frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 31 July 2025
DOI 10.3389/fcomp.2025.1572009

Check for updates

OPEN ACCESS

EDITED BY
Nicholas Kolokotronis,
University of Peloponnese, Greece

REVIEWED BY
Chengzu Dong,
Lingnan University, Hong Kong SAR, China
Huida Zhao,
Shenzhen University, China

*CORRESPONDENCE
Aristeidis Farao
✉ arisfarao@unipi.gr

RECEIVED 06 February 2025
ACCEPTED 09 July 2025
PUBLISHED 31 July 2025

CITATION
Farao A, Zarras A, Voudouris A, Paparis G and Xenakis C (2025) B2SAPP: blockchain based solution for maritime security applications. *Front. Comput. Sci.* 7:1572009.
doi: 10.3389/fcomp.2025.1572009

B2SAPP: blockchain based solution for maritime security applications

Aristeidis Farao[1,2]*, Apostolis Zarras[1,3], Anastassis Voudouris[1], Georgios Paparis[1] and Christos Xenakis[1]

[1]Department of Digital Systems, University of Piraeus, Piraeus, Greece, [2]InQbit Innovations SRL., Bucharest, Romania, [3]Foundation for Research and Technology – Hellas, Heraklion, Greece

The digitization of the maritime industry is accelerating rapidly. However, critical infrastructures face greater cyber security risks as they become more interconnected. As digital technologies advance, so do the adversaries that exploit them. The threat posed by cyber criminals and state-sponsored actors is more significant than ever, and the shipping sector's central role in global supply chains makes it a prime target for cyberattacks. This article introduces B2SAPP, an innovative privacy-preserving framework designed to deliver robust security and privacy protections for maritime operations. By leveraging Hyperledger Aries and Hyperledger Fabric, B2SAPP provides reliable authorization of the entities involved in the maritime ecosystem, as well as secure storage for Vessel operational data. We have implemented the core components of B2SAPP and conducted a quantitative performance assessment, demonstrating its feasibility. We further validate its security and privacy attributes, confirming that B2SAPP meets its design objectives. In summary, B2SAPP represents a forward-thinking solution poised to enhance cyber insurance against evolving cyber threats, offering a promising avenue for safeguarding organizations and policyholders in the digital era.

KEYWORDS

blockchain, self-sovereign identity, privacy preserving, maritime, smart contracts

1 Introduction

The maritime sector, a global trade and connectivity cornerstone, faces escalating cybersecurity threats that jeopardize operational integrity and efficiency. Recent advances in satellite technology and IoT integration have modernized maritime communication systems, expediting decision-making and facilitating real-time data transmission (Raza et al., 2023). Nevertheless, this progress has enlarged the attack surface (Yu et al., 2023; Danilin et al., 2021), exposing crucial systems to threats like spoofing (Spravil et al., 2023), jamming (Liu et al., 2023a), unauthorized access (Chernyi et al., 2018), and ransomware attacks (Potamos et al., 2023).

A series of recent incidents evidence the importance of addressing cybersecurity concerns in the maritime sector. For instance, at Singapore shipbuilder Sembcorp Marine, unauthorized access to the IT network via third-party software underscored the necessity for robust security protocols despite the absence of substantial financial consequences (Executive, 2025). Likewise, Voyager Worldwide, a maritime IT solutions provider serving over 25% of global shipping organizations, experienced a significant breach in December 2022 that disabled all systems and allegedly enabled further intrusions via IT service providers (Chambers, 2025). In January 2023, the group behind the ransomware PLAY compromised a Marine IT firm in addition to four other shipping companies, subsequently releasing stolen data on the dark web (The Record, 2025a). In December 2022, the Port of Lisbon suffered a major cyberattack by the "Lock Bit" group, which disabled operations for four days and threatened to disclose sensitive information unless a $1.5 million ransom was paid (The Record, 2025b). In January 2023, Norwegian shipping classification society DNV experienced a ransomware assault affecting 70 clients operating ∼1,000 Vessels, around 15% of its overall fleet (The Record, 2024).

The aforementioned occurrences highlight the urgent need for modern and comprehensive cybersecurity measures tailored to the maritime sector. Beyond ensuring navigation and operational safety, such measures are critical for safeguarding sensitive data, preserving the continuity of global supply chains, and mitigating substantial financial losses, reflecting the extensive vulnerabilities inherent in marine systems. Although cybersecurity policies have advanced considerably, existing solutions frequently fail to address the complex and evolving threats unique to maritime ecosystems (Clavijo Mesa et al., 2024).

To tackle these issues, we propose a Blockchain-based solution, B2SAPP, which integrates smart contracts and Self-Sovereign Identity (SSI) technology to confront maritime cybersecurity challenges. The framework leverages Hyperledger Fabric's permissioned Blockchain to provide secure, immutable, and transparent storage of maritime operational data, while smart contracts automate critical functionalities such as anomaly detection and response. SSI, implemented through Hyperledger Aries, delivers a robust identity management mechanism for Vessels, Command and Control Centers (CCCs), and personnel using Verifiable Credentials (VCs) and Decentralized Identifier (DID).

Overall, B2SAPP enhances security, operational efficiency, and privacy by mitigating threats like spoofing, signal interference, and data corruption. In essence, smart contracts enable real-time threat identification and automated operations like credential issuance and verification, while encryption safeguards sensitive information, preserving trust and protecting against unauthorized access. This comprehensive approach not only addresses current challenges but also establishes the framework as a future-proof solution that can adapt to the constantly evolving maritime cybersecurity landscape.

In summary, we make the following main contributions:

- We introduce the B2SAPP framework, leveraging Blockchain and SSI technologies to enhance privacy, security, and operational efficiency in maritime operations.
- We leverage smart contracts for real-time anomaly detection and automated operations, including credential issuance, verification, and secure data sharing among Vessels, command centers, and satellites.
- We perform a quantitative evaluation of the system's performance and resilience, demonstrating the feasibility of B2SAPP in addressing maritime cybersecurity challenges and its effectiveness against common cyber threats.

The remainder of this paper is organized as follows. Section 2 offers an in-depth examination of the proposed satellite–maritime communication ecosystem, discussing operational workflows, key components, and defining cybersecurity threats and requirements. Next, Section 3 details the technological foundation of the B2SAPP framework, highlighting its backbone infrastructure based on Hyperledger Fabric and Hyperledger Aries. Section 4 analyzes the architectural overview of the B2SAPP ecosystem together with the roles of the participant entities. In Section 5, we outline the operational processes within the B2SAPP framework, including Verifiable Credential issuance, verification, and anomaly detection mechanisms, as well as the role of smart contracts in securing data exchanges and enforcing commands. Section 6 evaluates B2SAPP's performance through metrics such as credential issuance time, Blockchain throughput, and overall system resilience, an analysis of the security protocols and encryption methods used, alongside a security analysis of common threats. In Section 7, we critically assess the limitations of the B2SAPP framework and propose potential enhancements. Next, Section 8 reviews prior research in satellite and maritime communication systems, highlighting advancements in Blockchain-based solutions and the need for integrating SSI for secure identity management. Finally, Section 9 concludes the paper by summarizing the framework's key contributions and suggesting directions for future research to advance maritime cybersecurity.

2 Decentralized satellite ecosystem with smart contracts and self-sovereign identity

This section concisely analyses the most prevalent threats confronting maritime satellite communication ecosystems, their operational context, and an associated threat model. Additionally, we outline the security and privacy requirements needed to ensure the trustworthy operation of frameworks functioning within this ecosystem.

2.1 Ecosystem overview

The modern maritime ecosystem is transforming into a sophisticated and secure environment by integrating advanced satellite communication, Blockchain technology, smart contracts, and SSI (Farao et al., 2024). This hybrid ecosystem improves traditional maritime operations by enabling real-time, secure, and automated data management among Vessels, command centers, and satellites. As a result, it promotes seamless coordination and enhances decision-making capabilities. The ecosystem includes the following components.

Vessels. Vessels are at the heart of maritime operations, responsible for transporting cargo and carrying out essential missions. They are equipped with advanced satellite communication systems that allow them to continuously gather and transmit important data, such as GPS coordinates, weather conditions, and equipment status. By utilizing VCs issued by the Nautical Operational Center (NOC), Vessels securely store this data on a Blockchain, ensuring its integrity and availability for authorized stakeholders.

Additionally, smart contracts integrated into the Blockchain monitor the Vessel's data and automatically trigger alerts or actions whenever specific conditions are met.

CCC. As the central hub of maritime operations, the CCC oversees all fleet activities. It processes real-time data from Vessels, identifies potential risks, and coordinates responses to ensure safe and efficient maritime operations. The CCC also acts as a verifier within the Blockchain ecosystem, validating the identity and credentials of Vessels before they engage in transactions on the Blockchain. By utilizing smart contracts, the CCC automates decision-making and provides an immutable audit trail, which enhances accountability and transparency.

Satellite. Satellites function as communication relays, ensuring continuous connectivity between Vessels and the CCC, even in remote ocean areas. They facilitate the secure transmission of data, including text, voice, and video, while also supporting synchronization by providing accurate timing signals across the maritime network. This precise timing alignment is essential for coordinated operations, especially in missions that demand strict temporal accuracy and data consistency.

NOC. The NOC plays a crucial role in the Blockchain network as a Hyperledger Aries issuer. It issues VCs to Vessels and CCC personnel based on verified identity attributes. These credentials provide secure, privacy-preserving access to data stored on the Blockchain, ensuring that only authorized entities have the ability to read from or write to it. Additionally, the NOC oversees the overall cybersecurity of the ecosystem, detecting threats and distributing alerts to help mitigate risks.

3rd-party service providers. As the ecosystem expands, the demand for specialized software and services is expected to increase. 3rd-party providers may create applications that enhance the Blockchain-based maritime ecosystem with advanced data analytics, cybersecurity solutions, and maintenance scheduling systems. They could also offer services that integrate smoothly with existing maritime operations, adding value by customizing solutions to meet specific needs.

Regulatory and compliance authorities. To ensure compliance with legal and regulatory standards, relevant authorities may monitor the network. They could oversee international maritime laws, cybersecurity requirements, and environmental regulations. By connecting with the Blockchain, these authorities can access operational data in real time, which improves auditing efficiency and enhances enforcement procedures.

This decentralized maritime satellite communication ecosystem, strengthened by Blockchain technology, smart contracts, and SSI, represents a significant advancement in maritime operations. The combination of these technologies creates a secure, transparent, and efficient environment that facilitates real-time decision-making and coordination within the maritime network.

By enabling secure data exchanges, automating responses to critical events, and ensuring the integrity and traceability of maritime operations, this ecosystem opens new avenues for innovative business models and operational efficiencies. Involving third-party service providers and regulatory authorities further enhances the network, ensuring resilience and adaptability to evolving challenges and opportunities.

Ultimately, the comprehensive integration of these advanced technologies within the maritime sector not only improves security and operational efficiency but also fosters a dynamic and flexible ecosystem capable of accommodating future innovations and meeting stakeholder demands.

2.2 Classic maritime satellite communication operations and cybersecurity threats

This section presents a fundamental maritime operational scenario in which Vessels, CCC, and satellites cooperate to achieve a shared mission. We first describe the system's core components and workflows, followed by the key cybersecurity threats this satellite–maritime communication ecosystem faces.

2.2.1 Maritime operation scenario

In this maritime satellite communication system, *Vessels* are equipped with advanced navigational instruments that rely on Global Navigation Satellite Systems (GNSS) for accurate positioning. Onboard sensors capture various data: meteorological readings from specialized weather instruments, cargo status via IoT-enabled devices, and equipment health assessments through condition monitoring systems. These data points are compiled into standardized messages (e.g., using the NMEA 0183 protocol) and transmitted to the *CCC* through a satellite link, ensuring robust communication even in challenging conditions. Once the CCC receives these data, a sophisticated analytical process detects operational patterns and applies anomaly detection algorithms to flag potential issues in real time. The outcomes of these analyses are then sent back to the Vessels.

The *satellite*, located in geostationary orbit for consistent coverage, acts as a communication relay, leveraging multiple access techniques and advanced modulation schemes to facilitate bandwidth-efficient data transfer. Timing synchronization is upheld via atomic clocks on the satellite, which periodically broadcast synchronization signals to Vessels, creating a cohesive temporal framework for the entire system. The Vessels, in turn, adjust their activities based on the CCC's directives. Additionally, they may coordinate with one another through established maritime communication protocols for Vessel-to-Vessel interactions.

This maritime satellite communication ecosystem integrates advanced technologies such as GNSS, IoT, sophisticated communication protocols, machine learning, and precise timing synchronization. These components facilitate real-time data exchange, enabling better decision-making and synchronized operations. This ultimately enhances the efficiency and safety of maritime missions.

2.2.2 Cybersecurity threats

Despite the technical sophistication of this maritime satellite communication environment, it is essential to acknowledge the cybersecurity risks accompanying interconnected, data-driven systems. The following list highlights key threats that can compromise the maritime satellite communication ecosystem (Clavijo Mesa et al., 2024; Akpan et al., 2022; Afenyo and Caesar, 2023).

CH1 —Spoofing and jamming: Spoofing involves broadcasting deceptive signals to manipulate satellite data, leading to compromised navigation data onboard maritime Vessels. Consequently, Vessels may stray from their intended routes, raising collision or navigational error risks. Jamming attacks, in contrast, intentionally disrupt satellite communications, potentially resulting in temporary or prolonged communication losses. During emergencies, such disruption impedes distress signals, endangering prompt response efforts. The repercussions include immediate safety concerns, operational downtime, and elevated susceptibility to maritime security threats (Tedeschi et al., 2022; Tabish and Chaur-Luh, 2024).

CH2—Unauthorized access: Adversaries who gain unauthorized entry to navigation, communication, or control systems can exploit vulnerabilities with potentially dire outcomes. Attackers may manipulate navigation functions, deliberately redirecting Vessels from their routes and increasing the likelihood of collisions, groundings, or navigational errors. Moreover, interference with communication systems hampers essential data exchanges between Vessels and onshore authorities, adversely affecting emergency coordination. Breaching control systems also jeopardize Vessel safety, cargo integrity, and crew welfare (Tabish and Chaur-Luh, 2024; Afenyo and Caesar, 2023).

CH3—Data interception: The interception of crucial data can cause far-reaching consequences, ranging from security breaches to theft and illicit use. In an interconnected maritime setting, where real-time communication is vital, such interceptions threaten data confidentiality and integrity (Tabish and Chaur-Luh, 2024; Afenyo and Caesar, 2023).

CH4—Malware and ransomware: A successful malware or ransomware attack can disrupt critical Vessel operations, affecting navigation systems, engine controls, and beyond. Sensitive data, such as cargo manifests or communication logs, may be compromised, enabling unauthorized access or nefarious use. Ransomware adds the risk of extortion, where attackers demand payment to restore critical systems, potentially paralyzing maritime activities until these demands are met (Tabish and Chaur-Luh, 2024).

CH5—Supply chain vulnerabilities: The fragility of the maritime supply chain arises from its dependence on a complex and globally distributed ecosystem of hardware, software, and service providers. Even a single compromised component, whether a navigation system or embedded firmware, can introduce systemic vulnerabilities across vessels and communication infrastructure. This fragility is compounded by the limited visibility maritime organizations often have into third-party suppliers and the absence of standardized verification mechanisms for hardware and software integrity. These weaknesses offer exploit opportunities for malicious actors to infiltrate and manipulate critical infrastructure. Potential impacts span unauthorized access, data breaches, and malicious code injection. Strengthening supply chain integrity is pivotal to preventing such breaches and sustaining robust communication systems (Polatidis et al., 2018; Tabish and Chaur-Luh, 2024; Afenyo and Caesar, 2023).

CH6—Insider threats: Malicious insiders motivated by financial gain or other factors may deliberately manipulate systems, compromise confidential data, and disrupt core operations. Conversely, well-intentioned insiders can inadvertently cause severe disruptions through misconfiguration or errors. The repercussions include financial losses, reputational harm, and weakened maritime security (Tabish and Chaur-Luh, 2024).

