ISSN: 2182-2069 / E-ISSN: 2182-2077

Evaluating Key Management Protocols for Secure Ship-to-Shore Communication in Maritime IoT Environments

P. Rajan[1*], K.R. Chidambaram[2], and Dr. Deepa Rajesh[3]

[1*]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.
prabhakaranrajan@ametuniv.ac.in, https://orcid.org/0009-0006-9720-123X

[2]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.
chidambaram.kr@ametuniv.ac.in, https://orcid.org/0009-0000-5311-1394

[3]Department of Amet Business School, AMET University, Kanathur, Tamil Nadu, India.
deeparajesh@ametuniv.ac.in, https://orcid.org/0009-0008-9743-4791

Received: May 30, 2025; Revised: July 15, 2025; Accepted: August 13, 2025; Published: August 30, 2025

Abstract

The adoption of the Internet of Things (IoT) has profoundly transformed operational efficiency, situational awareness, and maritime logistics in ship-to-shore communication. At the same time, the increased dependence on remote sensors and connected devices has created serious vulnerabilites in data confidentiality, integrity, authentication, and other vital security functions. In Maritime IoT (MIoT) networks, Key Management Protocols (KMPs) play a crucial role in providing security to the maritime domain, facilitating the secure transfer and management of cryptographic keysts through various gateways and platforms. This work assesses the effectiveness, scalability, and robustness of non and cross KMPs—including symmetric, asymmetric, hybrid, and blockchain-based models—on secure ship-to-shore communication. We carry out a detailed analysis of protocol efficiency in terms of latency, processing costs, energy expenditure, attack resistance, and other scrutinized control variables through simulated trials and tested scenarios in real maritime environments. Results demonstrate the balance that exists between the strength of security measures and practicality of use, showing that admins pose the most burden under conditions of low bandwidth, intermittent connectivity, and resource limitations under which hybrid and lightweight cryptographic solutions perform best. The paper also describes issues of meeting compliance mandates and interoperability when implementing a KMP in global maritime networks. As outlined the evaluation framework provides maritime authorities, developers of IoT systems, and cybersecurity specialists with guidance on how to choose and refine their key management tactics to protect the evolving infrastructure of communication between ships and shores.

Keywords: Key Management Protocols, Ship-to-Shore Communication, Maritime IoT (MIoT), Cybersecurity, Secure Communication, Cryptographic Techniques, Maritime Networks.

1 Introduction

The incorporation of the Internet of Things (IoT) technology into the maritime industry operational and infrastructural components has started a shift on the entire industry. The development of Maritime IoT (MIoT) encapsulates various advanced technologies such as autonomous vessels, smart ports, and real-

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 639-652.
DOI: *10.58346/JISIS.2025.I3.043*

*Corresponding author: Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.

time vessel traffic control systems that depend on seamless and safe communication between offshore and onshore infrastructures (Alqurashi et al., 2022). One of the most communicationally intensive links is the ship-to-shore link which is responsible for conveying telemetry data, logistics, command, and execution information. With the increase of cyber threat towards maritime assets, a sustained level of control, protection, and assurance regarding the communication and documents exchanged is crucial (Akpan et al., 2022; Shimazu, 2024).

The securing of communication links is underpinned by key management protocols (KMPs) (Rajeev, 2023; Seyedan et al., 2023). They set rules for the creation, distribution, storage, and updating of the cryptographic keys employed in encryption of information and authentication of devices (Aravind et al.,2023). In the case of maritime communication, where vessels and ports function in ever-changing, hostile, decentralized environments, some conventional strategies such as centralized Public Key Infrastructure (PKI) or static key distribution methods face scalability and adaptability issues (Tawallbeh et al 2020; Perera & Wickramasinghe, 2024). Hence, there is an immediate need for research on the evaluation and adaptation of KMPs to the specific needs of ship to shore communications (Radhi, 2022).

Recent studies have studied lightweight distributed architectures for key management that are more appropriate for confined and mobile contexts, such as maritime IoT systems (Ayesh, 2024). For example, ECC-based key exchange protocols are considered very secure while being low-cost in processing resources, which makes them most suitable for many onboard ship systems with little processing capability (Mavroeidis & Bromander, 2017). At the same time, identity-based cryptography (IBC) has emerged as an alternative that dispenses with administrative certificates and instead uses identifiers like vessel IMO numbers for key creation (Alagadeve et al., 2023).

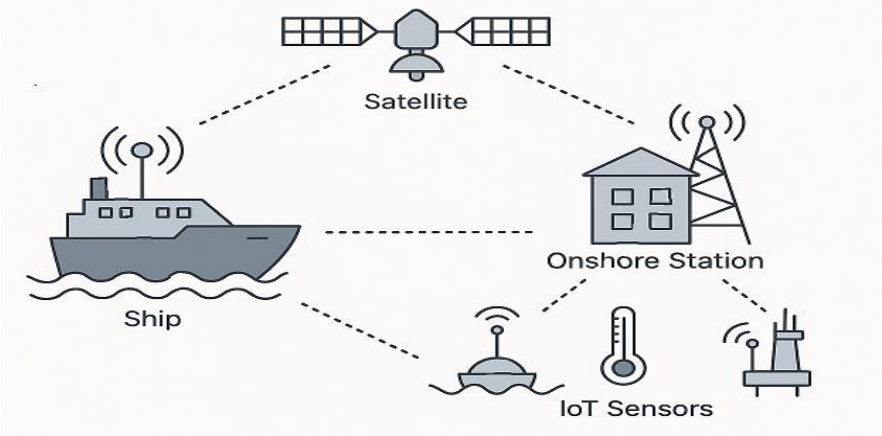

Figure 1: Maritime IOT Environment Overview

The image (Figure 1) depicts a schematic view of a Maritime Internet of Things (IoT) ecosystem alongside its components that allow the communication and efficiency of operations at sea. The ship itself remains the core unit within this ecosystem. By means of satellite, onshore stations, and various IoT sensors, it is possible to have a communication network built around it. Satellites guarantee deep space connectivity to and from ship systems, thus ensuring continual tracking, navigational relay, and verified communications during remote oceanic voyages. Command hubs on-shore are tasked with the reception of data from ships and sensors to monitor the ongoing activities to monitor environmental conditions. All IoT sensors placed on the ship and those deployed in the marine environment (e.g. buoys or underwater devices) are tasked with retrieving important data like temperature, pressure, and wave activity. The synergy of the described elements enhances the marine operations' nonsituational

