR and ISO standards to ensure lawful data processing and auditability. Compliance is seen not just as a constraint but as a vital aspect of trust and governance (Hu et al., 2020; Mell & Grance, 2011).

The second layer comprises the technological enablers of cloud-enabled access management: cloud architecture, APIs and interoperability, multi-factor authentication, alternative and fallback authentication mechanisms, auditability technologies, and monitoring dashboards (Carlan & Vanelslander, 2021; Sarabia-Jacome et al., 2020). Authentication diversity improves operational flexibility, particularly when biometric methods raise concerns about reliability, privacy, or user acceptance. Auditability may rely on conventional logging systems or, where tamper-resistant records and distributed trust are required, blockchain-based solutions (Agyekum et al., 2022; Yang et al., 2020). Dashboards and monitoring tools convert access data into actionable information for oversight and decision-making.

The third layer focuses on governance outcomes, including traceability, zone-based access, reduced manual intervention, interoperability, and operational resilience. Traceability supports auditing, incident investigation, and accountability, while zone-based access enables context-sensitive permissions across gates, terminals, warehouses, restricted areas, and vessel-related interfaces. Reduced manual control lowers administrative burden and allows staff to focus on exceptional cases. Interoperability strengthens coordination and data-driven governance, while operational resilience is enhanced through improved visibility, remote administration, credential revocation, incident response, and continuity management (Dimakopoulou & Rantos, 2024; Senarak, 2021). The proposed framework is presented in Figure 1.

Figure 1. Cloud-enabled access management framework for smart ports



Source: Authors' elaboration

The framework should not be viewed as a linear implementation process. The three layers are interdependent and can influence each other through feedback. For example, compliance requirements may affect authentication and data architectures, while interoperability constraints can shape deployment. Experience with operational outcomes may also lead to redesigning permissions and dashboards. Thus, the framework is a dynamic analytical structure rather than a fixed technological blueprint.

This interpretation highlights the difference between access control and access management. Access control focuses on the mechanisms for granting or denying access, whereas access management encompasses the governance of identities, permissions, user categories, zones, data responsibilities, exceptions, and accountability. In smart port ecosystems, this broader view is crucial, as access decisions are linked to complex operational relationships rather than isolated technical transactions.

The framework, therefore, positions cloud-enabled access management as an integrated governance capability rather than an isolated technical subsystem. Its value lies not in replacing individual access devices, but in enabling a more configurable, traceable and interoperable approach to managing identities, permissions and access-related processes across multiple actors and systems.

The proposed framework provides the basis for the next section, which examines the business model and regulatory requirements associated with its implementation.

4.5. BUSINESS MODEL AND REGULATORY REQUIREMENTS

The development of cloud-enabled access management in smart ports requires a solid business model, clear responsibilities, and a regulatory framework for data protection, cybersecurity, and operational continuity. The framework in Section 4.4 must be integrated into the organisational and economic structures that define value creation and governance in the port ecosystem. This reflects a broader movement from product-based access control towards service-oriented digital platforms, consistent with the business model innovation literature that emphasises the value proposition, delivery mechanisms, revenue logic, and customer-oriented value creation (Osterwalder et al., 2014; Teece, 2010).

Four interrelated requirements emerge from the analysis: value proposition, service configuration, cost structure and risk allocation. The value proposition must demonstrate how the system reduces manual procedures, improves traceability, supports compliance and strengthens resilience. Service configuration must define whether the model is cloud-based, hybrid or integrated with legacy infrastructures. The cost structure must consider subscription fees, integration, hardware adaptation, maintenance, cybersecurity safeguards, and staff training. Risk allocation must clarify responsibilities for data protection, availability, incident response, vendor dependency and service-level agreements.

Regulatory compliance is a core component of the proposed business model. In European ports, the GDPR establishes the legal basis for lawful, transparent, and proportionate processing of personal data. ISO/IEC 27001 provides a framework for information security management; ISO/IEC 27017 addresses cloud-specific security controls; and ISO/IEC 27018 focuses on protecting personally identifiable information in public cloud environments. NIST SP 800-144 provides guidance on cloud security and privacy, while NIST SP 800-145 defines cloud service and deployment models (European Parliament and Council of the European Union, 2016; International Organisation for Standardisation, 2015, 2019, 2022; Mell & Grance, 2011).