CH7—Denial of Service (DoS) attacks: Overloading communication or navigation systems with excessive requests can trigger widespread disruption. Compromised communication channels undermine critical data exchanges between Vessels and shore facilities, reducing situational awareness and coordination. Simultaneously, navigation or satellite-based systems may be impaired, preventing accurate position, course, and speed readings, thus posing risks to crew safety and maritime assets (Tabish and Chaur-Luh, 2024).

CH8—Data logging: Insufficient or absent logging strategies pose a significant cybersecurity risk, as navigation, communication, and other system activities may remain unmonitored. Detailed audit logs are essential for forensic investigations into cyber-physical attacks; without them, it becomes more challenging to detect anomalous or malicious activities promptly (Tabish and Chaur-Luh, 2024).

Other potential threats, such as *Cyber-physical attacks* and *Social Engineering Attacks*, have been examined. However, this study does not address these issues, as they cannot be sufficiently tackled using the current capabilities of Blockchain, Smart Contracts, or SSI, the core technologies that underpin our proposed architecture.

2.3 Security and privacy requirements

The satellite maritime ecosystem combines elements of satellite and maritime technology, leading to shared security and privacy requirements from both domains. This work is the first to define the necessary security and privacy requirements for solutions, such as architectures, frameworks, and schemes, intended for use in the maritime sector, as existing literature lacks this focus. After considering the satellite maritime ecosystem built on Blockchain and relevant research, the following security and privacy requirements have been established.

2.3.1 Security requirements

The definition of security requirements is crucial for identifying potential cybersecurity threats that a satellite maritime ecosystem may face. This proactive approach aims not only to reduce the likelihood of cybersecurity incidents, such as data breaches, but also to minimize their potential consequences. Below, we outline the security requirements that should be addressed by satellite maritime systems built on Blockchain technology.

S1—Data integrity: Data within the Blockchain, shared among involved entities, must be protected from alteration and duplication.

S2—Non-repudiation: All parties involved should be held accountable for their actions and cannot deny them.

S3—Authorization and access control: Access to Blockchain-stored data should only be granted to legitimate entities registered within the respective ecosystem.

S4—Accountability: All parties involved should be held accountable for their actions.

S5—Data confidentiality: Data collected must be accessible only to authorized entities. No entities should collaborate to obtain information.

2.3.2 Privacy requirements

The privacy requirements of B2SAPP are crafted to ensure secure handling of sensitive data while maintaining the confidentiality and anonymity of entities within the maritime ecosystem. This approach addresses both regulatory compliance and stakeholder trust.

P1—Data minimization: Only the minimum amount of data should be stored and exchanged among the entities.

P2—Privacy-preserving data accumulation: Data exchange among participants must occur in a secure and privacy-preserving manner to protect sensitive information from unauthorized disclosure or modification.

2.4 Threat model

The threat model for the satellite maritime ecosystem built on Blockchain relies on the interactions among participating entities and is based on several key assumptions. First, adversaries may attempt to steal or spoof the identities of Vessels or personnel from the CCC. This could allow them unauthorized access to the system and enable manipulation of Vessel data stored on the Blockchain. Such breaches might also result in the issuance of false commands by unauthorized individuals or provide access to sensitive information. Additionally, insiders like disgruntled employees could misuse their privileges to access confidential data, alter records, or sabotage operations within the Blockchain. This poses a risk to critical systems and can disrupt maritime activities. Furthermore, communications between Vessels and the CCC are vulnerable to interception and eavesdropping, potentially exposing operational plans, compromising confidentiality, or granting adversaries access to essential systems. Finally, another significant concern is the injection of false or misleading data into the Blockchain, which could lead to incorrect decisions at the CCC or result in erroneous actions by the Vessels.

3 Backbone infrastructure

This section provides a clear explanation of the technological foundations of B2SAPP, which offers a decentralized and privacy-focused solution for the satellite ecosystem. B2SAPP is built on reliable and well-established technologies recognized for their strong security and privacy features, specifically Hyperledger Fabric and Hyperledger Aries.

3.1 Hyperledger fabric

Hyperledger Fabric (Voudouris et al., 2024) is an open-source permissioned distributed ledger technology (DLT) platform specifically designed for applications in enterprise environments. It adheres to businesses' rigorous standards and requirements and operates under the auspices of the Hyperledger initiative, which is governed by the Linux Foundation.

Several notable characteristics distinguish Hyperledger Fabric. Firstly, as a permissioned network, it ensures that participants are known entities possessing defined roles and privileges. This differs significantly from public Blockchains, which permit unrestricted access to any participant. Additionally, Hyperledger Fabric facilitates the establishment of exclusive "channels," wherein transactions remain confidential among authorized parties, guaranteeing that sensitive information is disclosed only to those with a legitimate need for access.

Furthermore, Hyperledger Fabric employs smart contracts to encode business regulations within the network. Numerous implementations already exist, allowing for the programming of smart contracts using general-purpose programming languages. The platform's highly modular design enables network architects to integrate preferred implementations for critical components such as consensus mechanisms and membership services. Finally, Hyperledger Fabric performs better in managing elevated transaction rates than traditional Blockchain solutions and can scale efficiently to accommodate a more significant number of nodes within a network.

3.2 Hyperledger aries

Hyperledger Aries provides a comprehensive framework and set of tools for generating, transmitting, and storing verifiable digital credentials, commonly referred to as VCs. It primarily focuses on facilitating direct messaging between individuals, enabling secure and decentralized information exchanges grounded in self-sovereign identity principles. This innovative approach removes the reliance on external validation processes typically associated with identity management, thereby granting users enhanced control over their data.

The platform supports selective disclosure, allowing users to share only the essential information required for specific transactions. A noteworthy feature of Hyperledger Aries is its integration of Zero-Knowledge Proofs (ZKPs). This advanced cryptographic protocol verifies specific attributes, such as legal age, without revealing the underlying information, such as date of birth. This ensures privacy while still fulfilling regulatory requirements.

In addition to managing digital credentials, Hyperledger Aries enables encrypted and decentralized peer-to-peer communication through the Decentralized Identifier Communication (DIDComm) [World Wide Web Consortium (W3C), 2025] protocol. This facilitates confidential and ongoing interactions between parties, utilizing DIDs to establish privacy without usernames or passwords. This user-friendly characteristic helps maintain dynamic and secure digital connections. Moreover, the platform extends beyond simple credential exchanges; it proactively manages credential lifecycles, keeps users informed about credential revocations, and supports a robust messaging system that enhances user interaction and digital identity management.

4 Architectural overview and roles

We now provide a brief overview of the technological foundation of B2SAPP, which offers a decentralized and privacy-focused solution for the satellite ecosystem (see Figure 1). B2SAPP is built upon strong and proven technologies that are well-known for their security and privacy features, particularly Hyperledger Fabric and Hyperledger Aries.

The B2SAPP architecture exemplifies an advanced system that integrates traditional maritime satellite communication with contemporary Blockchain technology, smart contracts, and SSI. This integration facilitates the development of a secure, decentralized maritime communication network, thereby enhancing both operational efficiency and security. This section offers a detailed overview of the infrastructure and technical components comprising the backbone of the B2SAPP ecosystem while recommending additional considerations to further fortify the system's resilience and functionality.

The *CCC* functions as the central coordinating entity responsible for overseeing Vessel operations, managing potential risks, coordinating emergency actions, and ensuring safety at sea. It operates as a Hyperledger Aries verifier, validating the VCs provided by Vessels to confirm the authenticity of their identities and operational permissions. The CCC employs the Maritime Blockchain to analyze synchronized data, including Vessel positions, navigation logs, and performance metrics, which assists in maintaining effective oversight of fleet activities. Personnel at the CCC utilize their VCs to securely connect to the Blockchain and collaborate with both Vessels and the NOC.

The *satellite* enables uninterrupted data exchange between Vessels and the CCC, ensuring continuous communication regardless of location. It transmits Vessel telemetry data, synchronization timestamps, and emergency signals to the CCC

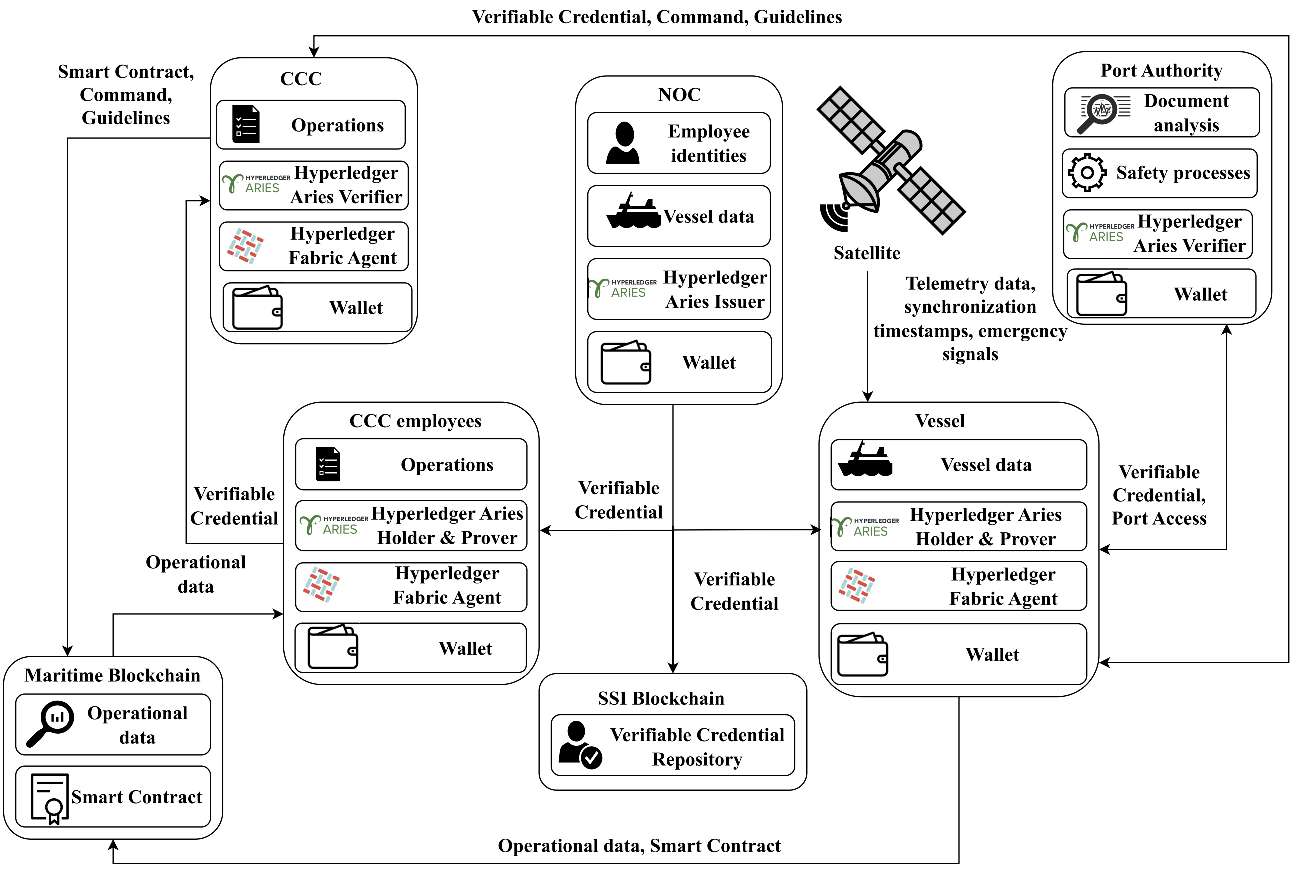

FIGURE 1
B2SAPP blueprint.

while receiving updated mission directives and safety notifications. This satellite infrastructure is critical in facilitating real-time data sharing in remote areas or open seas where traditional communication methods may be unavailable.

Each *Vessel* plays a vital role within the ecosystem, as it is responsible for navigating the seas, transporting cargo, or fulfilling mission objectives. Equipped with Time Synchronization Units (TSUs) and SSI-enabled VCs, Vessels can securely share their identities and operational information with the CCC and the Blockchain. Vessels transmit real-time telemetry, synchronization logs, and emergency alerts through the satellite network while receiving mission updates, safety guidance, and incident coordination details from the CCC. By utilizing VCs, Vessels ensure secure and validated data sharing, fostering trust throughout the ecosystem.

The *CCC employees* are integral to supervising Vessel operations, analyzing Blockchain data, and managing incidents as they arise. They use their SSI-enabled VCs to access sensitive information within the maritime Blockchain, ensuring that only authorized individuals can interact with the system. Their responsibilities include verifying Vessel credentials, assessing risks, and managing emergency responses. Additionally, the VCs enhances accountability, as employee actions are permanently documented on the Blockchain. This structured approach mitigates insider threat risk and promotes data management transparency.

The *NOC* serves as the authoritative body responsible for issuing VCs for Vessels and CCC employees. Before issuing credentials, it verifies identity details (Dong et al., 2021, 2024, 2020), such as Vessel registrations and employee roles. The NOC disseminates credential schemas and validation keys to the SSI Blockchain, thereby promoting reliability throughout the ecosystem. Furthermore, it collaborates with the CCC to provide operational insights and ensure that credentials comply with maritime regulations. The NOC is essential in establishing and maintaining the trust framework necessary for safe and effective maritime operations.

The *Maritime Blockchain* functions as a reliable and distributed ledger, preserving operational and synchronization information from Vessels. It also stores verified interactions and incident report records, facilitating real-time oversight of Vessel activities and generating automated notifications.

The *SSI Blockchain* supports the identity management system, enabling secure and private authorization/authentication for both Vessels and CCC employees who issue and verify Hyperledger Aries VCs. This capability fosters seamless collaboration, allowing CCC personnel and Vessels to authenticate and interact with one another while upholding stringent standards of privacy and security.

Finally, the *Port Authority* is responsible for managing port operations and ensuring the safety of Vessels, guaranteeing compliance with local, national, and international regulations. Its responsibilities include overseeing docking procedures, verifying that Vessels adhere to safety and environmental standards, conducting customs and security checks, and coordinating the loading and unloading of cargo. The Port Authority plays a pivotal role in ensuring the efficient utilization of port facilities, managing Vessel traffic, and addressing emergencies such as accidents or environmental incidents. It collaborates closely with Vessels to ensure operational safety, security, and overall efficiency within the port environment.

5 System architecture and operations

The B2SAPP architecture is specifically designed to enable Vessels to maintain effective control over their maritime operations while ensuring adherence to established security protocols. This architecture comprises the following essential operations: (*i*) Issuance of VCs; (*ii*) Verification of VCs; (*iii*) Enforcement of Commands; (*iv*) Verification and Clearance for Vessels Approaching Port. A comprehensive description of these operations will be provided in the context of both the Vessel and a CCC employee (refer to Table 1).

5.1 Credential issuance operation

As indicated by its designation, this operation is overseen by the NOC, which is responsible for issuing VCs following the principles of Hyperledger Aries, specifically concerning Vessels and CCC Employees. The primary objective of this operation is to establish a robust identification mechanism that enables accurate data transfer between Vessels and CCC Employees to both the CCC and, subsequently, the Port Authority. This operation is designed to integrate automated procedures in the identification phase for Vessels and CCC Employees to authenticate and authorize data exchange between the two entities (see Figure 2).

TABLE 1 Instances used in B2SAPP.