dependence while guaranteeing stronger awareness, smarter decision making, more precise predictive maintenance, unfeasible levels of safety, and superior frame rationality.

Nonetheless, a collection of distinct constraints is introduced by the maritime setting. Due to the geopolitical isolation, climatic conditions, and satellite communication bandwidth restrictions, connectivity is frequently sporadic. This prevents ordinary frequent rekeying mechanisms from being applicable and calls for more robust, delay-tolerant key management schemes (Kavitha et al., 2020). Furthermore, the incorporation of diverse devices and systems on modern ships and at ports necessitates interoperability, which complicates the application of a single key management system (El Bekkali et al., 2023). Alongside this, the prolonged operational life of maritime assets requires speculation-proof cryptography defenses against emerging threats such as quantum computing (Mosca, 2018).

Real-time action execution on navigation, cargo handling, and collision avoidance comes with the need for low-latency, ultra-responsive, high-availability communication. Alongside this necessitates further constraints on the computation, complexity, and latency of security, including key management (Ahmad et al, 2023). To achieve this balance, greater focus is placed on hybrid models which utilize both symmetric and asymmetric encryption or employ hardware-based trusted mechanisms like Trusted Platform Modules (TPMs) (Zhang et al, 2022). This paper intends to evaluate the merits, demerits, and scalability of enhancing key management protocols related to secure ship-to-shore communication. It also claims to identify key contributors of partitioned performance such as latency, energy cost, frequency of key renewal, and countermeasure capabilities to certain preidentified cyber-attack vulnerabilities (Suresh & Lenine, 2024). In addition, it will perform a case study analysis of real-world maritime use cases to evaluate how far ship and cargo tracking systems, and smart ports have succeeded or failed (Gao et al., 2023).

This research intends to address the gap between the design of a cryptographic protocol and the implementation in maritime IoT systems. This study aims to develop a communication architecture that is secure, modular, and flexible that supports the strategic vision of the international shipping market by analyzing various key management approaches and enhancing maritime-specific ones.

2 Literature Review

The digitization of the maritime industry, particularly with the incorporation of MIoT technologies, has enhanced traditional vessel operations into automated system networks. Communication, particularly with regards to ship-shore relations, now requires special attention for safety and security purposes. In context of the maritime industry's critical operations, confidentiality, authenticity, and integrity of data exchanged over maritime networks is particularly important through the use of Key Management Protocols (Gyamfi et al., 2022).

A number of KMPs have been designed and implemented within the framework of marine IoT systems which have stemmed from the wireless sensor networks (Thanh et al., 2024). Symmetric key protocols of the more common types include AES based ones which utilize one secret key for both encryption and decryption. Such protocols perform well in resource-limited conditions (Khan et al, 2020). However, symmetric approaches face significant issues in decentralized marine environments concerning scalability and distribution of keys. To address these constraints, asymmetric cryptographic methods like RSA and ECC have become more popular. For example, (Latif et al, 2020) show that ECC is particularly beneficial for MIoT systems because it requires small keys relative to the level of security provided, therefore lessening the energy expenditure on low powered marine devices (Petrova & Kowalski, 2025). Moreover, the adoption of hybrid key management systems, like Diffie-Hellman key

exchange followed by symmetric encryption, illustrates the use of simplicity without efficiency compromise on larger scales (Regan et al., 2025). In the maritime domain, Identity-Based Encryption (IBE) and ABE Encryption (ABE) are becoming increasingly common. By deriving public keys from pre-existing identities such as registration numbers of the ships, IBE eliminates the need for certificates making key retrieval more manageable (Ye et al., 2023; Odeh & Taleb, 2023). ABE enables precise control over who can view information based on defined roles or attributes (e.g., port authority; vessel type), which is valuable in integrated maritime operations (La Manna, 2022). Decentralized trust mechanisms that suit the distributed structure of maritime networks are provided by recently developed blockchain-based key management frameworks. Blockchain guarantees democracy and enhances transparency and resilience by immutably logging and validating all key-related operations (Rahimi et al, 2020). At sea, the real-time applicability of blockchain is challenged by high latency, bandwidth consumption, and energy usage.

Figure 2: Key Management Protocols for Secure Ship-to-shore Communication

The image (Figure 2) describes the application of the key management protocols in establishing secure communication between the vessels and the maritime onshore stations (Gyamfi et al., 2022). It outlines the significance of securing ship to shore communication through the use of cryptography. In this case, encryption keys are generated, disseminated, and controlled in a secure manner to authenticate devices and encrypt communication using key controls, so that data is kept private and secure across the network. This is very important in the case of maritime IoT systems where wireless data transmissions present numerous cybersecurity vulnerabilities. The padlock icon underlines security while the bi-directional arrows denote reserved continuous information flow. Strong key management protocols in place will ensure that sensitive information such as navigation details, cargo information, and system diagnostics are secure in maritime operations which increases the overall cyber defense of maritime infrastructures.