These requirements highlight the importance of privacy by design and security by design. Compliance should be embedded in the system architecture from the outset rather than added after deployment. This also requires a clear allocation of responsibilities among port authorities, terminal operators, technology providers, and cloud service providers.

Interoperability must likewise be treated as both a governance and compliance requirement. Port access systems may need to connect to Port Community Systems, single windows for logistics, surveillance systems, contractor databases, human resources platforms, and security operations. Although such integration can reduce fragmentation and manual intervention, it also increases the need for robust API governance, data-sharing rules, cybersecurity controls, and contractual clarity. Without these safeguards, interoperability may amplify rather than mitigate operational and security risks (Carlan & Vanelslander, 2021; Sarabia-Jacome et al., 2020; Tijan et al., 2021).

The main business model and regulatory requirements for cloud-enabled access management in smart ports are illustrated in Table 5.

Table 5. Business model and regulatory requirements for cloud-enabled access management

Requirement area	Main requirement	Relevance for smart ports
Value proposition	Demonstrate security, efficiency, traceability and compliance benefits	Ensures that the system responds to operational pain points rather than merely adding technology
Service configuration	Define cloud, hybrid or legacy-integrated deployment models	Supports gradual transition from existing infrastructures to scalable access management
Cost structure	Consider subscription, integration, maintenance, cybersecurity and training costs	Improves financial predictability and supports informed procurement decisions
Risk allocation	Clarify responsibilities for data protection, availability, incident response and vendor dependency	Reduces ambiguity among port authorities, operators and technology providers
GDPR compliance	Ensure lawful, transparent and proportionate processing of personal data	Protects users' rights and strengthens trust in digital access systems
ISO/IEC 27001	Establish an information security management system	Supports systematic governance of information security risks
ISO/IEC 27017	Define cloud-specific security controls and shared responsibilities	Clarifies obligations between cloud providers and port organisations
ISO/IEC 27018	Protect personally identifiable information in cloud environments	Strengthens privacy safeguards in cloud-based access records
NIST cloud guidance	Support cloud risk assessment, security controls and governance principles	Provides structured guidance for secure cloud adoption and incident response
Interoperability governance	Establish API governance, data-sharing rules and integration controls	Enables coordination while limiting cybersecurity and compliance risks

Source: Authors' elaboration

This section also clarifies the transition from access control to access governance. A technically advanced system may offer authentication, dashboards and remote management, but its long-term value depends on whether it can be governed responsibly. For this reason, the proposed framework positions compliance, risk allocation and business model design as integral components of cloud-enabled access management. This provides the basis for the Discussion section, where the findings are interpreted in relation to smart port governance, business model innovation and the transition from legacy systems to integrated digital ecosystems.

5. DISCUSSION

The findings suggest that the value of cloud-enabled access management lies not in the individual components of the proposed framework, but in their alignment across operational needs, technological capabilities, and governance responsibilities. Security, efficiency, scalability, and compliance generate value only when cloud architecture, authentication mechanisms, interoperability, and monitoring tools are configured to address concrete operational challenges and support accountable coordination among port actors. Cloud-enabled access management should therefore be understood as a component of smart port governance rather than as an isolated security technology.

This perspective extends the smart port literature, which has largely focused on automation, the Internet of Things, data exchange, Port Community Systems, digital twins, and logistics optimisation (Pham, 2023; Sarabia-Jacome et al., 2020; Tijan et al., 2021). Access management deserves greater attention because access points represent operational interfaces where identities, permissions, security rules, and digital records converge. It is

therefore relevant not only to physical security, but also to coordination, accountability, and the governance of operational interdependencies.

The findings also reinforce the view that port digitalisation is a socio-technical and governance process rather than a purely technological transition. Smart port development depends on interoperability, stakeholder coordination, and the integration of digital systems into operational routines (Aksentijevic et al., 2021; Carlan & Vanelslander, 2021; Sarabia-Jacome et al., 2020; Tijan et al., 2021). The proposed framework extends this argument by showing that identities and permissions form part of the port's digital coordination architecture. Role-, zone-, time-, and context-based permissions reflect the distribution of operational rights and responsibilities across actors, rather than merely technical system settings.