Vessel instance		CCC employee	
Attribute	Value	Attribute	Value
Vessel name	ARGO	Full name	John Doe
IMO number	IMO 123456	Employee ID	123456789
Vessel owner	Milky Way Ltd.	Department	Maritime Operations
Operator information	Milky Way Ltd.	Organization	Milky Way Ltd.
Vessel type	Cargo	Position	Operation Manager
Flag	Hellas	Role	Coordinator
Certifications	SOLAS	Permission	Access data
Vessel's size	366 m	Certification	SOLAS, IMS
TEU	15,000	Maintenance history	No issues in past 12 months
Fuel consumption	500 tons of fuel per month	Last maintenance	Engine overhaul on 2024-10-10
Emission	CO_2 1,500 tons annually	Next Inspection	2025-01-15
Insurance	Hull and machinery		

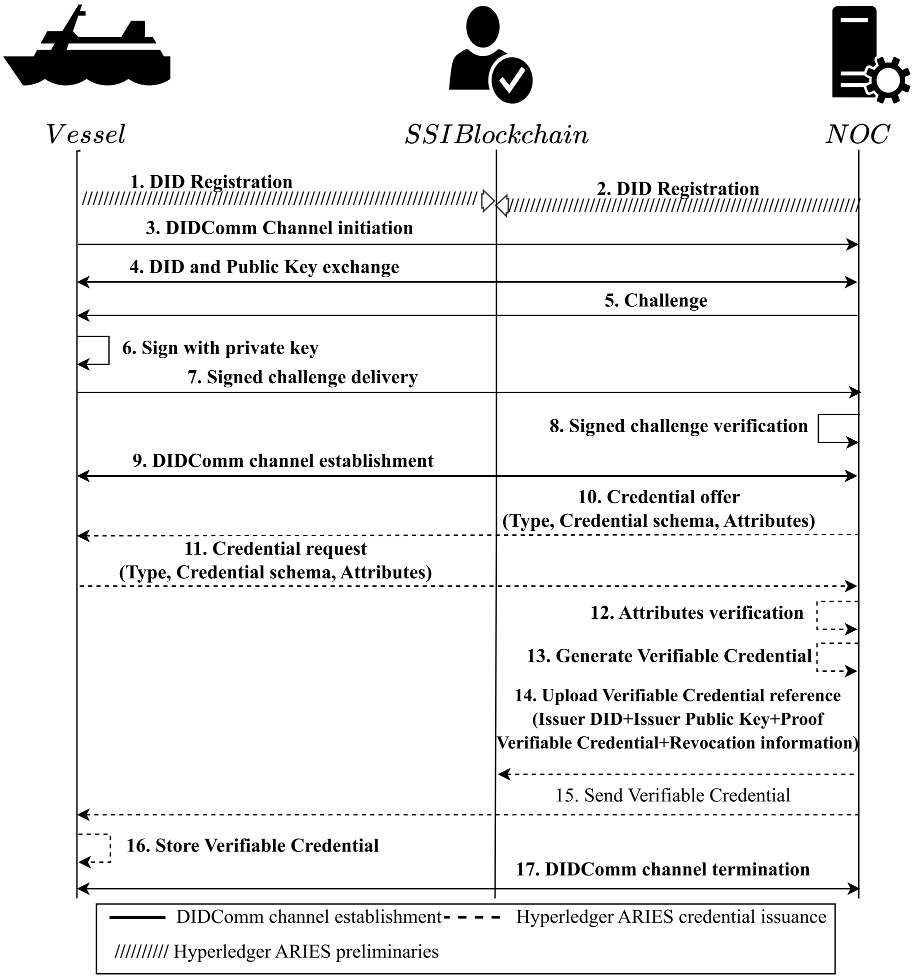
Vessel
SSIBlockchain
NOC
1. DID Registration
2. DID Registration
3. DIDComm Channel initiation
4. DID and Public Key exchange
5. Challenge
6. Sign with private key
7. Signed challenge delivery
8. Signed challenge verification
9. DIDComm channel establishment
10. Credential offer
(Type, Credential schema, Attributes)
11. Credential request
(Type, Credential schema, Attributes)
12. Attributes verification
13. Generate Verifiable Credential
14. Upload Verifiable Credential reference
(Issuer DID+Issuer Public Key+Proof
Verifiable Credential+Revocation information)
15. Send Verifiable Credential
16. Store Verifiable Credential
17. DIDComm channel termination
DIDComm channel establishment
Hyperledger ARIES credential issuance
////////// Hyperledger ARIES preliminaries

FIGURE 2
B2SAPP VC issuance.

In the VC issuance process (refer to *Steps 1–17* in Figure 2), it is assumed that both the Vessel and the NOC have previously generated a cryptographic key pair. The corresponding public key is encoded in a specific format that will later represent the DID (e.g., SHA-256) to be shared with other entities. In contrast, the private key is securely stored in a digital wallet (see Figure 1). Subsequently, the Vessel and the NOC publish their DIDs to the decentralized SSI Blockchain network (*Steps 1–2*).

The issuance of a Hyperledger Aries VC begins when the Vessel transmits a request to establish a DIDComm channel to the NOC, resulting in the exchange of DIDs and public keys between the two parties (*Steps 3–4*). Prior to initiating the DIDComm channel with the Vessel, the NOC aims to authenticate the Vessel through a challenge-response protocol. The Vessel authenticates this challenge using its private key, which is securely stored in its digital identity wallet and returns the response to the NOC for validation. The Vessel's device must be adequately secured to prevent unauthorized access to the private key. Upon successful completion of the verification process, the DIDComm channel is established (*Steps 5–9*).

Once the DIDComm channel has been successfully set up, the NOC, acting as the Issuer, sends a VC offer to the Vessel (*Step 10*). This offer details the credential type, schema, and the required attributes. Upon receipt of the offer, the Vessel issues a corresponding request that accepts the offer, providing its DID, credential schema, and verified attributes (*Step 11*).

Subsequently, the NOC conducts an internal verification of the attributes and issues the VC based on those attributes. For instance, a VC pertaining to Vessels may include the following data:

- **id:** a unique identifier for the VC issued to the Vessel (e.g., *https://noc.eu/verifiablecredential/1234*).
- **type:** indicates the type of the credential that is verifiable (e.g., *Verifiable Credential*).
- **issuer:** includes information about the issuer of the corresponding VC such as the name (e.g., *NOC*), its DID (e.g., *did:noc:9876543221*), and URL (e.g., *https://www.noc.miklyway.eu*).
- **issuanceDate:** the date and time when the credential was issued (e.g., *2024-31-12T10:30:00Z*).

- **expirationDate:** the date and time when the credential expires (e.g., *2024-06-05T10:30:00Z*).
- **credentialSubject:** contains information about the subject of the credential. In this paper, it includes the Vessel's DID, VesselName, imoNumber, VesselOwner, VesselOperator, VesselFlag, TEU, size, fuel, insurance, certifications.
- **proof:** include cryptographic proof of the authenticity and integrity of the VC, including the type of the proof's signature, the day of the proof creation, the purpose for the proof, the verification method used from verifier and the signature.

Finally, the NOC saves a reference to the credential on the SSI Blockchain network, ensuring that the issued VC remains secure and unmodifiable after issuance (*Steps 12–14*). This reference contains information about the NOC's DID, public key, proof, and revocation details. Subsequently, the NOC transmits the generated VC to the Vessel, which securely stores it in its digital identity wallet. At this point, the DIDComm channel is terminated (*Steps 15–17*).

At this point, it is essential to highlight that this process outlines the issuance of B2SAPP VCs for the Vessels. However, as previously mentioned, both the Vessels and CCC Employees will hold B2SAPP VCs. The issuance of a CCC employee's B2SAPP VC will also adhere to the Hyperledger Aries VC structure, similar to the description provided above. The key distinction lies in the *credentialSubject*, which will encompass the following attributes: employeeName, employeeSurname, employeeUID, employeeDepartment, employeeLevel, and employeeAccess.

5.2 Verifiable credential verification and maritime operation authorization

As indicated by its designation, this operation facilitates the exchange of operational data and commands between Vessels and employees of the CCC (see *Steps 1–37* in Figure 3).

Initially, the Vessel acquires satellite data, forwarding its operational data to the CCC (*Steps 1–2*). The process commences with the establishment of a presentation mechanism for the Hyperledger Aries VC between the Vessel and the CCC, which entails the creation of a DIDComm channel (*Steps 3–9*). The Vessel submits a request to the CCC to establish the DIDComm channel; at this point, both entities exchange their DIDs and public keys (*Steps 3–4*). Before forming a DIDComm channel with the selected Vessel, the CCC employs a challenge-response protocol to authenticate the Vessel's identity, sending a challenge to be addressed. The Vessel subsequently signs the received challenge utilizing its private key, securely housed within its digital identity wallet, and transmits the signed challenge back to the CCC for validation. Protecting the Vessel's wallet against potential attacks aimed at compromising the private key is imperative. Upon successful verification, the DIDComm channel is established (*Steps 5–9*).

Following the successful establishment of the DIDComm channel, the CCC, serving as the Hyperledger Aries VC verifier, initiates the VC presentation (Steps 10–15) by issuing a request to the Vessel for a specified set of VCs (Step 10). The Vessel then communicates with the CCC, proposing a presentation and detailing the credentials it intends to display. In response, the CCC sends a message requesting a presentation that outlines specific requirements or constraints. Once this request is received, the Vessel prepares a proof demonstrating its possession of the requisite credentials through a zero-knowledge proof methodology (Steps 11–5). The CCC then verifies the proof and evaluates the details of the presentation, providing either an acknowledgment or a rejection message (Step 16). All interactions transpire within the established DIDComm channel, which is subsequently terminated upon completion of the VC presentation.

Next, the Vessel invokes the function entitled SubmitData within B2SAPP's smart contract to submit its operational data to the Maritime Blockchain (*Step 16*). The **input** of this function is the following data: (i) VesselId, that is the Vessel's Unique identifier (e.g., *VSL-12345*); (ii) the Vessel's **location** including coordinates of latitude (e.g., *37.75839*) and longtitude (e.g., *25.561143*); (iii) the signalStrength that is the signal strength in dBm (e.g., *-75*); (iv) the timestamp (integer) that is the Time of submission in UNIX format (e.g., *1702387200*, equivalent to 12th December 2024, 00:00:00 UTC); (v) the Vessel's speed in knots (e.g., 14.5); (vi) the Vessel's heading in degrees (e.g., 45.2), and (vii) the environmental conditions including, wind speed (wind's speed in knots, e.g., *10.2*), wave height (the height of waves in meters, e.g., *2.5*), and temperature (the sea surface temperature in Celsius degrees, e.g., *24.3*). Also, its **output** is a new record stored within the Maritime Blockchain that includes all the aforementioned operational data.

Later, the CCC employee initiates the process to obtain authorization for performing actions on the Maritime Blockchain. The first step involves presenting the Hyperledger Aries VC between the CCC employee and the CCC, thereby creating a DIDComm channel (*Steps 17–23*). The CCC employee sends a request to their respective CCC to establish a DIDComm channel, during which both parties share their DIDs and public keys.

Before the CCC can establish this channel, it employs a challenge-response protocol to verify the identity of the CCC employee by sending a challenge. The CCC employee signs the received challenge using their private key, securely stored in their digital identity wallet and returns it to the CCC for verification. It is imperative to ensure that the Vessel's wallet is safeguarded against potential attacks aimed at accessing the private key. Once the verification is successful, the DIDComm channel is established.

Upon the successful creation of the DIDComm channel, the CCC, acting as the verifier for the Hyperledger Aries VC, commences the Hyperledger Aries VC presentation process by sending a request to the Vessel for a specific set of VCs (*Steps 24–29*). The CCC employee subsequently reaches out to the CCC with a message proposing a presentation and detailing the credentials they intend to showcase. Following this, the CCC forwards a message requesting a presentation, specifying any pertinent needs or limitations. Upon receiving this request, the CCC employee generates proof of possessing the necessary credentials using a zero-knowledge proof method. The CCC then verifies this proof along with the details of the presentation, providing a response that is either an acknowledgment or a rejection message. All

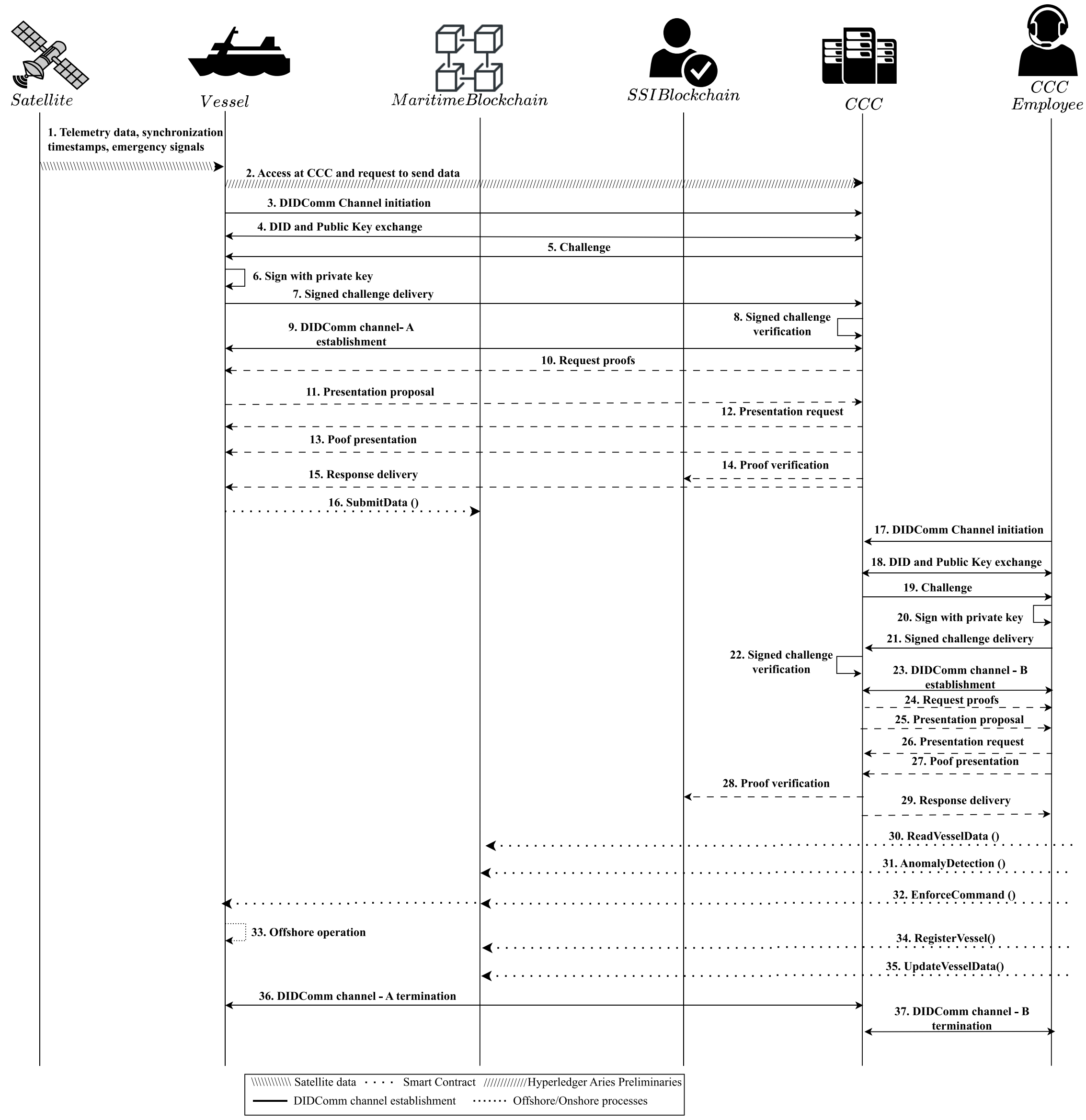
Satellite
Vessel
MaritimeBlockchain
SSIBlockchain
CCC
CCC Employee
1. Telemetry data, synchronization timestamps, emergency signals
2. Access at CCC and request to send data
3. DIDComm Channel initiation
4. DID and Public Key exchange
5. Challenge
6. Sign with private key
7. Signed challenge delivery
8. Signed challenge verification
9. DIDComm channel- A establishment
10. Request proofs
11. Presentation proposal
12. Presentation request
13. Poof presentation
14. Proof verification
15. Response delivery
16. SubmitData ()
17. DIDComm Channel initiation
18. DID and Public Key exchange
19. Challenge
20. Sign with private key
21. Signed challenge delivery
22. Signed challenge verification
23. DIDComm channel - B establishment
24. Request proofs
25. Presentation proposal
26. Presentation request
27. Poof presentation
28. Proof verification
29. Response delivery
30. ReadVesselData ()
31. AnomalyDetection ()
32. EnforceCommand ()
33. Offshore operation
34. RegisterVessel()
35. UpdateVesselData()
36. DIDComm channel - A termination
37. DIDComm channel - B termination
\\\\\\\\\\\\ Satellite data
Smart Contract
////////////Hyperledger Aries Preliminaries
DIDComm channel establishment
Offshore/Onshore processes

FIGURE 3
Present B2SAPP VC and enforce command in Vessel in emergency.

interactions occur within the established DIDComm channel, which is terminated upon the completion of the VC presentation.