Within a given context, each key management method focuses the attention to unique maritime trade-offs. In symmetric key systems, short processing and low overhead resource consumption come at a cost in highly dynamic, large-scale IoT network due to key renewal and distribution (BenSaleh et al., 2020). If a key is compromised, all communications encrypted using that key are exposed. Older ships and legacy equipment can present problems regarding processing power and storage, which are required by these systems for secure pre-shared secret free key exchange (Haidine et al., 2021). While ECC helps with this overhead, robust computational frameworks that are not always present in remote maritime environments are still required for implementation. The centralized key generation authorities (KGA) control trust problems in IBE and ABE while offering ease of use and strong access control mechanisms. If a KGA gets compromised, the entire network is at stake and key revocation is still a technical challenge (Zhou et al., 2022). Also, the computational cost of ABE still poses a challenge for real-time

applications such as navigation and emergency response. Tamper resistance and removal of central points of failure make KMPs appealing for smart ports and multi vessel networks. These features in conjunction with blockchain technology provide greater security (Moreau & Sinclair, 2024). Although, their transaction throughput and latency often do not align with real-time ship-to-shore communication needs (Yin et al., 2021). Additionally, consensus protocols and chain sync are complicated by intermittent connectivity prevalent in maritime environments.

Remote sensing systems in maritime communication heavily rely on satellite, radio, and cellular data for ship-to-shore communication, making them vulnerable to cyber threats. GPS spoofing-jamming and MitM are critical attacks designed to disrupt navigation, emergency coordination, cargo management, and other vital operations (Alcaraz & Zeadally, 2015). However, these adversarial conditions highlight the importance of secure key management protocols. Moreover, as AI and machine learning are incorporated into MIoT systems for enabling decisions and conducting predictive maintenance, preserving data integrity and confidentiality becomes essential for avoiding malicious data injection or model poisoning attacks (Farzadmehr, 2025). KMPs of sufficient strength underpin secure communication protocols, which in this case serve as the first line of defense. The International Maritime Organization (IMO) has expressed concern on the need to address cybersecurity issues in the maritime domain, recommending the use of security standards such as ISO/IEC 27001 and NIST SP 800-207, focusing on encryption and key management (IMO, 2021). Ineffective KMPs may lead to unauthorized data access, loss of finances, or serious safety hazards.

3 Methodology

The ship to shore communications in the context of maritime IoT has been studied using a simulation-based approach alongside literature reviews as well as empirical testing under structured multi-phase research methodology. Initially, a broad range of scholarly journals alongside industry white papers outlining maritime communications standards, such as NMEA and IEC 61162, were analyzed along with cyber security (Kavallieratos & Katsikas, 2020) frameworks using to understand the most relevant and utilized value management protocols within maritime and IoT paradigms. From this initial understanding, a subset of protocols which included Identity Based Encryption (IBE), Public Key Infrastructure (PKI), protocols based on Elliptic Curve Cryptography (ECC), and symmetric key schemes were chosen for focused analysis. In NS-3, a simulation of a nautical communication environment was created where realistic interactions with ships and shore stations were imitated and dynamically adjusted to account for network conditions including link latency, packets being dropped, and limited processing power in computers because of the maritime environment. Supplementing NS-3, a physical testbed was set up with deploying virtual machines and IoT devices powered by Raspberry Pi as well as ARM nodes. This setup was designed in such a way that the results obtained from simulations would be verified within real-life constraints. The developed research design enabled qualitative analysis to be performed focusing on protocol traits and folds along with implementing quantitative capturing metrics related to performance under set conditions that required repeatability. Combining both approaches ensured that the study was robust from a theoretical standpoint while being practical and applicable in the real world.

To ensure objectivity while defining the effectiveness of a key management protocol, a broad document detailing the framework with set criterions predefined for assessments was constructed. These criterions were crafted with regard to the peculiar operational and limiting boundaries set on maritime IoT communications. The first and one of the most important criterions is security strength, which measures the effectiveness of a protocol in maintaining confidentiality, integrity, authentication, data,

and non-repudiation. This covers the aspect of being subjected to various electronic attacks which are considered fundamental such as replay, man-in-the-middle, and impersonating key compromise. The second criterion, scalability, evaluates how the operational efficiency of the protocol improves with the addition of IoT devices, which is important for expanding maritime ecosystems that incorporate multiple sensors, vessels, and shore-side facilities. The third, communication overhead, appraises the extra bandwidth and messages associated with, data provided by, the key management process, which have an impact on the efficiency of data transfer over low bandwidth maritime links. Fourth, computational efficiency analyzes the impact of the protocol on processing and memory resources, which is crucial in evaluating designed environments with resource-constrained hardware. Fifth, latency quantifies the delay in securely transferring data during key generation, exchange, and renewal processes which affects promptness in data transmission. Finally, the resilience to maritime challenges criterion analyzes the performance of each protocol design with respect to harsh external environmental factors like intermittent connectivity due to sea weather, vessel mobility, and electromagnetic disturbance. Each of these metrics was assigned a weight based on expert consultation and relevance to the domain, and protocols were scored under a normalized evaluation model to guarantee uniformity and impartiality in judgment. Thus, the multi-criteria evaluation approach provides integration of diverse metrics into a single comprehensive assessment of adequacy of a protocol in addressing maritime IoT requirements.