This interpretation also broadens the scope of Port Community Systems. Existing research primarily emphasises cargo, document, and information flows as mechanisms to reduce fragmentation and improve coordination and competitiveness (Carlan et al., 2016; Koliousis, 2020). The findings suggest that interoperability should also include identities, permissions, and access-event data. However, such integration raises additional concerns regarding the allocation of responsibility, cybersecurity, and cross-organisational data governance. Interoperability should therefore be actively governed rather than assumed to be inherently beneficial.

From a cybersecurity perspective, the benefits of cloud-enabled access management are inseparable from the redistribution of responsibilities among port organisations, technology providers, and cloud service providers. Cloud-based and hybrid architectures may improve visibility, credential lifecycle management, and remote administration, but they also introduce dependencies that require explicit governance arrangements (Chauhan & Shiaeles, 2023; Sun, 2019). The central issue is therefore not whether cloud technologies inherently increase or reduce risk, but how risk ownership, access privileges, incident response, and continuity responsibilities are allocated across organisational boundaries.

The findings also support the relevance of context-sensitive authorisation models. Attribute-Based Access Control and other fine-grained mechanisms are well established in the access-control literature (Hu et al., 2020; Mohamed et al., 2022). Their specific relevance to this study lies in their applicability to port environments characterised by temporary users, differentiated zones and rapidly changing operational conditions. In such settings, static credentials are poorly suited to permissions that may depend on role, organisation, location, schedule, document validity or task. The contribution, therefore, lies not in proposing ABAC as a novel model, but in showing how context-sensitive authorisation supports the governance requirements of complex port ecosystems.

The stakeholder evidence similarly challenges technology-specific approaches to authentication. Rather than privileging a single mechanism, the findings support a portfolio logic in which biometric, mobile and physical credentials are selected according to operational context, risk and continuity requirements. This is particularly relevant where biometric reliability, privacy concerns, or device limitations make exclusive reliance on a single technology problematic (Bast & Yeh, 2024; Parkinson & Khan, 2023). Authentication diversity should therefore be interpreted as both an operational resilience mechanism and a security capability.

This argument leads to a broader principle of technological pragmatism. Cloud-enabled access governance need not rely exclusively on high-cost computer vision or advanced biometrics. RFID, barcode-based identifiers, and other Automatic Identification and Data Capture technologies may serve as effective components of modular architectures, particularly where legacy integration, lifecycle cost, or operational continuity constraints

require more sophisticated solutions. The implication is that technology selection should be problem-driven rather than novelty-driven. The cloud layer can provide a configurable environment for managing heterogeneous credentials and devices without requiring immediate replacement of existing infrastructure.

Auditability should be interpreted with similar caution. Existing studies have explored blockchain-based mechanisms for secure data sharing, privacy protection and tamper-resistant records (Agyekum et al., 2022; Yang et al., 2020). However, the findings do not support blockchain as a default component of cloud-enabled access management. Its relevance is limited to governance contexts that require distributed verification, cross-organisational trust, or strong resistance to record manipulation. Conventional logging mechanisms may be sufficient in many applications. This distinction helps avoid technology-driven implementation without demonstrated operational value.

The study also contributes to research on business model innovation. The key implication is that value creation depends on alignment rather than on service-based delivery alone. A subscription or cloud model does not constitute meaningful innovation if it fails to reduce operational friction, clarify responsibilities or integrate with existing infrastructures. The findings therefore support a broader interpretation of business model innovation in which value proposition, service configuration, cost structure and risk allocation are interdependent (Osterwalder et al., 2014; Teece, 2010). In this context, cloud-enabled access management creates value when technical capabilities are translated into outcomes that stakeholders recognise as operationally relevant.

The stakeholder evidence provides empirical support for this alignment perspective. Authentication failures, access delays, workforce variability, fragmented permissions and limited interoperability represent operational problems rather than abstract technological gaps. Mechanisms such as remote permission management, credential lifecycle control and API integration are valuable only insofar as they address those problems. This reinforces the usefulness of Value Proposition Design as a bridge between stakeholder requirements and system configuration (Osterwalder et al., 2014). It also supports ecosystem-based perspectives on port value creation, which argue that value emerges through coordination among actors rather than through isolated organisational decisions (De Martino, 2021; Tsvetkova & Hellström, 2022).