Once the CCC employee is authenticated and authorized to access the data stored within the Maritime Blockchain, they begin retrieving the Vessel's general information via the `ReadVesselData` function. Simultaneously, they fetch and analyze the corresponding operational data using the `AnomalyDetection` function to detect potential cyberattacks. Finally, based on the results obtained, the CCC employee issues commands to the Vessel through the `EnforceCommandVessel` function (*Steps 30–32*). The functions utilized by the CCC employee are further analyzed below:

`ReadVesselData` function enables a CCC employee to access and review data stored on the Blockchain pertaining to a specific Vessel. This functionality assists the employee in monitoring the Vessel's information, thereby facilitating informed decision-making. As **input**, it requires the VesselId (e.g., VSL-123456). The **output** of this function encompasses details such as the Vessel Name (e.g., ARGO), IMO number (e.g., IMO 1234567), Vessel Owner (e.g., Milky Way Ltd.), Operator Information (e.g., Milky Way Ltd.), type (e.g., Cargo), flag (e.g., Greece), certifications (e.g., SOLAS), Vessel size (e.g., 366m), TEU (e.g., 15,000), consumption (e.g., 500 tons of fuel per month), and insurance specifics (e.g., Hull and Machinery).

`AnomalyDetection` is initiated by the CCC employee and is accountable for executing checks on the data submitted through the SubmitData function. As **input**, it receives the

VesselId (e.f., VSL 123456), and as **output**, it conveys any identified threats (e.g., spoofing) along with the respective operational data. Each check guarantees that the data aligns with expected operational parameters, and deviations beyond designated thresholds will highlight potential anomalies, as delineated below:

- **Location consistency** verifies whether the Vessel is within its expected route or proximity. **Theshold**: deviation more than 10 nautical miles from the planned route.
- **Signal strength**: checks for weak or inconsistent signal strength, which could indicate a jamming attack. **Acceptable range**: from –30 dBm to –90 dBm (e.g., if SignalSstrength is –120 dBm means potential jamming).
- **Speed validation** compares Vessel's speed to the expected operational range based on its type and conditions. **Acceptable range**: from 5 knots to 25 knots (e.g., 45 knots, is unrealistic for a cargo ship).
- **Heading deviation** assesses if the Vessel's heading aligns with its planned direction of travel. **Deviation** more than 15 degrees from the planned heading over a short interval.
- **Environmental data**: detects inconsistencies between reported sensor data and regional forecasts or averages.
- **Timestamp consistency** ensures the data timestamp aligns with the reporting schedule or expected frequency. **Threshold**: maximum 5 min more from the expected submission interval (e.g., delay more than 20 min means potential spoofing.

EnforceCommand empowers an authorized CCC employee to issue commands to a Vessel (e.g., to reroute or halt operations). It accepts the VesselId and the corresponding command (e.g., stop routing) as **input**. This command is also documented within the maritime Blockchain, and the related Vessel is duly notified. While, its **output** is a new record stored within the Maritime Blockchain that indicated the CCC Employee who enforced the command, the timestamp, the VesselId and the corresponding command (e.g., stop routing)

Upon receipt of the command, the Vessel implements the new directive and continues its operations (*Step 33*). Beyond the previously mentioned functions, the CCC employee can execute additional functions for registering a new Vessel on the Blockchain or updating general information for an already registered Vessel as needed (*Steps 34–35*).

RegisterVessel function is performed by a CCC employee to register a Vessel within the Blockchain system. As **input**, it receives the data delineated in Table 1. Its **output** is a new record within the Maritime Blockchain that includes all the Vessel data and later on can be fetched by the CCC Employees.

UpdateVesselData function is activated by a CCC employee to modify existing Vessel data. It accepts the VesselId and the updated Vessel details as **input**. While, its **output** the new updated record dedicated for that Vessel that includes the updated data.

Lastly, DIDComm channels are terminated for both entities (*Steps 36–37*).

6 System evaluation

This section comprehensively evaluates B2SAPP, which encompasses a detailed performance assessment of both the Maritime Blockchain and the SSI Blockchain networks. Additionally, it includes a thorough security and privacy analysis of the entire system, demonstrating that B2SAPP can address the challenges identified in Section 2. An assessment against prominent cybersecurity threats that may target the foundational technologies of B2SAPP is also included.

6.1 Performance evaluation

We first conduct a performance evaluation of B2SAPP to examine the feasibility and efficiency of the proposed framework. Our analysis focuses on the execution time associated with (i) issuing a B2SAPP Hyperledger Aries VC and (ii) presenting a B2SAPP Hyperledger Aries VC, as well as the frequency of issuance and presentation of VCs with and without requirements' satisfaction. These evaluations are critical to ensure that credential interactions occur within acceptable timeframes for real-time maritime operations, where delays could compromise mission-critical decision-making. Additionally, we assess throughput, average latency, and CPU utilization for the execution of each B2SAPP Hyperledger Fabric smart contract function. This enables us to measure the system's scalability and computational efficiency under varying workloads, helping determine whether the blockchain layer can reliably support operational demands such as anomaly detection, data submission, and command enforcement in a distributed maritime environment.

To this end, we implemented the Maritime Blockchain framework utilizing the well-established Hyperledger Fabric (Voudouris et al., 2024; LF Decentralized Trust, 2025c) to maintain a distributed network of peer nodes employing the Raft consensus mechanism. This mechanism facilitates agreement on transaction ordering and ensures a consistent state within the Blockchain ledger. We specifically selected Hyperledger Fabric version 2 with the Raft consensus method due to its substantial advantages in operational simplicity and system reliability over the Kafka-based solutions presented in version 1. The Raft consensus model streamlines network setup and maintenance by removing external dependencies, such as Zookeeper, required for Kafka. Furthermore, it provides a more direct and reliable approach to consensus, which enhances fault tolerance and overall efficiency of the Blockchain network. Additionally, the B2SAPP smart contract was developed using *Node.js*, and we employed Hyperledger Caliper (LF Decentralized Trust, 2025a) to evaluate the performance of the maritime Blockchain implementation.

Furthermore, the B2SAPP SSI Blockchain has been constructed on the Hyperledger Aries framework (LF Decentralized Trust, 2025b), based on Hyperledger Indy. This framework supports the secure establishment of DIDs and the issuance, revocation, and verification of B2SAPP VCs. In this architecture, peers function as issuers, holders, and verifiers, while Aries Agents, developed using the Aries Cloud Agent

Python (OpenWallet Foundation, 2025), facilitate interactions, VC exchanges, and management of DID documents. Each Aries agent comprises the Aries Framework component for engagements with ledgers, wallets, and other agents, in addition to the Aries Controller component that governs behavior according to established business rules. Each agent maintains a wallet utilizing a *SQLite* database, serving as the repository for secret keys, connections, and VCs.

Our proof of concept was deployed on an Ubuntu 18.04 desktop, configured with an Intel Xeon(R) Silver CPU operating at 2.20 GHz and equipped with 12 GB of RAM. The deployment environment included Docker containers for all peers of Hyperledger Fabric, Hyperledger Caliper client machines, and the SSI Blockchain peer.

We have to mention here that the experiments for the SSI Blockchain were performed three times, while the experiments for the B2SAPP Blockchain were performed five times. All of them were conducted in a controlled virtualized environment to eliminate external network variability and a dockerization approach was applied. The validation scope focuses on functional performance of the system under different transaction and credential exchange scenarios, without introducing adversarial testing or fault injections. Also, it is worth-mentioning that no third-party audits were conducted for this initial prototype; the results were cross-verified using internal test scripts and benchmark logs for consistency.

To evaluate the performance of the B2SAPP SSI Blockchain being built upon Hyperledger Aries, we measured the average time required to issue and verify a VC. To achieve this, each experimental trial was executed three times to ensure reliability. In our proof of concept implementation, we deployed three Aries agents: (*i*) one for the CCC to issue the VC, (*ii*) one for the CCC to verify the VC, and (*iii*) one for the Vessel to present the VC. The configuration of the Hyperledger Aries credential is as follows:

1. **Vessel name:** this field denotes the official name of the Vessel (e.g., *ARGO*).
2. **Vessel Id:** a unique Vessel's identifier (e.g., *123456*)
3. **IMO number:** a unique seven-digit identifier issued by the International Maritime Organization (IMO) (e.g., *IMO 1234567*).
4. **Vessel owner:** the maritime organization with legal title to the Vessel (e.g., *Milky Way Ltd.*).
5. **Vessel operator:** the entity responsible for the day-to-day management and operation of the Vessel (e.g., *Milky Way Ltd.*).
6. **Vessel type:** a classification describing the primary function and design of the Vessel (e.g., *Cargo*).
7. **Vessel Flag:** Denotes the country of registration (e.g., *Greece*).
8. **Certifications:** Documents attesting that the Vessel meets specific international or domestic regulatory requirements (e.g., *SOLAS*).
9. **Vessel size:** represents the overall dimensions of the Vessel, typically indicated by length in meters (e.g., *366 m*).
10. **TEU:** twenty-foot Equivalent Unit quantifies the cargo capacity (e.g., *15,000*).
11. **Fuel consumption:** indicates the Vessel's rate of fuel usage over a specified period (e.g., *500 tons of fuel per month*).
12. **Emission**: this value reflects the volume and type of pollutants emitted (e.g., *CO_2 1,500 tons annually*) by the corresponding Vessel.
13. **Insurance:** this attributes specifies the insurance coverages being active for the Vessel (e.g., *Hull and Machinery*) during the corresponding route.

The performed experiments were conducted by simultaneously submitting bulk requests (5, 10, 50, 100, 200, and 300 requests of credential presentation/issuance) with a specific number of attributes (5, 10, and 20 attributes per presentation of credential). Particularly, in the experiments utilizing five attributes, the following attributes were included: *Vessel Name*, *Vessel Id*, *IMO Number*, *Vessel Owner*, and *Vessel Operator*. Furthermore, in the experiments involving ten attributes, the aforementioned five were considered in addition to *Vessel Type*, *Vessel Flag*, *Certifications*, *Vessel Size*, and *TEU*. In addition, the experiments with 20 and 40 attributes incorporated all previously mentioned data, along with *Fuel Consumption*, *Emission*, *Insurance*, and additional attributes with alphanumeric values (e.g., *abc16b78m0*).

Figure 4 presents the average time needed to issue a B2SAPP VC using Hyperledger Aries. Specifically, when issuing credentials with fve attributes, the average issuance time is 0.42, 0.34, 0.29, 0.32, 0.32, and 0.33 s for the issuance of 5, 10, 50, 100, 200, and 300 credentials, respectively. When 10 attributes are included, these average times are 0.44, 0.36, 0.31, 0.33, 0.34, and 0.34 s. For credentials containing 20 attributes, the average times are 0.46, 0.41, 0.34, 0.37, 0.37, and 0.37 s, while for 40 attributes, the values are 0.57, 0.44, 0.39, 0.43, 0.44, and 0.44 s.

Overall, these results indicate that the average time required to issue a B2SAPP VC with Hyperledger Aries increases as the number of attributes grows. Moreover, although this average time decreases when the number of requested credentials rises from 5 to 50, it increases once the number of credentials surpasses 50,

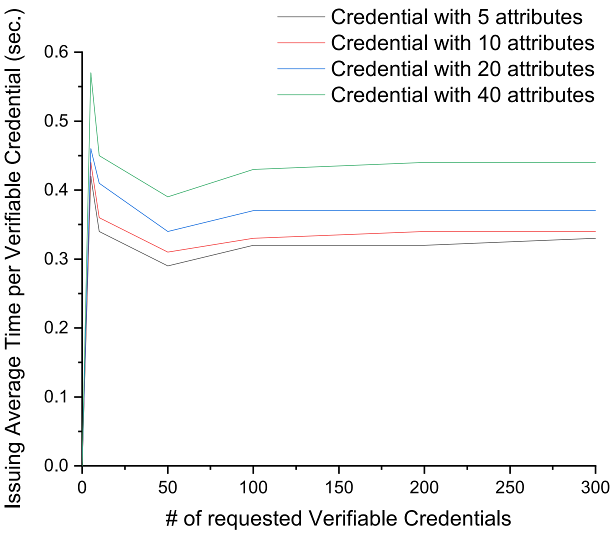

FIGURE 4
Average time issuing B2SAPP VC based on the Hyperledger Aries.

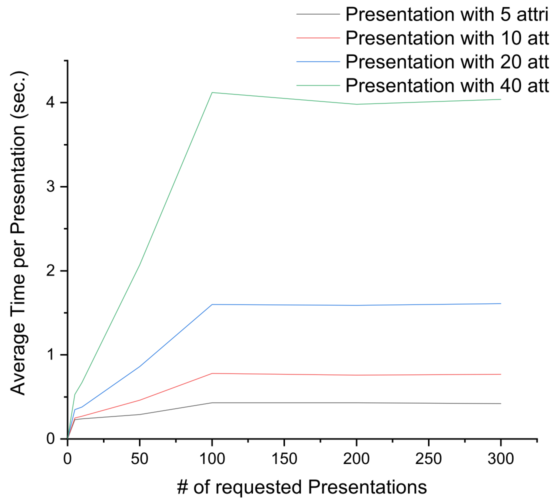

FIGURE 5
Average time of presentation verification based on the Hyperledger Aries satisfying predicate.

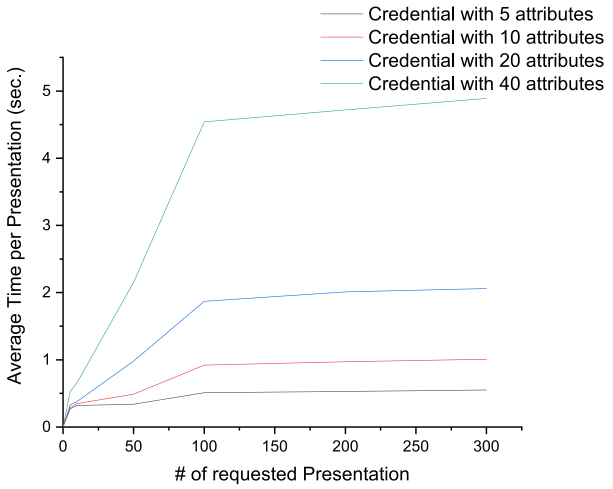

FIGURE 6
Average time of presentation verification based on the Hyperledger Aries without satisfying predicate requests.

particularly between 50 and 100, and continues to slightly increase beyond 100.

Figure 5 illustrates the average time required to present a B2SAPP VC based on Hyperledger Aries while satisfying the requests of CCC. Specifically, when verifying presentations with five attributes, the average time is 0.23, 0.24, 0.29, 0.42, 0.43, and 0.42 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. For 10 attributes, the average time is 0.25, 0.27, 0.46, 0.78, 0.76, and 0.77 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. Verifying 20-attribute presentations requires 0.35, 0.38, 0.86, 1.60, 1.59, and 1.61 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. Finally, verifying 40-attribute presentations requires 0.53, 0.67, 2.07, 4.12, 3.98, and 4.04 s for 5, 10, 50, 100, 200, and 300 presentations, respectively.

Figure 6 presents the average time needed to verify a B2SAPP VC based on Hyperledger Aries without satisfying the requests of CCC. Specifically, the average verification time for five attributes is 0.27, 0.32, 0.34, 0.51, 0.53, and 0.53 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. For 10 attributes, the average verification time is 0.29, 0.35, 0.49, 0.92, 0.97, and 1.01 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. When verifying 20-attribute presentations, the average time is 0.33, 0.38, 0.98, 1.87, 2.01, and 2.06 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. Verifying 40-attribute presentations requires 0.53, 0.66, 2.15, 4.54, 4.72, and 4.89 s for 5, 10, 50, 100, 200, and 300 presentations, respectively. Overall, it can be observed that increasing the number of requested attributes results in greater average verification times, regardless of whether the requests are satisfied.

Overall, the measured issuance and verification times are sufficiently short to enhance user satisfaction by providing seamless interactions. Moreover, monitoring these average times can detect deviations that could lead to potential issues or security risks (Farao et al., 2020; Paparis et al., 2025), ensuring that the system remains reliable and trustworthy.