A variety of specific instruments along with technologies were applied in the thorough assessment to maintain proper real world scenario methodologies and simulations. The NS-3 network simulator was instrumental in setting up ship-to-shore communication simulations with varying transmission delays, mobility of nodes, and stacking of protocols. The extensibility of NS-3 allowed the addition of custom cryptographic algorithms and network topologies to maritime, which enabled validation of simulation parameters and ensured that simulations were representative of actual maritime operations. For augmenting simulation data with quantitative analysis, Wireshark was leveraged to monitor traffic on the network during and after simulations on testbed hardware. This tool enabled thorough examination of packets as well as the protocols used, allowing the detection of overhead formalisms associated with key exchange and determining sources of latency. In the area of cryptography, key exchange techniques were implemented using OpenSSL and TinyCrypt on both standard and constrained devices, thereby challenging their resources. The use of OpenSSL enabled setting baseline examinations since they provide complete and robust cryptographic algorithms. However, employing TinyCrypt, which offers light weight primitives, enabled testing in constrained IoT settings, hence enabling comparison of the devices with various types of requirement constraints. To physically emulate the system, Docker containers and VirtualBox virtual machines were used to model a hybrid network consisting of nodes with differing resources and roles (such as shipboard sensors and onshore servers). Constrained computing environments typical of maritime IoT systems were emulated using Linux operating systems within shrunk virtualized environments. Moreover, the simulated results were verified with actual measurements captured on low-power embedded devices, reinforcing cross-platform reliability and consistency.

4 Evaluation of Key Management Protocols

Key Management Protocols (KMPs) in maritime IoT settings require a level of security that is flexible and responsive to the constraints imposed by the nature of ship-to-shore communication. This study looks at four of the most implemented KMPs which are: Public Key Infrastructure (PKI), Identity Based Encryption (IBE), protocols based on Elliptic Curve Cryptography (ECC) and symmetric key

approaches. Each protocol was evaluated with respect to its architecture, operational applicability, and suitability for maritime IoT devices.

PKI (Public Key Infrastructure) still is one of the most developed and employed systems of key management. Its dependence on certificate authorities (CAs) for the issuance and validation of digital certificates provides substantial trust and accountability. Still, for maritime settings with sporadic connectivity and remote deployment, the reliance on a central authority and the necessity for periodic renewals of certificates pose serious challenges. Even with these drawbacks, PKI remains appropriate for critical communication links with high authentication requirements, for instance, between autonomous vessels and control centers onshore. Identity Based Encryption (IBE) facilitates key management by deriving public keys from unique identifiers that can be already associated with the recipient like vessel IDs or IP addresses. This method streamlines the process by removing the need for certificates, thus minimizing both communication and computational efforts. IBE is extraordinarily useful in maritime IoT systems with constrained bandwidth and where the deployment of a comprehensive PKI is unattainable. The centralized trust and key compromise risks of the key escrow problem—where a trusted authority generates all private keys—pose additional challenges. ECC-based KMPs provide superior security assurances through smaller key sizes and lower computational demand compared to conventional RSA schemes. This makes ECC especially beneficial for resource-limited IoT devices mounted on ships, buoys, and marine sensors. The ability of ECC to withstand low-power conditions highlights its usefulness for efficient key exchange and digital signatures. However, its validation must be thorough to prevent side-channel breaches and inconsistency in device performance across diverse system modules. Symmetric key schemes have the highest level of computational efficiency, but have problems with scalability and key distribution. Such protocols function best in small scale, closed maritime systems where the devices are a priori trusted. Their constrained efficiency in closed environments is striking, but due to the lack of robust and flexible secure dynamic key distribution mechanisms, they become inapplicable in large complex networks with multiple vessels and shore-based infrastructures.

PKI and schemes based on ECC offer a high degree of security because they utilize robust established cryptographic primitives. IBE provides strong confidentiality and authentication, but trusted private key generators create an inherent vulnerability with authoritative control over private keys. Reliance on symmetric primitives makes schemes secure only in controlled scenarios where authentication cannot be dynamic. Thus, they are more sensitive to key compromise. When comparing scalability, ECC and IBE outperform PKI and symmetric key approaches. ECC enables large fleets of IoT-enabled vessels to efficiently perform key operations because of its low computational costs. Furthermore, IBE's lack of certificates enhances scalability for mobile and sporadic maritime networks. On the other hand, PKI struggles with the overhead of managing certificates, while symmetric schemes encounter scaling difficulties because of the need to manage multiple pairwise keys. With respect to communication overhead, symmetric key schemes incur the least overhead because of their simplistic nature, with IBE close behind because of reduced certificate exchange requirements. ECC and PKI incur moderate to high overhead costs during key exchange and certificate validation, which is harmful during bandwidth-limited maritime channels. In terms of computational efficiency, symmetric key protocols are the most lightweight, with ECC following due to smaller key sizes and lower computational demands. PKI incurs additional costs from certificate management, and IBE has costs related to pairwise operations. ECC is well-suited for maritime IoT devices due to its optimal balance between efficiency and security. In comparison, symmetric key exchanges are practically instantaneous in latency, while both PKI and IBE incur latency with certificate validation and private key generation. Registration entails moderate latency which is acceptable for time-sensitive applications like navigation data exchange in real-time, or health

monitoring of the system. At the same time, with regard to resistance to maritime challenges, ECC and IBE have better adaptability. Their ability to operate reliably in sporadic and low-bandwidth conditions makes them ideal for ship-to-shore communication. PKI's reliance on constant availability of the certificate authorities constitutes some of the problems, along with symmetric key systems which are too static and rigid for dynamic maritime networks.