Operational resilience should likewise be interpreted as a contingent outcome rather than an inherent property of cloud adoption. Cloud-enabled access management may support continuity through remote administration, rapid permission changes and improved visibility, but centralised services may also create connectivity dependencies, concentration risks or vendor-related vulnerabilities. Resilience, therefore, depends on redundancy, fallback arrangements, continuity planning, and clear allocation of responsibility. This explains why hybrid architectures may remain relevant in operationally critical environments.

A central theoretical implication is the distinction between access control and access management. Access control concerns the mechanisms used to grant or deny entry, whereas access management encompasses identities, permissions, credential lifecycles, user categories, zones, exceptions, data responsibilities, and accountability. The findings show that many of the most significant challenges in port environments are organisational rather than device-specific. They arise from coordinating changing user populations, differentiated permissions, multiple systems, and cross-organisational responsibilities. Reframing access management as a governance capability is therefore a principal contribution of this study.

This distinction also clarifies the dual role of interoperability. Technically, interoperability depends on APIs, device compatibility, and integration with legacy infrastructure.

From a governance perspective, it can reduce fragmentation and improve coordination. However, integration may also expand attack surfaces and create uncertainty regarding data ownership, accountability, and incident response. Interoperability is therefore both an operational enabler and a governance challenge, extending the smart port and Port Community System literature to include identities, permissions, and access-event data (Carlan & Vanelslander, 2021; Sarabia-Jacome et al., 2020; Tijan et al., 2021).

The findings further support a gradual approach to digital transformation. Ports commonly operate historically layered systems, heterogeneous devices, and legacy infrastructure. Cloud-enabled access management should therefore not assume immediate system replacement. Hybrid deployment, modular integration, and compatibility with existing technologies may offer more feasible transition pathways, consistent with research emphasising migration planning, organisational readiness, and risk controls (Chauhan & Shiaeles, 2023; Sun, 2019).

Cloud-enabled access management can support smart port transformation under three conditions. First, implementation must address clearly defined operational and governance problems rather than pursue technology adoption for its own sake. Second, systems must be embedded in secure, interoperable, and responsibility-aware governance structures. Third, the business model must align stakeholder value, service configuration, lifecycle costs, compliance, and risk allocation.

The principal theoretical contribution is therefore to position cloud-enabled access management at the intersection of smart port governance, cybersecurity, and business model innovation. Access management is not merely an authentication issue, but a socio-technical coordination challenge involving operational needs, technological capabilities, governance responsibilities, and value creation. The practical contribution is a structured framework that port authorities, terminal operators, and technology providers can use to assess drivers of adoption, implementation requirements, business model considerations, and expected governance outcomes.

6. CONCLUSION

This study examined how cloud-enabled access management can support the transition from fragmented legacy systems to integrated smart port governance. Drawing on a literature review, market benchmarking, stakeholder consultations, and value proposition analysis, it developed a three-layer framework linking adoption drivers, technological enablers, and governance outcomes.

The findings show that cloud-enabled access management can support smart port governance when four conditions are jointly satisfied. First, implementation must respond to clearly defined operational and governance needs, particularly security, efficiency, scalability, and compliance. Second, these needs must be matched with appropriate technological enablers, including cloud architecture, APIs, interoperability, multi-factor authentication, fallback mechanisms, auditability tools, and real-time monitoring. Third, implementation should generate governance outcomes such as traceability, granular access control, reduced manual intervention, interoperability, and operational resilience. Fourth, these elements must be embedded in a coherent business model and regulatory framework that clarifies value creation, deployment, lifecycle costs, risk allocation, and data governance responsibilities.

The study makes three theoretical contributions. First, it extends the smart port literature by positioning access management as part of the digital governance infrastructure of port ecosystems. Although previous research has focused primarily on automation, the Internet of Things, data exchange, and Port Community Systems, identities, permissions, and ac-

cess-event data have received less attention (Pham, 2023; Sarabia-Jacome et al., 2020; Tijan et al., 2021). The findings show that access points are not merely physical barriers, but operational interfaces through which people, assets, rules, and digital records are coordinated.