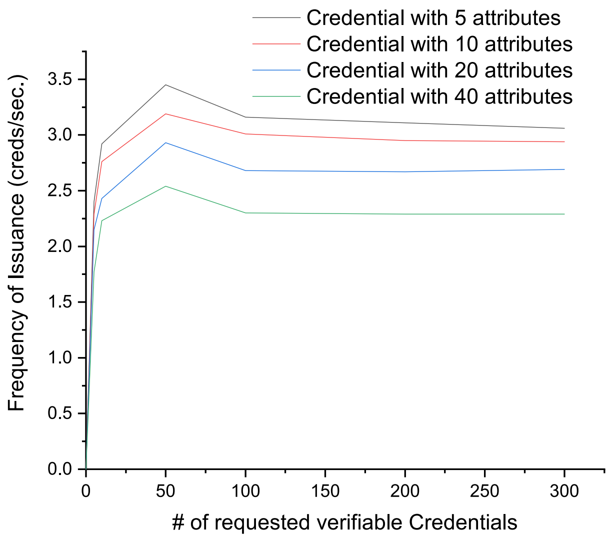

FIGURE 7
Frequency of issuance B2SAPP VC based on Hyperledger Aries.

In addition, the issuance (see Figure 7) and verification (see Figures 8, 9) frequencies were measured to demonstrate the scalability of the Hyperledger Aries environment. As shown in Figure 7, the issuance rate of B2SAPP VCs (with five attributes) in terms of credentials per second (creds/sec) is 2.4, 2.92, 3.45, 3.16, 3.11, and 3.06 for 5, 10, 50, 100, 200, and 300 requested credentials, respectively. For 10 attributes, the issuance rate is 2.29, 2.76, 3.19, 3.01, 2.95, and 2.94 creds/s for 5, 10, 50, 100, 200, and 300 requested credentials, respectively. When issuing VCs with 20 attributes, the rate is 2.15, 2.43, 2.93, 2.68, 2.67, and 2.69 creds/sec, and for 40 attributes, it is 1.77, 2.23, 2.54, 2.30, 2.29, and 2.29 creds/s for 5, 10, 50, 100, 200, and 300 requested credentials, respectively. Overall, there is a noticeable increase in the issuance rate from 5 to

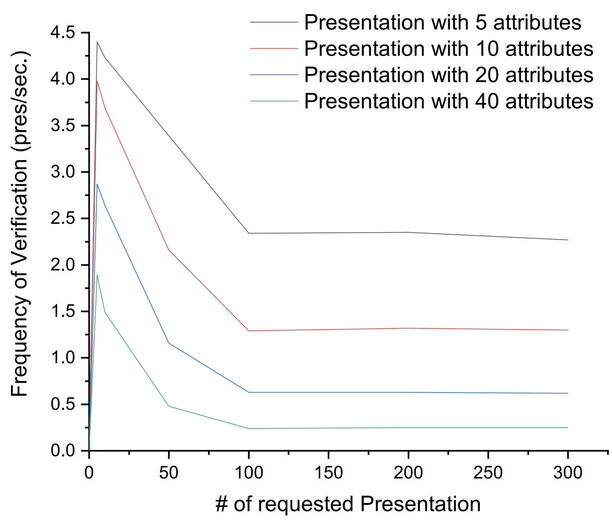

FIGURE 8
Frequency of presentation verification based on the Hyperledger Aries satisfying predicate requests.

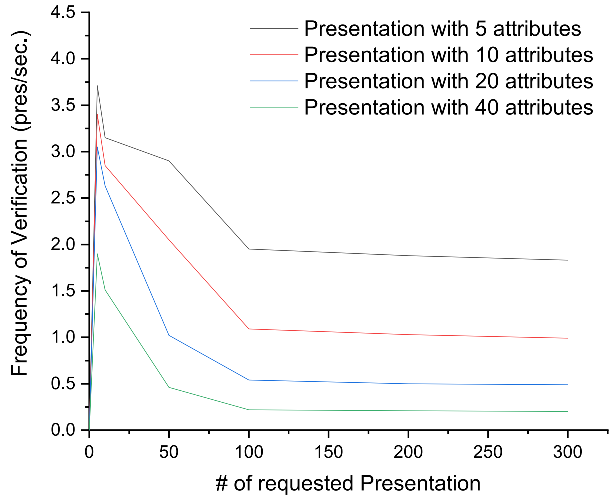

FIGURE 9
Frequency of presentation verification based on the Hyperledger Aries without satisfying predicate requests.

50 requested credentials, followed by a slight decrease from 50 to 100, after which the rate stabilizes when the number of requested credentials exceeds 100.

Figures 8, 9 depict the verification frequency of presentations with and without satisfying the requests. When verifying credentials that satisfy the requests (Figure 8), the frequency for 5-attribute VCs is 4.4, 4.23, 3.39, 2.34, 2.35, and 2.27 creds/s for 5, 10, 50, 100, 200, and 300 presentations, respectively. For 10 attributes, the rate is 3.98, 3.69, 2.16, 1.29, 1.32, and 1.3 creds/sec. Verifying 20-attribute presentations yields 2.87, 3.69, 2.16, 1.29, 1.32, and 1.3 creds/sec, while 40-attribute presentations achieve 1.89, 1.49, 0.48, 0.24, 0.25, and 0.25 creds/s for 5, 10, 50, 100, 200, and 300 presentations.

On the other hand, the frequency for verifying credentials without satisfying the requests is as follows (see Figure 9): for verifying VC with five attributes the frequency is as follows: 3.71, 3.15, 2.9, 1.95, 1.88, and 1.83 cred/s for requests of 5, 10, 50, 100, 200, and 300 credentials, respectively. Additionally, the verification rate of a B2SAPP VC (with 10 attributes) per second is 3.4, 2.85, 2.05, 1.09, 1.03, and 0.99 cred/s for requests of 5, 10, 50, 100, 200, and 300 credentials, respectively. Moreover, the issuance rate of VC (with 20 attributes) per second is 3.05, 2.63, 1.02, 0.54, 0.5, and 0.49 cred/s for requests of 5, 10, 50, 100, 200, and 300 credentials, respectively. Also, the verification rate of VC (with 40 attributes) per second is 1.9, 1.51, 0.46, 0.22, 0.21, and 0.2 cred/s for requests of 5, 10, 50, 100, 200, and 300 credentials, respectively.

In contrast, when verifying credentials without satisfying the requests (Figure 9), the frequency for 5-attribute VCs is 3.71, 3.15, 2.9, 1.95, 1.88, and 1.83 creds/s for 5, 10, 50, 100, 200, and 300 presentations. For 10 attributes, it is 3.4, 2.85, 2.05, 1.09, 1.03, and 0.99 creds/sec, while verifying 20-attribute presentations yields 3.05, 2.63, 1.02, 0.54, 0.5, and 0.49 creds/sec. Finally, 40-attribute presentations achieved 1.9, 1.51, 0.46, 0.22, 0.21, and 0.2 creds/s for 5, 10, 50, 100, 200, and 300 presentations, respectively.

Comparing these figures reveals that the verification frequency decreases as the number of requested attributes increases. Moreover, the frequency spikes when the number of requested presentations increases from 0 to 5, decreases from 5 to 50, and remains relatively stable beyond 100 presentations, regardless of whether the requests are satisfied.

For the evaluation of the Maritime Blockchain, the average latency (in s), throughput (transactions per second), and CPU consumption (percentage utilization) were measured for six discrete smart contract functions. Throughput refers to the number of successful transactions per second, where a successful transaction is processed, included in a block, and committed to the Blockchain. Average latency indicates the time from transaction submission to its commitment on the ledger. CPU utilization reflects the load on peers during each experiment. Each experiment was repeated five times with the following parameters: (*i*) two or four nodes (representing the number of peers in the Maritime Blockchain), (*ii*) a batch size of 2,000 (representing the number of transactions per block), and (*iii*) 100, 1,000, 1,500, or 2,000 total sent transactions. These experiments aim to demonstrate how the Maritime Blockchain behaves under varying numbers of nodes, batch sizes, and transaction volumes.

Figures 10, 11 depict the throughput (transactions per second) for networks comprising two nodes and four nodes. For the `AnomalyDetection` function, the throughput values are 18.73, 32.96, 35.60, and 36.93 with two nodes and 13.86, 21.86, 24.13, and 25.36 with four nodes for 100, 1,000, 1,500, and 2,000 transactions, respectively. The `EnforceCommand` function achieves throughputs of 13.50, 26.20, 29.30, and 30.60 with two nodes and 12.90, 19.00, 22.10, and 23.40 with four nodes. For `ReadVesselData`, the throughput for two nodes is 33.10, 46.60, 53.60, and 53.20 and 32.70, 46.00, 49.80, and 51.00 for four nodes. The `RegisterVessel` function yields 15.40, 30.50, 24.60, and 29.50 with two nodes and 7.80, 12.70, 14.00, and 16.30 with four nodes. For `SubmitData`, two nodes achieve throughputs of 10.40, 19.60, 21.30, and 21.70, whereas four nodes achieve 13.80, 19.80,

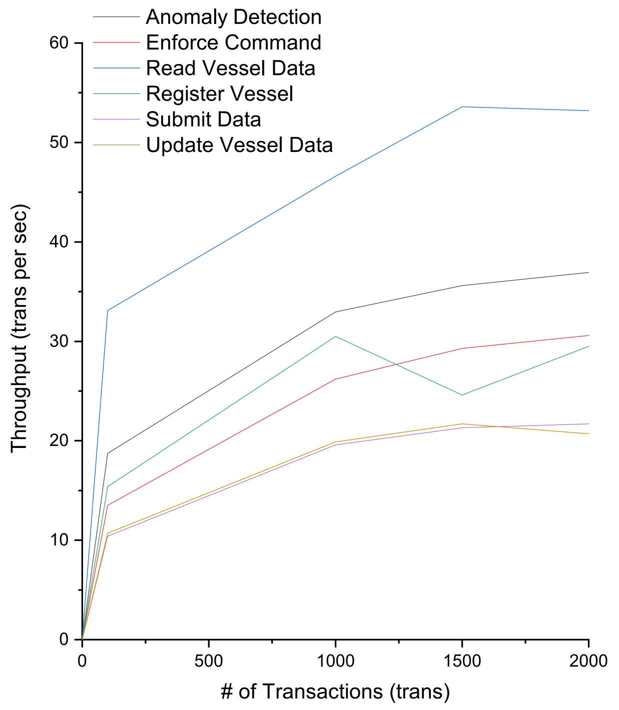

FIGURE 10
Throughput with two nodes.

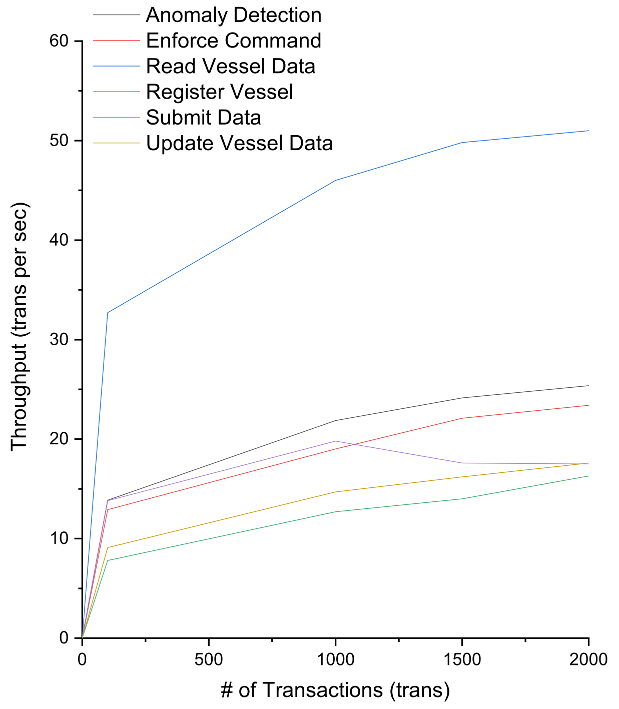

FIGURE 11
Throughput with four nodes.

17.60, and 17.50. Finally, UpdateVesselData reaches 10.70, 19.90, 21.70, and 20.70 with two nodes and 9.10, 14.70, 16.20, and 17.60 with four nodes.

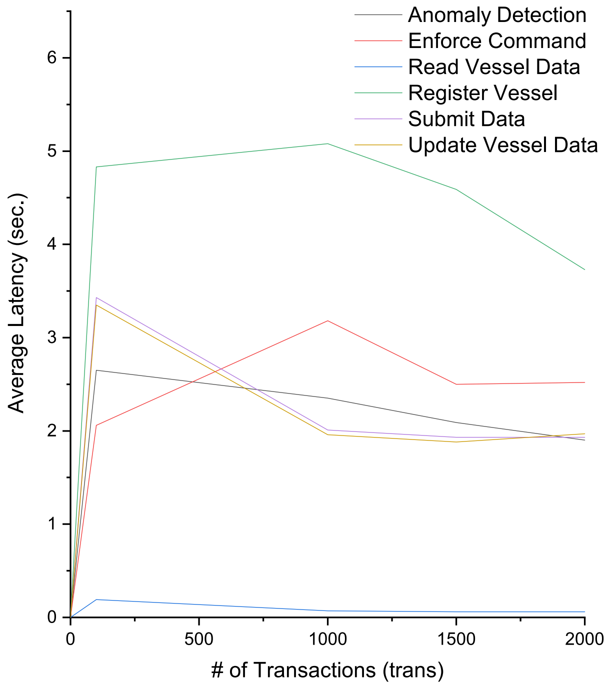

FIGURE 12
Average latency with two nodes.

Figures 12, 13 present the average latency (in s) for two- and four-node configurations. The average latency for AnomalyDetection is 2.65, 2.35, 2.09, and 1.90 s with two nodes and 9.23, 48.53, 62.61, and 92.39 s with four nodes for 100, 1,000, 1,500, and 2,000 transactions. The EnforceCommand function exhibits latencies of 2.06, 3.18, 2.50, and 2.52 s with two nodes and 5.84, 32.48, 32.09, and 35.05 s with four nodes. For ReadVesselData, the average latency is 0.19, 0.07, 0.06, and 0.06 s with two nodes and 0.19, 0.08, 0.06, and 0.06 s with four nodes. The RegisterVessel function requires 4.83, 5.08, 4.59, and 3.73 s (two nodes) and 6.47, 43.22, 9.64, and 19.77 s (four nodes). For SubmitData, latencies of 3.43, 2.01, 1.93, and 1.93 s occur with two nodes, while four nodes yield 5.32, 32.11, 52.35, and 64.77 s. Lastly, UpdateVesselData has latencies of 3.35, 1.96, 1.88, and 1.97 seconds with two nodes and 4.82, 8.36, 6.17, and 6.21 seconds with four nodes.

Figures 14, 15 show CPU consumption (percentage) for two- and four-node network configurations, respectively. For AnomalyDetection, CPU utilization is 2.65%, 23.19%, 5.88%, 6.28%, and 6.73% with two nodes and 2.90%, 3.12%, 2.62%, and 2.38% with four nodes for 100, 1,000, 1,500, and 2,000 transactions, respectively. The EnforceCommand function exhibits 2.86%, 5.11%, 5.25%, and 5.55% CPU usage with two nodes and 3.25%, 4.28%, 4.77%, and 4.73% with four nodes. For ReadVesselData, CPU consumption is 2.24%, 4.12%, 4.47%, and 4.74% (two nodes) versus 2.35%, 4.14%, 4.30%, and 4.70% (four nodes). The RegisterVessel function yields 3.26%, 5.80%, 5.44%, and 5.62% (two nodes) and 1.96%, 3.05%, 3.45%, and 3.46% (four nodes). For SubmitData, CPU usage is 2.31%, 3.94%, 4.45%, and 4.29% with two nodes, while four nodes exhibit 3.17%, 4.38%, 4.11%, and 4.20%. Finally, UpdateVesselData

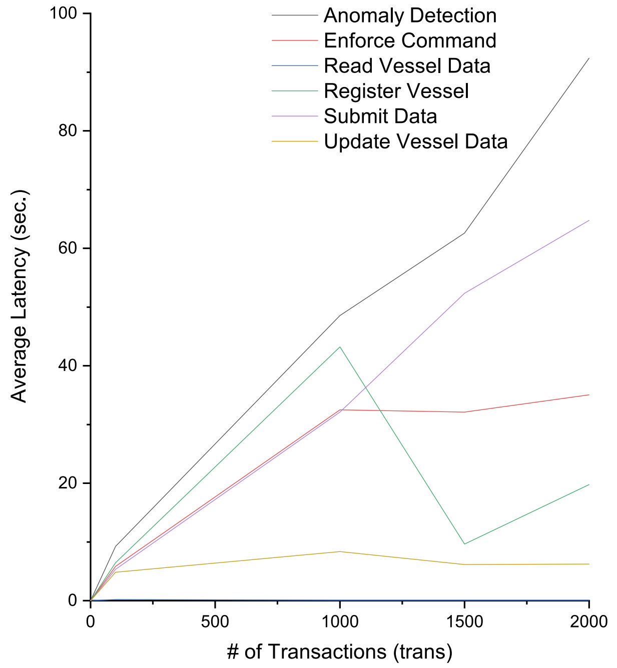

FIGURE 13
Average latency with four nodes.