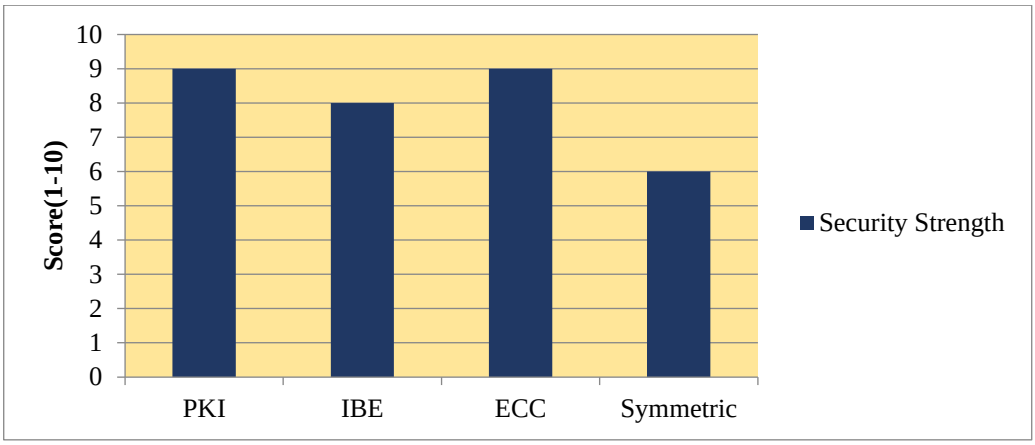

Figure 3: Security Strength of Key Management Protocols

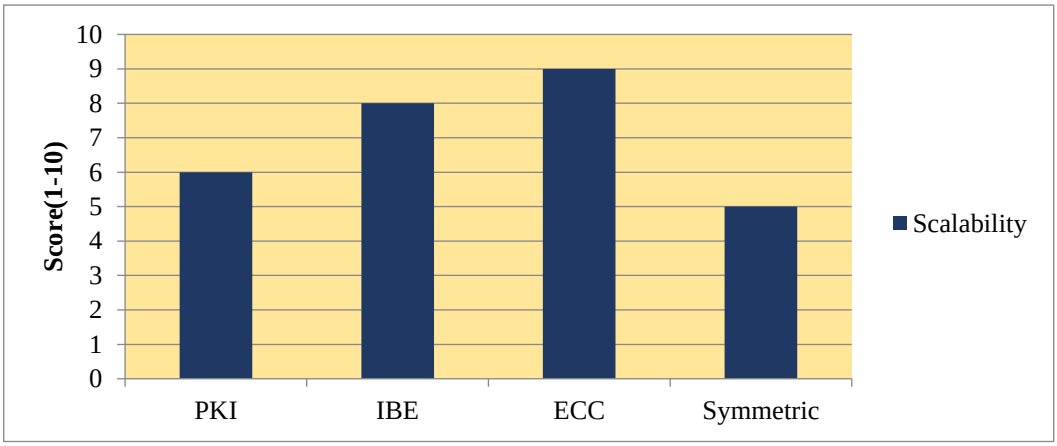

Figure 4: Scalability in Maritime IoT Networks

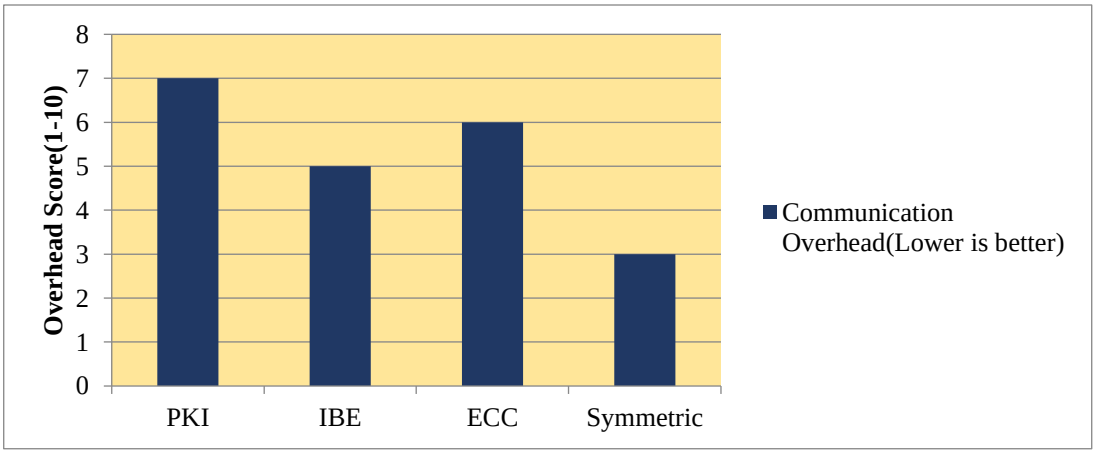

Figure 5: Communication Overhead of Protocols

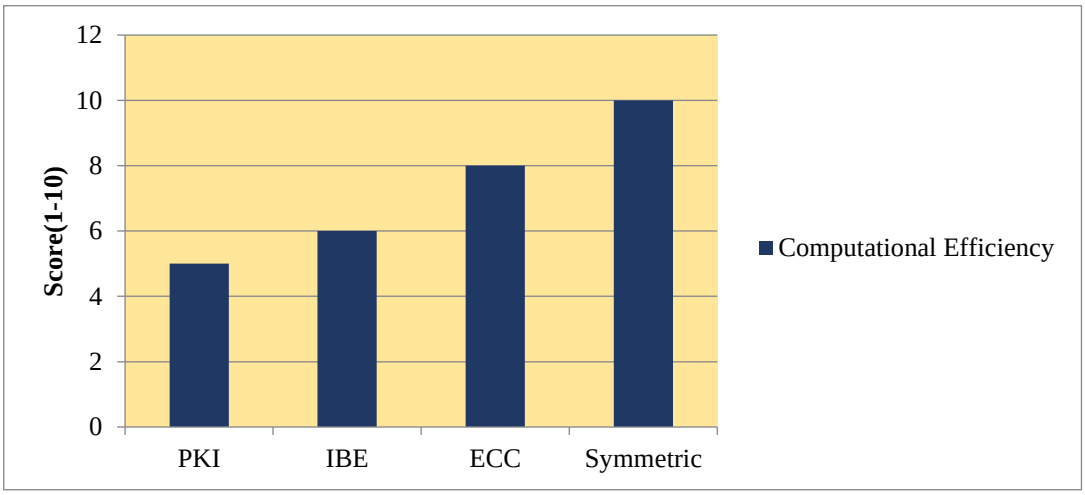

Figure 6: Computational Efficiency on Resource-constrained Devices

This graph (Figure 3) assesses the strength of each key management protocol (KMP) concerning common threats like eavesdropping, spoofing, and man-in-the-middle attacks. The scores of PKI and ECC indicate that their use of cryptographic primitives and authentication methods was thorough and sophisticated; hence they received the highest marks (9/10). IBE also shows strong security posture at (8/10), although the centralized key generation exposes some possible weaknesses. While symmetric key schemes can be efficient, they scored lower (6/10) due to being more prone to key compromise and lacking scalable methods of authentication. Scalability graph (Figure 4) describes the growing responsiveness of a protocol in accommodating an increasing number of IoT nodes, vessels, and communication endpoints. ECC (9/10) leads in this area because its light cryptographic functions and low overhead make it appropriate for large and dynamic maritime networks. IBE (8/10) also scales well as it eliminates certificate management which enhances efficiency. In contrast, PKI (6/10) has difficulties with certificate life cycle renewals and revocation. Symmetric key schemes (5/10) face significant challenges in key distribution as network size increases. The graph (Figure 5) illustrates the additional external communication needed for accurate implementation of a given protocol, including key exchange and handling. Symmetric schemes incur the lowest cost of data exchange (three points). After these come IBE and ECC, scoring five and six respectively, which incur moderate overhead due to inconsequential authentication requirements. Next is PKI at seven, which adds substantial amount of overhead due to certificate validation and transmission, which poses major issues in bandwidth constrained maritime settings. For preserving dependable data transfer via satellite and long range radio communication, it is critical to reduce the communicated data per transaction. This graph (Figure 6) evaluates the performance of each protocol on Maritime IoT hardware with limited CPU and Memory resources. Symmetric key protocols (10/10) are optimal since they require very little processing, making them ideal for devices with stringent resource limitations. ECC (8/10) is also relatively good because of the smaller keys and faster computations in comparison to RSA. IBE (6/10) performs moderately well but struggles with the inefficiency that arises from bilinear pairings' complexity. PKI (5/10) is the least efficient because it consumes too much cost in certificate management, making it inapplicable to small sensors and embedded systems.

The outcome of the evaluation confirms the absence of a single key management protocol that would entirely meet the requirements of the maritime IoT environments. The findings, though perhaps surprising to some, indicate that the most viable options stem from solutions based on ECC protocols and IBE schemes. This is attributed to the balance in security, efficiency, and flexibility offered by the