Second, the study distinguishes access management from access control. While access control concerns the mechanisms used to grant or deny entry, access management encompasses the governance of identities, permissions, credential lifecycles, user categories, zones, exceptions, and accountability. This distinction is especially relevant in ports, where access decisions depend on changing roles, operational conditions, and cross-system interactions.

Third, the study contributes to research on business model innovation by showing that cloud-enabled access management should not be evaluated solely as a technical architecture. Its value depends on the alignment of stakeholder needs, service configuration, cost structures, regulatory compliance, and risk allocation (Osterwalder et al., 2014; Teece, 2010).

Methodologically, the study integrates academic literature, market evidence, stakeholder insights, and design-oriented artefacts within a single analytical structure. The framework is therefore presented as a design-oriented contribution rather than a universally validated model.

In practical terms, the framework can assist port authorities in assessing traceability, interoperability, differentiated permissions, and resilience; support terminal operators and logistics firms in reducing manual procedures and improving credential management; guide technology providers towards modular and interoperable solutions; and help policymakers embed privacy, cybersecurity, and responsibility allocation into system design from the outset.

The findings also support a pragmatic approach to technology selection. Cloud-enabled access management does not require exclusive reliance on advanced biometrics, computer vision or other high-complexity technologies. RFID, barcode-based identification, mobile credentials, cards and biometric methods may coexist within modular architectures. The relevant criterion is not technological novelty, but the capacity of the selected configuration to respond to risk, throughput, environmental conditions, interoperability requirements and lifecycle cost.

Several limitations should be acknowledged. First, the study is exploratory and design-oriented and does not provide a longitudinal evaluation of a fully deployed cloud-enabled access management system. Second, the literature review was conducted to support conceptual integration and framework development rather than as a fully systematic review or meta-analysis. Third, market benchmarking identified recurring capabilities and business model patterns but did not compare or rank commercial providers. Fourth, the stakeholder component involved six participants across nine consultation meetings and therefore does not statistically represent the wider population of port actors. Finally, the framework emerged from a specific port-innovation context and may require adaptation based on port scale, governance model, digital maturity, regulatory conditions, and existing infrastructure.

Future research should therefore test and refine the framework in different port environments. Comparative studies could examine whether drivers of adoption and technology enablers vary across large gateway ports, regional ports, and specialised terminals. Longitudinal studies could evaluate effects on access delays, incident response, user experience, compliance performance and operational continuity. Further research could also explore the role of artificial intelligence, anomaly detection, predictive analytics and digital twins in access management. Attention should be given to the ethical and legal implications of

biometric processing, automated access decisions, data retention and cross-organisational data sharing.

In conclusion, cloud-enabled access management can contribute to the transformation of smart ports when designed as a secure, interoperable, and value-oriented governance capability. Its strategic relevance lies not merely in digitising access control, but in improving how port ecosystems coordinate identities, permissions, data, responsibilities and operational risk across heterogeneous actors and systems. By integrating security, efficiency, scalability, compliance and resilience, cloud-enabled access management can become an important component of contemporary smart port governance.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the author(s) used Scite.ai and SciSpace.ai to organise and interact with documents. After using these tools/services, the author(s) reviewed and edited the content as needed and took full responsibility for the publication's content.

Conflicts of interest

The authors declare no conflicts of interest.

Funding

Content produced within the scope of the Agenda "NEXUS - Pacto de Inovação – Transição Verde e Digital para Transportes, Logística e Mobilidade", financed by the Portuguese Recovery and Resilience Plan (PRR), with no. C645112083-00000059 (investment project n.º 53)

Acknowledgment

NECE - Research Centre for Business Sciences funded by the Multiannual Funding Program of R&D Centers of FCT—Fundação para a Ciência e Tecnologia, Portugal, under Grant number UID/04630/2025, DOI: 10.54499/UID/04630/2025

REFERENCES

Agyekum, K. O.-B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2022). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. *IEEE Systems Journal*, *16*(1), 1685–1696. https://doi.org/10.1109/JSYST.2021.3076759