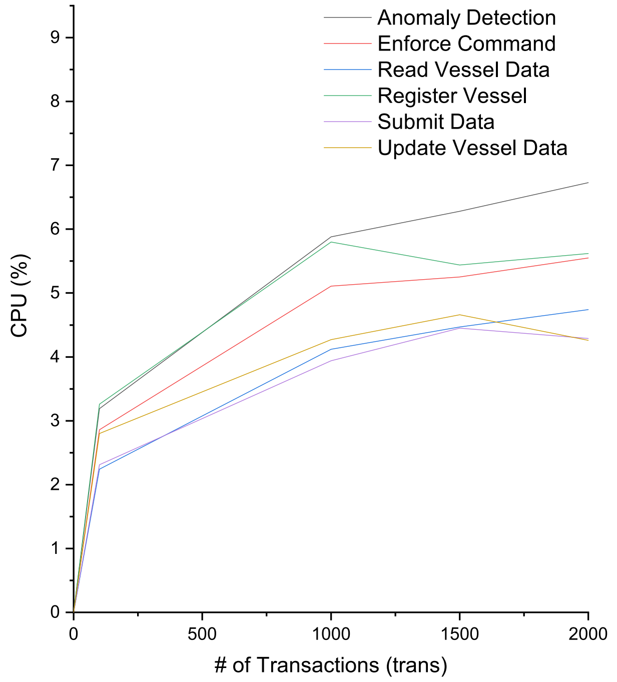

FIGURE 14
CPU consumption with two nodes.

requires 2.80%, 4.27%, 4.66%, and 4.26% CPU (two nodes) and 2.56%, 3.30%, 3.70%, and 3.72% CPU (four nodes).

In summary, experiments in the in-house Raft-based Hyperledger Fabric network indicate that four-node configurations demonstrate better CPU consumption and average latency than two-node configurations, primarily due to more efficient workload distribution and improved consensus efficiency. Increasing the number of nodes can reduce CPU usage because the tasks related to transaction endorsement, log replication, and consensus are more evenly shared. However, the throughput decreases as the number of nodes increases, likely because the Raft-based consensus mechanism requires additional coordination for log replication and agreement among more participants, thereby increasing overall latency and reducing throughput.

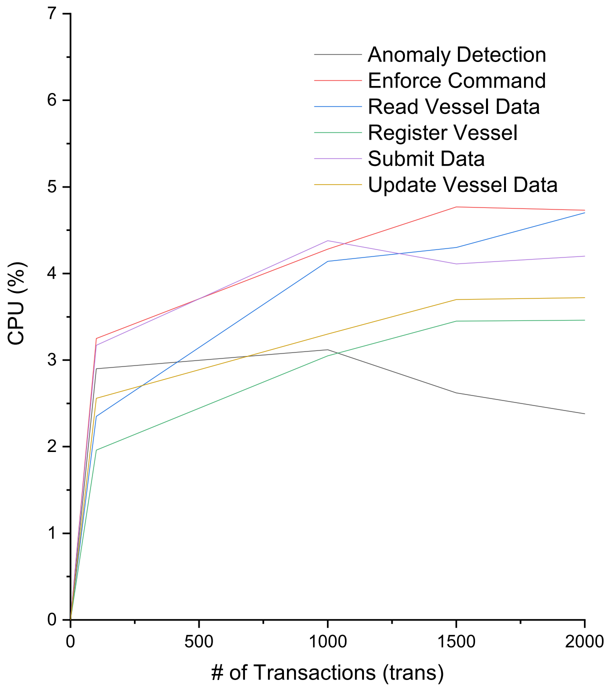

FIGURE 15
CPU consumption with four nodes.

Overall, our implementation was a prototype, not an optimized production system. For example, credential payloads were minimal (only essential fields) and network parameters were set to allow fast commits. As a result, performance numbers should be interpreted as baseline capabilities; real-world deployments (with larger payloads or heavier processing) might exhibit higher latencies. In addition, tests were limited to a small network (e.g., two–four nodes). While we varied client load, we did not evaluate performance on a large distributed deployment. Consequently, the observed metrics do not account for factors like inter-node network delays, bandwidth constraints, or large-scale concurrency bottlenecks. Finally, as we previously mentioned that B2SAPP evaluation relied on built-in timestamps and logging.

6.2 Security and privacy analysis

It is strongly contended that B2SAPP can address all of the cybersecurity challenges mentioned in Section 2, apart from the CH5 Supply Chain Vulnerabilities, while also proactively defending against other common attacks. Thus, firstly we will analyze the specific security protocols and encryption methods used in B2SAPP and later on we elaborate on these challenges and illustrate how B2SAPP mitigates them.

First and foremost, the uniqueness of B2SAPP is inherited by the blockchain in network security due to ability to provide decentralized trust, tamper-evident logging, and verifiable data integrity without reliance on a central authority. Unlike traditional security mechanisms, which often depend on centralized control, blockchain distributes trust across multiple nodes, reducing single points of failure and insider risk. This is particularly crucial in maritime, where assets, identities, and communications must be managed securely across organizational boundaries. Furthermore, blockchain enables cryptographically verifiable and immutable audit trails, ensuring that all actions (i.e., data submissions, access events, or credential verifications) are permanently recorded and auditable. When paired with SSI, it facilitates privacy-preserving identity proofs and fine-grained access control without exposing sensitive personal data.

In B2SAPP, security and data integrity are enforced through a combination of advanced cryptographic techniques and well-established security protocols. On the one hand, Hyperledger Fabric, serving as the underlying blockchain infrastructure, employs Transport Layer Security to ensure encrypted communication between nodes and utilizes strong encryption algorithms, such as Elliptic Curve Digital Signature Algorithm, to authenticate transactions and verify identities. On the other hand, the Hyperledger Aries leverages DIDs and VCs that can be cryptographically signed using JSON Web Signatures, ensuring both the authenticity and integrity of identity claims. Data exchanged between entities is further protected using end-to-end encryption protocols, and the storage of verifiable logs on the immutable ledger guarantees non-repudiation and auditability. The combination of these protocols and encryption methods enables secure, verifiable, and privacy-preserving communication and authentication across the maritime ecosystem, aligning with both modern cybersecurity standards and regulatory compliance requirements.

Below, we elaborate on these challenges and illustrate how B2SAPP mitigates them.

CH1—Spoofing and jamming: B2SAPP counters spoofing and jamming attacks by integrating technologies such as Blockchain, Smart Contracts, and SSI. In B2SAPP, every Vessel must verify its identity through its Hyperledger Aries VC prior to submitting operational data to the maritime Blockchain, ensuring that only authenticated and trustworthy Vessels can interact with the system. Furthermore, the anomaly detection function within B2SAPP's smart contracts continuously monitors incoming data (e.g., Vessel operational data) and evaluates them against predefined thresholds. Any atypical behavior (Suciu et al., 2022), such as an implausible speed (e.g., 45 knots for a cargo Vessel) or inconsistent heading, is flagged as suspicious and generates alerts for subsequent investigation. Simultaneously, monitoring signal strength data from Vessels facilitates the detection of jamming attacks that undermine signal transmission via B2SAPP's anomaly detection. For instance, a sudden decrease in signal strength (e.g., below −100, dBm) or delayed data submissions would trigger the anomaly detection mechanism, indicating a potential jamming scenario. The immutable records of the maritime Blockchain further guarantee that historical data remain resistant to tampering, enabling verification of past Vessel positions and behaviors to expose discrepancies arising from compromised or disrupted signals. Concurrently, the CCC can leverage real-time anomaly alerts through the maritime Blockchain to initiate immediate countermeasures, including rerouting Vessels or heightening monitoring efforts. By combining decentralized trust through the maritime Blockchain, data validation through smart contracts, and secure identity management with SSI, B2SAPP provides robust safeguards against spoofing and jamming, thereby upholding the security and integrity of maritime operations.

CH2—Unauthorized access to system: In B2SAPP, this challenge is primarily addressed via Hyperledger Aries VCs issued by the CCC. These VCs verify identities, roles, and permissions, ensuring that only validated entities (e.g., a CCC employee) can access specific system functionalities (e.g., issuing an operational command). Concretely, a Vessel must verify its identity using its B2SAPP VC before contributing operational data to the maritime Blockchain, whereas CCC employees require valid VCs to retrieve and oversee Vessel data. Illicit attempts, such as Vessels lacking proper VCs or individuals impersonating CCC personnel, are immediately rejected and generate notifications for further review. By integrating both SSI and Blockchain technologies, B2SAPP establishes a trustworthy infrastructure via VCs and smart contracts, thereby diminishing the probability of unauthorized access and fostering a secure, role-based maritime environment.

CH3—Data interception: Employing Hyperledger Aries ensures that each participating entity is authenticated via VCs before engaging in B2SAPP operations. These VCs are issued and validated by the CCC, granting only authorized entities the ability to initiate or receive data exchanges. Furthermore, VCs enable secure, end-to-end communication among participants through DIDComm protocols. Additionally, operational data from Vessels and CCC personnel is protected by encryption both during transmission [e.g., AES-256-GCM in DIDComm (Curren et al., 2022)] and while at rest [e.g., AES-256 for encrypting ledger data via the BCCSP (Hyperledger Fabric, 2025a,b; Gao et al., 2023)]. Thus, even if adversaries manage to intercept these communications, the encryption mechanisms supplied by Aries and Fabric render the captured data unintelligible and unusable.

CH4—Malware and ransomware: Through Hyperledger Aries, B2SAPP ensures that only authenticated entities possessing valid VCs can access the system. This identity-based verification minimizes the possibility that unauthorized or compromised devices can infiltrate critical infrastructures, thus mitigating the likelihood of malware and ransomware attacks. In addition, Hyperledger Fabric reinforces security through an immutable Blockchain ledger, in which all submitted data is cryptographically hashed and securely stored. Consequently, the data remains intact even if malware compromises a system. Moreover, the decentralized nature of the Blockchain replicates data across multiple nodes, facilitating rapid restoration without reliance on ransom payments. By combining identity-based access, immutable data, real-time anomaly detection, and distributed backups, B2SAPP is well-positioned to defend against malware and ransomware threats.

CH6—Insider threats: B2SAPP addresses insider threats by leveraging Hyperledger Fabric and Hyperledger Aries for robust access control, data verifiability, and system accountability. Participating entities use Hyperledger Aries to authenticate their identities with VCs before engaging with maritime operational systems. This identity-centric approach guarantees that only entities with appropriate roles and permissions can invoke smart contract functions or access sensitive data. Hyperledger Fabric further enhances resilience by maintaining an immutable ledger of all transactions and interactions, ensuring that any malicious or accidental changes can be comprehensively audited. For deliberate insider threats, this unalterable audit trail serves as a powerful deterrent and a source of forensic evidence to promptly uncover and address unauthorized behaviors. Smart contracts act as a preventative barrier for unintentional mistakes by enforcing stringent validation protocols that detect and discard errors or invalid inputs before integrating into the system.

CH7—DoS attacks: B2SAPP effectively mitigates DoS attacks by leveraging Hyperledger Fabric and Hyperledger Aries for resilient access control, data validation, and fault tolerance. Through SSI, B2SAPP enforces identity verification with VCs before allowing entities to utilize communication channels or submit data to the Blockchain. This mechanism prevents malicious users from inundating the system with spurious requests since entities lacking valid VCs are immediately barred. In addition, smart contracts in Hyperledger Fabric bolster the system's defense by implementing rate limits and threshold checks on data submissions. The decentralized nature of the Blockchain ensures data availability even in the event of partial network disruptions (e.g., if one node becomes unavailable, other nodes can still provide access). Lastly, continuous monitoring and detection features enable the prompt identification of DoS-type anomalies and facilitate swift actions to neutralize the source of the disturbance.

CH8—Data logging: B2SAPP leverages Hyperledger Fabric and Hyperledger Aries to secure the data-logging workflow. In B2SAPP, data logging occurs via designated smart contract functions, which only become active once an entity (e.g., a Vessel or CCC employee) has verified its identity via the corresponding B2SAPP VC. This requirement guarantees that any newly added data is securely stored, digitally signed, verifiable, and safeguarded from manipulation.

Beyond addressing the aforementioned challenges, B2SAPP also safeguards the maritime ecosystem and the system's core infrastructure from various other cybersecurity threats (Symes et al., 2024):

Sybil attack: An adversary might create multiple fraudulent identities in an attempt to dominate or mislead a network (e.g., injecting incorrect information into the Blockchain). B2SAPP, however, requires each participant to present Hyperledger Aries VCs for authentication, thereby blocking attackers from introducing illegitimate identities. VCs are granted only following thorough identity verification by the CCC, ensuring that false Vessel or CCC identities cannot be fabricated.

Replay attack: This attack involves capturing legitimate transactions or data and resubmitting them to perform illicit operations (e.g., reusing Vessel data logs to introduce faulty Blockchain entries). B2SAPP employs timestamp and nonce checks within its smart contracts, such that data submissions and VC activities contain unique timestamps, allowing any reused or replayed transactions and VCs to be identified and invalidated. For instance, a Vessel's navigation data bearing an outdated timestamp would be automatically flagged.

Data tampering: This occurs when adversaries alter transmitted data or stored information to undermine the system's reliability. In B2SAPP, any data recorded on the Blockchain remains immutable due to the cryptographic properties of Hyperledger Fabric; thus, any modification attempt is revealed by a hash mismatch. Furthermore, data exchanges between Vessels, the CCC, and the Blockchain are protected through secure communication methods, ensuring that tampering cannot occur during transmission.

Eclipse attack In such attacks, a node within a decentralized network is cut off from the legitimate network by being surrounded by hostile nodes. This isolation prevents the victim node from communicating with the broader system. In B2SAPP, Hyperledger Fabric operates within a permissioned environment requiring node authentication. Consequently, adversaries cannot control or isolate a node, as each node is rigorously vetted and maintained under a trusted infrastructure.

7 Discussion and future perspectives

This section outlines the current limitations of B2SAPP and identifies potential avenues for future work.

7.1 Identified limitations and constraints

Although B2SAPP addresses key challenges such as Spoofing and Jamming (CH1) and Supply Chain Vulnerabilities (CH5), it does not entirely eliminate these threats. By leveraging SSI and Blockchain technologies, B2SAPP establishes robust mechanisms to verify entity authenticity and the integrity of exchanged data, thereby mitigating the likelihood of spoofing attacks. Moreover, the application of timestamps and anomaly detection functions can assist in identifying abnormal patterns, thus contributing to uninterrupted operations and partially mitigating the impact of jamming. However, fully addressing spoofing and jamming ultimately requires the integration of external countermeasures, including specialized anti-jamming techniques.

A parallel observation applies to "Supply Chain Vulnerabilities". While B2SAPP includes verification and authentication mechanisms for all IT/OT components interacting with the Blockchain and SSI systems, these mechanisms predominantly operate post-deployment, and therefore do not address pre-deployment vulnerabilities inherent in the supply chain lifecycle. B2SAPP's design, anchored in blockchain's immutable transaction logging and SSI's fine-grained access control, offers a monitoring and forensic capability that can help detect anomalies originating from compromised components.

Although the paper does not formalize a dedicated supply chain measure serves as a foundation for future development of such metrics. In this way, B2SAPP does not eliminate supply chain fragility but provides a layer of operational resilience that can support quicker detection, traceability, and response when vulnerabilities are exploited.