two. With IBE's lack of certificates, membership dependency relayed with decentralized remote networks complement each other while simultaneously, ECC's cryptographic strength with low resource consumption aligns with embedded devices such as maritime. Such research suggests that a hybrid key management technique could provide the greatest benefit in securing communication from the ship to the shore. For example, ECC would be useful for securing session establishment and authenticating devices, whereas symmetric keys would ease the computational burden of encrypting large volumes of data. In the same way, IBE could function as a low-weight option for certain applications where trust is able to be centralized and securely controlled within the confines of sensitive latency and bandwidth restrictions. Moreover, the study focuses on having an outline for an intelligent selection of the protocol that is most relevant for the use case in maritime IoT deployments. Vessel classification, communication intervals, hardware's operational capabilities, and the environment within which the system operates should dictate the selection and design of the key management system. The study also points out the lack of existing work on lightweight, distributed, and self-repairing key management systems equipped with the ability to respond to the flexible demands of maritime operations while maintaining security.

5 Recommendations

The identification of the maritime specialized features such as operations constraints, structural communication systems, and security requirements specifically for the use of maritime technology considers the key management protocol (KMP) of Maritime IoT systems. This system must not rely on a general approach, rather, should use a context specific explanation which takes different layers into account. For instance, in the case of vessels, it is suggested that shipboard sensors and actuators with low power capabilities use Elliptic Curve Cryptography (ECC), as it is efficient and offers high security. As for autonomous underwater vehicles and offshore platform's temporary structures, unlike the value traditional certificate management serves, Identity Based Encryption (IBE) performs well for use in dynamically configured networks. Within a tightly controlled and pre-registered vessel system, symmetric key management is more usable. While the Public Key Infrastructure (PKI) system makes sense for trust establishment initially between command centers onshore and the ship, given its constituents and requirements, It should be used with light or blockchain aided structures to reduce complexity. The conclusion drawn from this reasoning is that using multiple security strategies based on the specific need for a certain network or critical data needs is best, as it merges high security with scalability and enhanced performance.

Enhancement of security for ship-to-shore communication in Maritime IoT systems needs both a technological and operational approach. The automation of the key lifecycle management for landbased communication systems could safeguard security on its own by periodically updating keys, revoking access or distributing them where necessary based on device behavior or risk events that may occur. Communication with shore offices should be done with TLS1.3 and DTLS for both low and high latency marine communication environments to minimize tampering or interception. HSM or TPM device integration can protect cryptographic keys on maritime devices from physical and unauthorized access allowing these pieces of equipment to be secured as well. A more comprehensive framework would also be able to account mod AI with behavioral anomaly detection systems allowing for identification of outlier communication activities that may be cyber intrusions. For policy measures, more international cooperation on global information system policies is needed. Development of uniform and cross-border guidelines will enable vessels of any nationality to access shore based infrastructure while enabling free flow of information to ensure secure communication. To mitigate human error, technical restrictions

should not be the only focus. Security awareness and training programs should be the first steps to address these issues.