Aksentijevic, S., Tijan, E., Panjako, A., & Mrcela, G. (2021). Digitalization of Port Access Control: Case Study Port of Šibenik. *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1294–1299. https://doi.org/10.23919/MIPRO52101.2021.9596650

Barasti, D., Troscia, M., Lattuca, D., Tardo, A., Barsanti, I., & Pagano, P. (2021). An ICT Prototyping Framework for the "Port of the Future". *Sensors*, *22*(1), 246. https://doi.org/10.3390/s22010246

Bast, C., & Yeh, K.-H. (2024). Emerging Authentication Technologies for Zero Trust on the Internet of Things. *Symmetry*, *16*(8), 993. https://doi.org/10.3390/sym16080993

Carlan, V., Sys, C., & Vanelslander, T. (2016). How port community systems can contribute to port competitiveness: Developing a cost–benefit framework. *Research in Transportation Business & Management*, *19*, 51–64. https://doi.org/10.1016/j.rtbm.2016.03.009

Carlan, V., & Vanelslander, T. (2021). Economic Aspects of Introducing Artificial Intelligence Solutions in Logistics and Port Sectors: The Data Entry Case. *Frontiers in Future Transportation*, *2*. https://doi.org/10.3389/ffutr.2021.710330

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), 422–450. https://doi.org/10.3390/network3030018

Chenail, R. (2016). Bringing Method to the Madness: Sandelowski and Barroso's Handbook for Synthesizing Qualitative Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2009.2820

Creswell, J. W. (2009). *Research Design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). SAGE Publications. Inc. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf, accessed on 24/05/2024.

de Langen, P. W., Sornn-Friese, H., & Hallworth, J. (2020). The Role of Port Development Companies in Transitioning the Port Business Ecosystem; The Case of Port of Amsterdam's Circular Activities. *Sustainability*, *12*(11). https://doi.org/10.3390/su12114397

De Martino, M. (2021). Value Creation for Sustainability in Port: Perspectives of Analysis and Future Research Directions. *Sustainability*, *13*(21), 12268. https://doi.org/10.3390/su132112268

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919

Ding, W., Yan, Z., & Deng, R. H. (2020). Privacy-Preserving Data Processing with Flexible Access Control. *IEEE Transactions on Dependable and Secure Computing*, *17*(2), 363–376. https://doi.org/10.1109/TDSC.2017.2786247

Dubey, S., & Rai, P. K. (2021). A Review of Cloud Service Security with Various Access Control Methods. *International Journal of Computer Science and Mobile Computing*, *10*(3), 39–45. https://doi.org/10.47760/ijcsmc.2021.v10i03.005

El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*, *29*(1), 223–246. https://doi.org/10.1007/s11831-021-09573-y

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. L 119, 1–88. *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, accessed on 04/05/2025.

Ferrari, E. (2010). Access Control in Data Management Systems. *Synthesis Lectures on Data Management*, *2*(1), 1–117. https://doi.org/10.2200/S00281ED1V01Y201005DTM004

Garzia, F., Sammarco, E., & Cusani, R. (2009). *Integrated access control system for ports*. 313–323. https://doi.org/10.2495/SAFE090301

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research1. *MIS Quarterly*, *28*(1), 75–106. https://doi.org/10.2307/25148625

Hu, V. C., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A. (2020). *General access control guidance for cloud systems*. https://doi.org/10.6028/NIST.SP.800-210

International Organization for Standardization. (2015). *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO*. https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027017-2015.pdf

International Organization for Standardization. (2019). *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information in public clouds acting as PII processors. ISO*. https://www.glocertinternational.com/services/iso-certifications/iso-27018, accessed on 04/07/2026.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022* Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf, accessed on 04/07/2026.