Despite B2SAPP's ability to enhance cybersecurity in the maritime sector, it does not protect against physical attacks or threats aimed at satellite infrastructure. Physical attacks (e.g., tampering with hardware on Vessels or CCC facilities) remain outside the purview of the system's digital safeguards, and malicious interference with satellite systems (e.g., from high-powered ground stations) is similarly unaddressed. Mitigating these threats necessitates specialized physical security measures, satellite backup solutions, and satellite-specific defensive protocols beyond the scope of this paper.

Instead, B2SAPP primarily focuses on ensuring data integrity, authenticity, and continuity of operations in the maritime ecosystem. By employing advanced technologies, B2SAPP secures data sharing, validates the involved stakeholders, and sustains operations despite various digital challenges. Nonetheless, defending against physical or satellite-based risks requires a holistic, coordinated effort involving satellite operators, national security agencies, and physical security strategies, highlighting the need for a comprehensive approach that integrates digital safeguards with broader protective measures.

Another notable limitation is the simple nature of the smart contract functions defined in Section 5. These functions are intentionally designed as illustrative examples to demonstrate the synergies among SSI, Blockchain, and smart contract functionalities within a maritime context. As such, they do not capture the full complexity and range of operations required in a real-world maritime setting. This is a consequence of the paper's primary emphasis on assessing these technologies' feasibility and foundational architecture within maritime domains rather than delivering a complete, production-ready implementation.

Furthermore, several potential barriers to adoption must be addressed to ensure successful implementation. One significant challenge is the integration of blockchain and SSI technologies into existing maritime infrastructure. Additionally, there may be a lack of technical expertise among stakeholders to manage decentralized identity systems and smart contracts securely. Regulatory uncertainty surrounding the use of decentralized technologies in critical infrastructure may also hinder widespread adoption. To overcome these barriers, it is essential to promote standardization efforts, offer comprehensive training programs, and develop user-friendly interfaces that abstract the complexity of blockchain and SSI operations.

7.2 Future research directions

Future research avenues involve integrating novel technologies to further fortify the maritime ecosystem against emerging threats. One potential enhancement is incorporating quantum-resistant cryptographic methods into SSI and Blockchain frameworks, thereby ensuring the long-term confidentiality and integrity of critical data in the face of quantum computing advancements. Additionally, using Artificial Intelligence techniques in B2SAPP could facilitate more robust anomaly detection, including identifying Advanced Persistent Threats.

Exploring Blockchain interoperability protocols also allows for establishing a global maritime network, fostering seamless data exchange and collaboration across diverse fleets and organizations. In parallel, rapid developments in Artificial Intelligence (Petihakis et al., 2024; Pantelakis et al., 2023) and 6G communication may enable ultra-fast interactions and real-time decision-making, thereby enhancing the efficiency and security of maritime systems. These innovative directions can potentially transform B2SAPP into a critical component of a technologically advanced maritime infrastructure.

Finally, B2SAPP is assessed as a *proof-of-concept* that effectively showcases how blockchain, smart contracts, and SSI can be integrated to enhance security and interoperability within maritime systems, we have recognized the importance of validating B2SAPP in a real-world operational context. As part of our future work, we plan to initiate a pilot deployment in real-life environment. This evaluation will allow us to assess system performance, scalability, interoperability with existing infrastructure, and user acceptance under realistic conditions, thereby providing stronger empirical evidence of the framework's practicality and value.

8 Related work

Satellite communication systems have witnessed significant advancements, with increasing attention toward securing data transmission against potential threats. Navigation Message Authentication has emerged as a critical mechanism to ensure the authenticity and reliability of navigation data. Among such efforts, the Chips Message Robust Authentication (CHIMERA) system employs a hybrid NMA solution for GPS signals, leveraging both symmetric and asymmetric cryptographic methods. It utilizes ECDSA P-224 for cryptographic operations and requires periodic access to non-GPS channels for validated GPS public keys authenticated via a Public Key Infrastructure (PKI) (Anderson et al., 2017, 2022). The development and implementation of CHIMERA have been extensively discussed, particularly highlighting its role in protecting GPS receivers from spoofing attacks (Divis, 2019) and detailing its application within GPS software receivers (Nicola et al., 2021).

The Galileo Global Navigation Satellite System, also known as GNSS, employs the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol for message authentication, offering low computational overhead and suitability for one-to-many broadcasts (Perrig and Tygar, 2003). TESLA secures message origin and integrity using a Message Authentication Code (MAC), with the key for MAC computation provided post-message through a one-way function chain (Perrig et al., 2002). However, TESLA-based NMA systems face computational challenges, as highlighted in analyses of terminal load (Cancela et al., 2019). Additionally, vulnerabilities have been noted, particularly concerning cryptanalysis and potential spoofing attacks (Caparra et al., 2016; Ghorbani et al., 2020). Complementary studies have explored cross-authentication checks in GNSS signals, assessing their effectiveness against non-authenticated signal vulnerabilities (Ardizzon et al., 2023). Broader reviews further examine NMA methods and their integration into existing GNSS systems (Chen et al., 2023; Yuan et al., 2023), alongside the adoption of message authentication to counter spoofing in Satellite-Based Augmentation Systems (Chen et al., 2021).

Blockchain technology has recently found application in satellite communications, emerging as a transformative solution for enhancing security, scalability, and efficiency. The Proof of Space Transactions protocol, for instance, introduces space digital tokens to secure satellite transactions (Torky et al., 2022). Other Blockchain-enabled systems include decentralized reputation mechanisms for satellite relay networks (Clark et al., 2020) and the BlendCAC framework, which integrates Blockchain and smart contracts for decentralized authentication and capability-based access control in space systems (Xu et al., 2019). Additional innovations include Blockchain-based spectrum sharing approaches for satellite and terrestrial networks (Wang et al., 2024), protocols for secure spectrum trading (Li et al., 2020), and frameworks leveraging satellite broadcasting to address traditional Blockchain throughput limitations (Zhang and Liu, 2020).

Blockchain technology has increasingly been explored as a transformative solution for modernizing business processes and enhancing data security also in maritime communications and logistics. Several studies have investigated the integration of blockchain into maritime supply chain systems to address longstanding industry challenges such as lack of transparency, data spoofing, and inefficient information exchange. Liu et al. (2023b) provided a comprehensive literature review coupled with an industrial investigation to map the current state of blockchain adoption in maritime logistics, highlighting prevailing problems and future challenges. In particular, the authors emphasized the need for interoperable and scalable blockchain frameworks to support the sector's digital transformation. Recent efforts have focused on the design of blockchain-based platforms that integrate with existing maritime systems. AISChain (Duan et al., 2022), is a notable example, utilizing consortium blockchain technology to enhance the Automatic Identification System (AIS) with a focus on data integrity and scalability. Similarly, Freire et al. (2022) proposed a permissioned blockchain-based Maritime Monitoring System that employs consensus algorithms such as Raft to secure vessel traffic data. These approaches aim to improve the reliability of maritime data exchange, reduce operational risk, and provide protection against attacks such as AIS spoofing (Tsiulin et al., 2020; Goudosis and Katsikas, 2022).

The role of blockchain in Digital Supply Chain (DSC) operations has also been widely discussed. Korpela et al. (2017) examined the potential of blockchain to accelerate business-to-business (B2B) transactions and integrate DSC processes, emphasizing the value of secure and transparent data sharing in improving overall supply chain efficiency. The adoption of blockchain in global seaborne containerized logistics has been further investigated in Shirani (2018) and Oloruntobi et al. (2023), where the authors discussed its benefits for trading partners and shipping companies. These studies underline the necessity of broader industry acceptance and standardized implementation strategies for realizing blockchain's full potential in maritime logistics. Another comprehensive survey by Farah et al. (2024) delved into the implications of blockchain for supply chain management in the maritime context. The authors highlighted blockchain's capabilities in enhancing transparency, traceability, and operational efficiency across the complex network of maritime logistics stakeholders.

In terms of real-world deployment, one of the most prominent initiatives was the collaboration between Maersk and IBM on the TradeLens platform (McDaniel and Norberg, 2019; Kjærsgaard, 2020). TradeLens aimed to provide real-time access to shipping data, integrating IoT sensor information within a blockchain-backed system. Despite initial success, the collaboration was eventually discontinued (Maersk, 2022), illustrating the difficulties in achieving broad industry-wide adoption and stakeholder alignment. In addition to proprietary systems, several proof-of-concept (PoC) models have been developed and assessed. Ni and Irannezhad (2024) introduced LogisticChain, an open-source PoC on a high-frequency blockchain network using Hyperledger Caliper, tailored for international maritime logistics. Empirical evaluations of various PoCs reveal both potential and limitations in scalability and performance. While some implementations such as CargoX operate on public blockchains like Ethereum (Elmay et al., 2022), the majority of PoCs—such as ProductChain for the food supply chain (Malik et al., 2018), TrustChain for trust management (Malik et al., 2019), and Fabric-PSChain for port logistics (Gao et al., 2022)—have been developed on Hyperledger Fabric. TradeLens itself has also been partially realized on this platform (Kouhizadeh et al., 2021).

Several studies have also addressed the socio-technical and organizational aspects of blockchain adoption. Philipp et al. (2019) explored how blockchain-enabled smart contracts can support collaborative logistics structures and the integration of small and medium-sized enterprises (SMEs) into sustainable maritime supply chains. The study was grounded in expert interviews and case analyses, offering qualitative insights into the barriers and enablers of blockchain adoption. Wagner and Wiśnicki (2019) classified existing and planned blockchain applications in maritime shipping through web content analysis and multi-case studies. The authors noted that while many container shipowners are involved in blockchain projects, these account for ∼84% of the world's container fleet tonnage, suggesting a concentration of innovation among large operators.

Economic considerations have also been analyzed in recent literature. Peronja et al. (2020) quantified the time and cost savings enabled by blockchain, particularly in container freight rates, offering predictive scenarios for cost evolution under blockchain adoption. In parallel, novel applications of blockchain in maritime IoT and secure communications have emerged. Rahimi et al. (2020) proposed a blockchain-based authentication mechanism for UAV-assisted maritime sensing systems. By employing a private blockchain linked to a terrestrial fusion center, their system validates received packets using stored blockchain identities to prevent unauthorized access and intrusions.

Self-Sovereign Identity (SSI) technology has the potential to further enhance decentralized systems by providing robust identity management. SSI relies on DIDs and VCs, ensuring privacy and security. Although SSI has been recognized for its potential in maritime and satellite communications (Čučko et al., 2023;

Ma et al., 2022), its integration into Blockchain-based systems remains limited. Efforts have primarily focused on authentication protocols and access control frameworks, with minimal exploration of how SSI can revolutionize identity management in these domains (Bolgouras et al., 2022).

Despite the significant advancements in satellite and maritime communications using Blockchain technology, one critical gap remains: the integration of SSI. Most existing research focuses on improving data integrity (Muñoz et al., 2021, 2020), authentication (Farao et al., 2021), and decentralized management. However, the potential of SSI to provide secure and private identity management, especially in Blockchain-based systems, is largely unexplored. This work addresses that gap by combining SSI with Blockchain to create more efficient, secure, and privacy-respecting solutions for maritime communications. Our approach aims to bring innovative identity management and coordination capabilities to these critical communication networks.

9 Conclusions

This article introduces a novel maritime authorization framework, B2SAPP, which leverages well-established technologies. On the one hand, Hyperledger Fabric participates as the crux of B2SAPP, offering Smart Contracts and secure storage to ensure security, fairness, trust, and interoperability among participating entities. On the other hand, Hyperledger Aries provides essential functionalities such as data minimization, robust identification, data interoperability, portability, decentralization, and transparency. The integrated use of Hyperledger Fabric and Hyperledger Aries has effectively enabled B2SAPP to address common maritime cybersecurity challenges. Additionally, this article presents a comprehensive performance evaluation of both utilized technologies, confirming B2SAPP's effectiveness and efficiency. Furthermore, the security and privacy appraisal complements the performance assessment by demonstrating B2SAPP's capability to defend against various well-known cybersecurity attacks and to fulfill cyber insurance security and privacy requirements. The findings of this research are intended to serve as a foundation for designing robust cybersecurity frameworks and architectures that will shape the future of the cyber insurance ecosystem.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

AF: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. AZ: Writing – original draft, Writing – review & editing, Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization. AV: Writing – original draft, Writing – review & editing. GP: Writing – original draft, Writing – review & editing. CX: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This research has received funding from European Commission's Horizon Europe and Horizon 2020 research and innovation programs under grant agreements No. 101082440 (CHRISS), No. 101092702 (OASEES), No. 101131481 (SOVEREIGN), and No. 101120962 (RESCALE).

Conflict of interest

AF was employed by InQbit Innovations SRL.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Afenyo, M., and Caesar, L. D. (2023). Maritime cybersecurity threats: gaps and directions for future research. *Ocean Coast. Manage.* 236:106493. doi: 10.1016/j.ocecoaman.2023.106493

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network* 2, 123–138. doi: 10.3390/network2010009

Anderson, J., Lo, S., and Walter, T. (2022). "Efficient and secure use of cryptography for watermarked signal authentication," in *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation* (Long Beach, CA), 68–82. doi: 10.33012/2022.18228

Anderson, J. M., Carroll, K. L., DeVilbiss, N. P., Gillis, J. T., Hinks, J. C., O'Hanlon, B. W., et al. (2017). "Chips-message robust authentication (CHIMERA) for GPS civilian signals," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)* (Portland, OR), 2388–2416. doi: 10.33012/2017.15206

Ardizzon, F., Crosara, L., Tomasin, S., and Laurenti, N. (2023). On the limits of cross-authentication checks for gnss signals. *arXiv* [Preprint] arXiv:2304.02977. doi: 10.48550/arXiv.2304.02977

Bolgouras, V., Angelogianni, A., Politis, I., and Xenakis, C. (2022). "Trusted and secure self-sovereign identity framework," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–6. doi: 10.1145/3538969.3544436

Cancela, S., Calle, J. D., and Fernández-Hernández, I. (2019). "CPU consumption analysis of tesla-based navigation message authentication," in *2019 European Navigation Conference (ENC)* (Warsaw: IEEE), 1–6. doi: 10.1109/EURONAV.2019.8714171

Caparra, G., Sturaro, S., Laurenti, N., and Wullems, C. (2016). "Evaluating the security of one-way key chains in tesla-based gnss navigation message authentication schemes," in *2016 International Conference on Localization and GNSS (ICL-GNSS)* (Barcelona: IEEE), 1–6. doi: 10.1109/ICL-GNSS.2016.7533685

Chambers, S. (2025). *Voyager Worldwide Hit by Cyber Attack*. Splash247.com. Available online at: https://splash247.com/voyager-worldwide-hit-by-cyber-attack/ (Accessed July 17, 2025).

Chen, X., Luo, R., Liu, T., Yuan, H., and Wu, H. (2023). Satellite navigation signal authentication in gnss: a survey on technology evolution, status, and perspective for BDS. *Remote Sen*. 15:1462. doi: 10.3390/rs15051462

Chen, Y., Gao, W., Chen, X., Liu, T., Liu, C., Su, C., et al. (2021). Advances of SBAS authentication technologies. *Satell. Navig*. 2, 1–7. doi: 10.1186/s43020-021-00043-1

Chernyi, S. G., Marley, V. E., Lopyrev, S. S., Bulov, A. A., and Bordug, A. S. (2018). "Systems of identification authentication and encoding in maritime industry," in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* (New York City, NY: IEEE), 37–39. doi: 10.1109/EIConRus.2018.8317023

Clark, L., Tung, Y.-C., Clark, M., and Zapanta, L. (2020). "A blockchain-based reputation system for small satellite relay networks," in *2020 IEEE Aerospace Conference* (New York City, NY: IEEE), 1–8. doi: 10.1109/AERO47225.2020.9172516

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., and Guevara Carazas, F. J. (2024). Cybersecurity at sea: a literature review of cyber-attack impacts and defenses in maritime supply chains. *Information* 15:710. doi: 10.3390/info15110710

Čučko, Š., Keršič, V., Turkanović, M. (2023). Towards a catalogue of self-sovereign identity design patterns. *Appl. Sci*. 13:5395. doi: 10.3390/app13095395

Curren, S., Looker, T., and Terbu, O. (2022). *DIDComm Messaging v2.0*. Available online at: https://identity.1142foundation/didcomm-messaging/spec/v2.0/ (Accessed July 17, 2025).