There are various potent IoT environments such as those concerning maritime security alongside its key management which are yet to be practiced. One of those include the implementation of Post Quantum Cryptography (PQC) algorithms integration which defends against quantum computer attacks on existing public key frameworks. Considerable work is yet to be done wirelessly through maritime specific PQC scheme analysis that considers factors such as low connectivity and low computation capabilities. Another area that is still emerging is the enabling of decentralized, unforgeable, and trust management systems utilizing blockchain technology for more complex and forged proof trust management solutions wherein blockchain technology can get rid of single points of weakness while also enabling certificate revocation and control over access in a distributed manner. Moreover, adaptive key management systems powered with AI present remarkable possibilities in terms of pro active threat surveillance and self-security measures in case a threat is detected in high mobility environments. Ultra light-weight cryptographic systems designed for buoys and underwater sensors devices placed in oceans would need more research in terms of supporting energy constraint measures. Lastly, simulated and tested deployment of maritime based cryptographic systems could benefit from the use of digital twins. In addition to these technological advancements, further research needs to be undertaken in regard to policies that would govern the ethical, lawful, and regulated movement of such systems in ungoverned waters.

6 Conclusion

Based on this marine IoT research, secure ship-to-shore communication key management protocols gave the most attention. Based on our data analysis, no one key management solution is optimal for everyone is feasible. Public Key Infrastructure (PKI) has proven helpful for trust establishment but is still slow in decentralized and bandwidth limited maritime environments. Elliptic Curve Cryptography (ECC) is a computationally effective and secure solution that is feasible for use in devices onboard ships. IBE also does not require certificates for dynamic and ad-hoc maritime networks. That holds promise but poses several trust delegation issues. Meanwhile, symmetric key protocols are light for closed systems. Depending on the system, they may lack scalability or become key distribution constrained. Based on the evidence collected, it becomes apparent that the most optimized and secure option is the creation of hybrid implementations that meld multiple lines of policies modified to specific device power capabilities, network contexts, and sensibility of the data. The protection of communications from the ship to shore is important for the functioning of maritime IoT systems. The protection of data pertaining to ship navigation, cargo, real-time telemetry, environmental sensing, and other IoT is crucial in terms of its integrity and confidentiality. The maritime domain uniquely poses challenges that require sophisticated, reliable, and flexible security measures that endure. The existence of unprotected communication paths leads to potential threats such as data leakage, cyber warfare, and other operational issues that are highly unfavorable for maritime infrastructure. This research demonstrates the merits and demerits of various KMPs which helps maritime engineers, cyber-security know who's, and policymakers in understanding different perspectives. By advocating for tunable, anticipatory approaches such as post-quantum cryptography and blockchain-based trust management, this research attempts to increase defense resiliency for maritime IoT systems. Thus, strategically and technically, trust key management mountaineers positions itself at the heart of enabling safe, smart, and IoT integrated next generation maritime operations.

References

[1] Ahmad, Z., Acarer, T., & Kim, W. (2023). Optimization of maritime communication workflow execution with a task-oriented scheduling framework in cloud computing. *Journal of Marine Science and Engineering, 11*(11), 2133. https://doi.org/10.3390/jmse11112133

[2] Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network, 2*(1), 123-138. https://doi.org/10.3390/network2010009

[3] Alagdeve, V. D., Singh, R., Parihar, B., Dhananjeyan, S., & Ashreetha, B. (2023, October). Efficient data encryption and signature generation scheme for resource-constrained IoT environments. In *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 262-269). IEEE. https://doi.org/10.1109/I-SMAC58438.2023.10290224.

[4] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

[5] Alqurashi, F. S., Trichili, A., Saeed, N., Ooi, B. S., & Alouini, M. S. (2022). Maritime communications: A survey on enabling technologies, opportunities, and challenges. *IEEE Internet of Things Journal, 10*(4), 3525-3547. https://doi.org/10.1109/JIOT.2022.3219674

[6] Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An efficient privacy-aware authentication framework for mobile cloud computing. *International Academic Journal of Innovative Research, 10*(1), 1-7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[7] Ayesh, A. N. (2024). Enhancing Urban Living in Smart Cities Using the Internet of Things (IOT). *International Academic Journal of Science and Engineering, 11*(1), 237-246. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1127

[8] BenSaleh, M. S., Saida, R., Kacem, Y. H., & Abid, M. (2020). Wireless sensor network design methodologies: A survey. *Journal of Sensors, 2020*(1), 9592836. https://doi.org/10.1155/2020/9592836

[9] El Bekkali, A., Essaaidi, M., & Boulmalf, M. (2023). A blockchain-based architecture and framework for cybersecure smart cities. *IEEE Access, 11*, 76359-76370. https://doi.org/10.1109/ACCESS.2023.3296482

[10] Farzadmehr, M. (2025). *AI-powered solutions assessment in port and maritime sector* (Doctoral dissertation, University of Antwerp). https://doi.org/10.63028/10067/211729015116216514 1

[11] Gyamfi, E., Ansere, J. A., Kamal, M., Tariq, M., & Jurcut, A. (2022). An adaptive network security system for iot-enabled maritime transportation. *IEEE transactions on intelligent transportation systems, 24*(2), 2538-2547.

[12] Haidine, A., Ait-Allal, A., Aqqal, A., & Dahbi, A. (2021). Networking layer for the evolution of maritime ports into a smart environment. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 46*, 251-257. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-251-2021

[13] Kavallieratos, G., & Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering, 8*(10), 768. https://doi.org/10.3390/jmse8100768

[14] Kavitha, B. C., Vallikannu, R., & Sankaran, K. S. (2020). Delay-aware concurrent data management method for IoT collaborative mobile edge computing environment. *Microprocessors and Microsystems, 74*, 103021. https://doi.org/10.1016/j.micpro.2020.103021

[15] Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal, 8*(6), 4132-4156. https://doi.org/10.1109/JIOT.2020.3026493

[16] La Manna, M. (2022). Applying Attribute-Based Encryption in IoT and Automotive Scenarios.