Koliousis, I. (2020). A conceptual framework that monitors port facility access through integrated Port Community Systems and improves port and terminal security performance. *International Journal of Shipping and Transport Logistics*, *12*(4), 251. https://doi.org/10.1504/IJSTL.2020.10029955

Marinov, Y. A., & Lisenyi, Y. V. (2024). The Role of Cloud Technologies in the Management of Logistics Operations. *Business Inform*, *9*(560), 94–101. https://doi.org/10.32983/2222-4459-2024-9-94-101

Marjohan, M., Satria, R., Sunanto, S., & Ishwara, P. I. (2026). The Implementation of Financial Technology in Digital Investment Applications for the Citizens of Indonesia. *ECONOMICS - Innovative and Economic Research Journal, 14*(2), 393-413. https://doi.org/10.2478/eoik-2026-0042

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing*. https://doi.org/10.6028/NIST.SP.800-145

Miles, M. B., Huberman, M. A., & Saldaña, J. (2013). *Qualitative-Data-Analysis* (Helen Salmon, Ed.; Third edition). SAGE Publications, Inc. https://www.metodos.work/wp-content/uploads/2024/01/Qualitative-Data-Analysis.pdf, accessed on 10/05/2026.

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*, *3*(4), 414–430. https://doi.org/10.1108/MABR-08-2018-0026

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*, *18*(2–3), 156–180. https://doi.org/10.1108/IJWIS-04-2022-0077

Mussina, S., Khussainova, Z., Atabayeva, A., & Kazbekov, T. (2026). Estimating the Effects of Macroeconomic Factors on Net Migration: A 2SLS Approach in Panel Data. *ECONOMICS - Innovative and Economic Research Journal, 14*(2), 415 - 433. https://doi.org/10.2478/eoik-2026-0043

Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. *Concurrency and Computation: Practice and Experience*, *31*(3). https://doi.org/10.1002/cpe.4364

Nguyen, H. P., Nguyen, P. Q. P., Nguyen, D. K. P., Bui, V. D., & Nguyen, D. T. (2023). Application of IoT Technologies in Seaport Management. *JOIV : International Journal on Informatics Visualization*, *7*(1), 228. https://doi.org/10.30630/joiv.7.1.1697

Nguyen, M. H., Tran, T. M. T., & Pham, S. A. (2026). Shock, Skills, or Sales? Disentangling the Drivers of Green Action in ASEAN Enterprises. *ECONOMICS - Innovative and Economic Research Journal, 14*(2), 269-291. https://doi.org/10.2478/eoik-2026-0036

Osterwalder, A., Pigneur, Y., Bernarda, G., Smith, A., & Papadakos, T. (Designed by). (2014). *Value proposition design: How to create products and services customers want* (Ed. K. R. S. Wiley, Ed.). https://content.e-bookshelf.de/media/reading/L-3223510-409f7d175c.pdf, accessed on 07/05/2026

Parkinson, S., & Khan, S. (2023). A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective. *ACM Computing Surveys*, *55*(6), 1–28. https://doi.org/10.1145/3533703

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pham, T. Y. (2023). A smart port development: Systematic literature and bibliometric analysis. *The Asian Journal of Shipping and Logistics*, *39*(3), 57–62. https://doi.org/10.1016/j.ajsl.2023.06.005

Sarabia-Jacome, D., Palau, C. E., Esteve, M., & Boronat, F. (2020). Seaport Data Space for Improving Logistic Maritime Operations. *IEEE Access*, *8*, 4372–4382. https://doi.org/10.1109/ACCESS.2019.2963283

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2023). *Research Methods for Business Students* (9th ed.). Pearson Education Limited. https://www.researchgate.net/publication/240218229_Research_Methods_for_Business_Students, accessed on 16/04/2025.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access*, *7*, 147420–147452. https://doi.org/10.1109/ACCESS.2019.2946185

Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning*, *43*(2–3), 172–194. https://doi.org/10.1016/j.lrp.2009.07.003

Tijan, E., Jović, M., Panjako, A., & Žgaljić, D. (2021). The Role of Port Authority in Port Governance and Port Community System Implementation. *Sustainability*, *13*(5), 2795. https://doi.org/10.3390/su13052795

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tsvetkova, A., & Hellström, M. (2022). Creating value through autonomous shipping: an ecosystem perspective. *Maritime Economics & Logistics*, *24*(2), 255–277. https://doi.org/10.1057/s41278-022-00216-y

Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud. *IEEE Access*, *8*, 70604–70615. https://doi.org/10.1109/ACCESS.2020.2985762