Danilin, G., Sokolov, S., Knysh, T., and Singh, V. (2021). "Information security incidents in the last 5 years and vulnerabilities of automated information systems in the fleet," in *International Scientific Siberian Transport Forum* (Cham: Springer), 1541–1550. doi: 10.1007/978-3-030-96383-5_172

Divis, D. A. (2019). *New Chimera Signal Enhancement Could Spoof-proof GPS Receivers*. Red Bank, NJ: Inside GNSS.

Dong, C., Jiang, F., Li, X., Yao, A., Li, G., Liu, X., et al. (2021). "A blockchain-aided self-sovereign identity framework for edge-based UAV delivery system," in *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)* (New York City, NY: IEEE), 622–624. doi: 10.1109/CCGrid51090.2021.00074

Dong, C., Wang, Z., Chen, S., and Xiang, Y. (2020). "BBM: a blockchain-based model for open banking via self-sovereign identity," in *International Conference on Blockchain* (Cham: Springer), 61–75. doi: 10.1007/978-3-030-59638-5_5

Dong, C., Yao, A., Xu, Z., Lu, M., Jiang, F., Chen, S., et al. (2024). "A blockchain-based self-sovereign identity system for kyc processes," in *Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure* (New York, NY: ACM), 1–11. doi: 10.1145/3659463.3660026

Duan, Y., Huang, J., Lei, J., Kong, L., Lv, Y., Lin, Z., et al. (2022). Aischain: blockchain-based ais data platform with dynamic bloom filter tree. *IEEE Trans. Intell. Transp. Syst*. 24, 2332–2343. doi: 10.1109/TITS.2022.3188691

Elmay, F. K., Salah, K., Yaqoob, I., Jayaraman, R., Battah, A., Maleh, Y., et al. (2022). Blockchain-based traceability for shipping containers in unimodal and multimodal logistics. *IEEE Access* 10, 133539–133556. doi: 10.1109/ACCESS.2022.3231689

Farah, M. B., Ahmed, Y., Mahmoud, H., Shah, S. A., Al-Kadri, M. O., Taramonli, S., et al. (2024). A survey on blockchain technology in the maritime industry: challenges and future perspectives. *Future Gener. Comput. Syst*. 157, 618–637. doi: 10.1016/j.future.2024.03.046

Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., et al. (2020). "Secondo: a platform for cybersecurity investments and cyber insurance decisions," in *Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14-17, 2020, Proceedings 17* (Cham: Springer), 65–74. doi: 10.1007/978-3-030-58986-8_5

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., Xenakis, C., et al. (2024). Inchain: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *Int. J. Inf. Secur*. 23, 347–371. doi: 10.1007/s10207-023-00741-8

Farao, A., Veroni, E., Ntantogian, C., and Xenakis, C. (2021). P4g2go: a privacy-preserving scheme for roaming energy consumers of the smart grid-to-go. *Sensors* 21:2686. doi: 10.3390/s21082686

Freire, W. P., Melo, W. S. Jr., do Nascimento, V. D., Nascimento, P. R., and de Sá, A. O. (2022). Towards a secure and scalable maritime monitoring system using blockchain and low-cost iot technology. *Sensors* 22:4895. doi: 10.3390/s22134895

Gao, N., Han, D., Weng, T.-H., Xia, B., Li, D., Castiglione, A., et al. (2022). Modeling and analysis of port supply chain system based on fabric blockchain. *Comput. Ind. Eng*. 172:108527. doi: 10.1016/j.cie.2022.108527

Gao, W., Hei, X., and Wang, Y. (2023). The data privacy protection method for hyperledger fabric based on trustzone. *Mathematics* 11:1357. doi: 10.3390/math11061357

Ghorbani, K., Orouji, N., and Mosavi, M. R. (2020). Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS l1. *Wirel. Pers. Commun*. 113, 1743–1754. doi: 10.1007/s11277-020-07289-z

Goudosis, A., and Katsikas, S. (2022). Secure automatic identification system (SECAIS): proof-of-concept implementation. *J. Mar. Sci. Eng*. 10:805. doi: 10.3390/jmse10060805

Hyperledger Fabric (2025a). *Frequently Asked Questions*. Available online at: https://hyperledger-fabric.readthedocs.io/ml/release-2.5/Fabric-FAQ.html (Accessed July 17, 2025).

Hyperledger Fabric (2025b). *Setting up the Development Environment*. Available online at: https://hyperledger-fabric.readthedocs.io/es/latest/dev-setup/devenv.html (Accessed July 17, 2025).

Kjærsgaard, L. F. (2020). Blockchain technology and the allocation of taxing rights to payments related to initial coin offerings. *Intertax* 48, 879–903. doi: 10.54648/TAXI2020088

Korpela, K., Hallikas, J., and Dahlberg, T. (2017). "Digital supply chain transformation toward blockchain integration", in *Proceedings of Hawaii International Conference on System Sciences*, 4182–4191. doi: 10.24251/HICSS.2017.506

Kouhizadeh, M., Saberi, S., and Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers. *Int. J. Prod. Econ*. 231:107831. doi: 10.1016/j.ijpe.2020.107831

LF Decentralized Trust (2025a). *Caliper*. Available online at: https://www.lfdecentralizedtrust.org/projects/caliper (Accessed July 17, 2025).

LF Decentralized Trust (2025b). *Hyperledger Aries*. Available online at: https://www.lfdecentralizedtrust.org/projects/aries (Accessed July 17, 2025).

LF Decentralized Trust (2025c). *Type: Distributed Ledger Software*. Available online at: https://www.lfdecentralizedtrust.org/projects/fabric (Accessed July 17, 2025).

Li, F., Lam, K.-Y., Jia, M., Zhao, J., Li, X., Wang, L., et al. (2020). Blockchain-based approach for securing spectrum trading in multibeam satellite systems. *arXiv* [Preprint] arXiv:2012.10681. doi: 10.48550/arXiv.2012.10681

Liu, C., Zhang, Y., Niu, G., Jia, L., Xiao, L., Luan, J., et al. (2023a). Towards reinforcement learning in UAV relay for anti-jamming maritime communications. *Digit. Commun. Netw*. 9, 1477–1485. doi: 10.1016/j.dcan.2022.08.009

Liu, J., Zhang, H., and Zhen, L. (2023b). Blockchain technology in maritime supply chains: applications, architecture and challenges. *Int. J. Prod. Res*. 61, 3547–3563. doi: 10.1080/00207543.2021.1930239

Ma, B., Zheng, X., Zhao, C., Wang, Y., Wang, D., and Meng, B. (2022). A secure and decentralized SSI authentication protocol with privacy protection and fine-grained access control based on federated blockchain. *PLoS One* 17:e0274748. doi: 10.1371/journal.pone.0274748

Maersk (2022). *A.P. Moller - Maersk and IBM to Discontinue TradeLens, a Blockchain-Enabled Global Trade Platform – maersk.com*. Available online at: https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens (Accessed July 17, 2025).

Malik, S., Dedeoglu, V., Kanhere, S. S., and Jurdak, R. (2019). "Trustchain: trust management in blockchain and iot supported supply chains," in *2019 IEEE International Conference on Blockchain (Blockchain)* (Atlanta, GA: IEEE), 184–193. doi: 10.1109/Blockchain.2019.00032

Malik, S., Kanhere, S. S., and Jurdak, R. (2018). "Productchain: scalable blockchain framework to support provenance in supply chains," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)* (Cambridge, MA: IEEE), 1–10. doi: 10.1109/NCA.2018.8548322

McDaniel, C. A., and Norberg, H. C. (2019). *Can Blockchain Technology Facilitate International Trade*? Mercatus Research Paper. Arlington, VA: Elsevier. doi: 10.2139/ssrn.3377708

Muñoz, A., Farao, A., Correia, J. R. C., and Xenakis, C. (2020). "ICITPM: integrity validation of software in iterative continuous integration through the use of trusted platform module (TPM)," in *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17-18, 2020, Revised Selected Papers 25* (Cham: Springer), 147–165. doi: 10.1007/978-3-030-66504-3_9

Muñoz, A., Farao, A., Correia, J. R. C., and Xenakis, C. (2021). P2ise: preserving project integrity in ci/cd based on secure elements. *Information* 12:357. doi: 10.3390/info12090357

Ni, L., and Irannezhad, E. (2024). Performance analysis of logisticchain: a blockchain platform for maritime logistics. *Comput. Ind.* 154:104038. doi: 10.1016/j.compind.2023.104038

Nicola, M., Motella, B., and Gamba, M. T. (2021). "GPS chimera: a software receiver implementation," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2021)* (St. Louis, MO), 4264–4273. doi: 10.33012/2021.18127

Oloruntobi, O., Mokhtar, K., Gohari, A., Asif, S., and Chuah, L. F. (2023). Sustainable transition towards greener and cleaner seaborne shipping industry: challenges and opportunities. *Clean. Eng. Technol.* 13:100628. doi: 10.1016/j.clet.2023.100628

OpenWallet Foundation (2025). *ACA-Py-A Cloud Agent - Python*. Available online at: https://github.com/openwallet-foundation/acapy (Accessed July 17, 2025).

Pantelakis, V., Bountakas, P., Farao, A., and Xenakis, C. (2023). "Adversarial machine learning attacks on multiclass classification of iot network traffic," in *Proceedings of the 18th International Conference on Availability, Reliability and Security* (New York, NY: ACM), 1–8. doi: 10.1145/3600160.3605086

Paparis, G., Zarras, A., Farao, A., and Xenakis, C. (2025). Crashed: cyber risk assessment for smart home electronic devices. *J. Inf. Secur. Appl.* 91:104054. doi: 10.1016/j.jisa.2025.104054

Peronja, I., Lenac, K., and Glavinović, R. (2020). Blockchain technology in maritime industry. *Pomorstvo* 34, 178–184. doi: 10.31217/p.34.1.19

Perrig, A., Canetti, R., Tygar, J. D., and Song, D. (2002). The tesla broadcast authentication protocol. *RSA CryptoBytes* 5:2002.

Perrig, A., and Tygar, J. (2003). "Tesla broadcast authentication," in *Secure Broadcast Communication. Wired and Wireless Networks* (Cham: Springer), 29–53. doi: 10.1007/978-1-4615-0229-6_3

Petihakis, G., Farao, A., Bountakas, P., Sabazioti, A., Polley, J., Xenakis, C., et al. (2024). "AIAS: AI-assisted cybersecurity platform to defend against adversarial ai attacks," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–7. doi: 10.1145/3664476.3669920

Philipp, R., Prause, G., and Gerlitz, L. (2019). Blockchain and smart contracts for entrepreneurial collaboration in maritime supply chains. *Transp. Telecommun.* 20, 365–378. doi: 10.2478/ttj-2019-0030

Polatidis, N., Pavlidis, M., and Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand Interfaces* 56, 74–82. doi: 10.1016/j.csi.2017.09.006

Potamos, G., Theodoulou, S., Stavrou, E., and Stavrou, S. (2023). "Building maritime cybersecurity capacity against ransomware attacks," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20-21 June; Wales*(Cham: Springer), 87–101. doi: 10.1007/978-981-19-6414-5_6

Rahimi, P., Khan, N. D., Chrysostomou, C., Vassiliou, V., and Nazir, B. (2020). "A secure communication for maritime iot applications using blockchain technology," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (Marina del Rey, CA: IEEE), 244–251. doi: 10.1109/DCOSS49796.2020.00047

Raza, Z., Woxenius, J., Vural, C. A., and Lind, M. (2023). Digital transformation of maritime logistics: exploring trends in the liner shipping segment. *Comput. Ind.* 145:103811. doi: 10.1016/j.compind.2022.103811

Shirani, A. (2018). Blockchain for global maritime logistics. *Issues Inf. Syst.* 19, 175–183. doi: 10.48009/3_iis_2018_175-183

Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., and Bauer, J. (2023). Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. *J. Mar. Sci. Eng.* 11:928. doi: 10.3390/jmse11050928

Suciu, G., Farao, A., Bernardinetti, G., Palamà, I., Sachian, M.-A., Vulpe, A., et al. (2022). SAMGRID: security authorization and monitoring module based on SealedGRID platform. *Sensors* 22:6527. doi: 10.3390/s22176527

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., and Shaw, E. (2024). Cyberattacks on the maritime sector: a literature review. *J. Mar. Sci. Appl.* 23, 689–706. doi: 10.1007/s11804-024-00443-0

Tabish, N., and Chaur-Luh, T. (2024). Maritime autonomous surface ships: a review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access* 12, 17114–17136. doi: 10.1109/ACCESS.2024.3357082

Tedeschi, P., Sciancalepore, S., and Di Pietro, R. (2022). Satellite-based communications security: a survey of threats, solutions, and research challenges. *Comput. Netw.* 216:109246. doi: 10.1016/j.comnet.2022.109246

The Maritime Executive (2025). *Sembmarine Reports Cyber Breach Affecting Information on Personnel – maritime-executive.com*. Available online at: https://maritime-executive.com/article/sembmarine-reports-cyber-breach-affecting-information-on-personnel

The Record (2024). *Ransomware Attack on Maritime Software Impacts 1,000 Ships – therecord.media*. Available online at: https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships (Accessed July 17, 2025).

The Record (2025a). *Dutch Shipping Giant Royal Dirkzwager Confirms Play Ransomware Attack – therecord.media*. Available online at: https://therecord.media/royal-dirkzwager-ransomware-attack-dutch-shipping (Accessed July 17, 2025).

The Record (2025b). *Port of Lisbon Website Still Down as LockBit Gang Claims Cyberattack – therecord.media*. Available online at: https://therecord.media/port-of-lisbon-website-still-down-as-lockbit-gang-claims-cyberattack (Accessed July 17, 2025).

Torky, M., Gaber, T., Goda, E., Snasel, V., and Hassanien, A. E. (2022). A blockchain protocol for authenticating space communications between satellites constellations. *Aerospace* 9:495. doi: 10.3390/aerospace9090495

Tsiulin, S., Reinau, K. H., Hilmola, O.-P., Goryaev, N., and Karam, A. (2020). Blockchain-based applications in shipping and port management: a literature review towards defining key conceptual frameworks. *Rev. Int. Bus. Strategy* 30, 201–224. doi: 10.1108/RIBS-04-2019-0051

Voudouris, A., Farao, A., Panou, A., Polley, J., and Xenakis, C. (2024). "Integrating hyperledger fabric with satellite communications: a revolutionary approach for enhanced security and decentralization in space networks," in *Proceedings of the 19th International Conference on Availability, Reliability and Security* (New York, NY: ACM), 1–8. doi: 10.1145/3664476.3669921

Wagner, N., and Wiśnicki, B. (2019). "Application of blockchain technology in maritime logistics," in *DIEM: Dubrovnik International Economic Meeting, Volume 4* (Dubrovnik: Sveučilište u Dubrovniku), 155–164.

Wang, Z., Cao, M., Jiang, H., Cao, B., Wang, S., Sun, C., et al. (2024). Blockchain-enabled dynamic spectrum sharing for satellite and terrestrial communication networks. *arXiv* [Preprint]. arXiv:2408.02013. doi: 10.48550/arXiv.2408.02013

World Wide Web Consortium (W3C) (2025). *Decentralized Identifiers (DIDs) v1.0*. Available online at: https://www.w3.org/TR/did-core/ (Accessed July 17, 2025).

Xu, R., Chen, Y., Blasch, E., and Chen, G. (2019). Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. *Opt. Eng.* 58:041609. doi: 10.1117/1.OE.58.4.041609

Yu, H., Meng, Q., Fang, Z., and Liu, J. (2023). Literature review on maritime cybersecurity: state-of-the-art. *J. Navig.* 76, 453–466. doi: 10.1017/S0373463323000164

Yuan, M., Tang, X., and Ou, G. (2023). Authenticating gnss civilian signals: a survey. *Satell. Navig.* 4:6. doi: 10.1186/s43020-023-00094-6

Zhang, Y.-H., and Liu, X. F. (2020). "Satellite broadcasting enabled blockchain protocol: a preliminary study," in *2020 Information Communication Technologies Conference (ICTC)* (Nanjing: IEEE), 118–124. doi: 10.1109/ICTC49638.2020.9123248