[17] Latif, M. A., Ahmad, M. B., & Khan, M. K. (2020, October). A review on key management and lightweight cryptography for IoT. In *2020 Global conference on wireless and optical technologies* (GCWOT) (pp. 1-7). IEEE. https://doi.org/10.1109/GCWOT49901.2020.9391613

[18] Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)* (pp. 91-98). IEEE. https://doi.org/10.1109/EISIC.2017.20

[19] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.

[20] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy*, *16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

[21] Odeh, A., & Taleb, A. A. (2023). A Multi-Faceted Encryption Strategy for Securing Patient Information in Medical Imaging. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(4), 164-176. https://doi.org/10.58346/JOWUA.2023.I4.012

[22] Perera, K., & Wickramasinghe, S. (2024). Design Optimization of Electromagnetic Emission Systems: A TRIZ-based Approach to Enhance Efficiency and Scalability. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(1), 31-35.

[23] Petrova, E., & Kowalski, D. (2025). Energy-Efficient Microalgae Filtering and Harvesting Using an Extremely Low-Pressure Membrane Filter with Fouling Control. *Engineering Perspectives in Filtration and Separation*, *2*(1), 25-31.

[24] Radhi, A. A. A. H. (2022). Marketing Communications and their Impact on Managing Crises in Tourist Destinations. *International Academic Journal of Social Sciences*, *9*(1), 9-20. https://doi.org/10.9756/IAJSS/V9I1/IAJSS0902

[25] Rahimi, P., Khan, N. D., Chrysostomou, C., Vassiliou, V., & Nazir, B. (2020, May). A secure communication for maritime IoT applications using blockchain technology. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 244-251). IEEE. https://doi.org/10.1109/DCOSS49796.2020.00047

[26] Rajeev, S. (2023). An Analysis of NEP 2020: Certain Key Issues. *Indian Journal of Information Sources and Services*, *13*(1), 10-16. https://doi.org/10.51983/ijiss-2023.13.1.3443

[27] Regan, R., Rangasamy, R., Krishna, B. V., & Manikandan, J. (2025). A Hybrid Group Key Management System for Secure IoT Networks Using IT2FONC-HKM Approach. *International Journal of Communication Systems*, *38*(15), e70231. https://doi.org/10.1002/dac.70231

[28] Seyedan, A., Soroushpour, S., & Gholamrezazadeh, S. (2023). Family and its changes in Cyberspace and the explanation of its future perspectives in the communication era. *International Academic Journal of Organizational Behavior and Human Resource Management*, *2*(2), 01–06.

[29] Shimazu, S. (2024). Intelligent, sustainable supply chain management: A configurational strategy to improve ecological sustainability through digitization. *Global Perspectives in Management*, *2*(3), 44-53.

[30] Suresh, G., & Lenine, D. (2024). Gaps of Indian Electrical Energy Sector and its Optimal Mitigation by Using Optimal Utilization of Indian Renewable Energy Policy with the Help of the P&O Mppt Technique. *Archives for Technical Sciences*, *31*(2), 94-115. https://doi.org/10.70102/afts.2024.1631.094

[31] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

[32] Thanh, N. T. P., Hien, D. T. N., Dung, P. A., & Hai, N. X. (2024). Mobile and Phone Speaker Recognition with IoTs and IAI Robot Control System Applications for Production. *International Journal of Advances in Engineering and Emerging Technology*, *15*(1), 19-23.

[33] Ye, J., Cao, X., & Guo, Z. (2023). Secure marine environment communication: A multiobject authentication protocol based on secret sharing. *International Journal of Intelligent Systems, 2023*(1), 1814053. https://doi.org/10.1155/2023/1814053

[34] Zhang, M., Zhu, B., Li, Y., & Wang, Y. (2022). TPM-based conditional privacy-preserving authentication protocol in VANETs. *Symmetry, 14*(6), 1123. https://doi.org/10.3390/sym14061123

Authors Biography

P. Rajan is an Teaching assistant in the Department of Marine Engineering, bringing a remarkable blend of academic and industry expertise to the classroom. With over 31 years of sailing experience, with 2 years' workshop experience including 15 years as a 3rd Engineer, and nearly 14 years of teaching experience, he offers deep insights into marine operations and engineering. He holds a B.E. in Mechanical Engineering and a MOT Class 4 old Certificate, specializing in Marine Engineering. His teaching portfolio includes key subjects such as Marine Internal Combustion Engines and Marine Auxiliary Machinery and marine workshop including ship in campus. A member of the Institute of Marine Engineers (India).

K.R. Chidhambaram, Director – Marine Engineering, holds a B.E. in Mechanical Engineering and a First Class Motor Certificate (MEO Class I). With an extensive sailing career spanning 31 years and 19 years of teaching experience in maritime education, he brings a wealth of practical and academic expertise. His areas of specialization include Afloat Training, Ship Construction and Stability, and Marine Engineering Practice. He has filed two patents in the field of marine engineering and has published several research papers, including "Critical Analysis and Preventive Measures in Grounding of Ship" in the International Journal of Applied Engineering Research (IJAER), and "Cargo Delay and Consequences" and "Coastal Accidents – Need Prevention" in the Institute of Marine Engineers India (IMEI) journal.

Dr. Deepa Rajesh stands as a beacon of excellence in academia, administration, research, and philanthropy. With an impressive portfolio of qualifications, including M.Com, MBA, M.Phil, and Ph.D., she epitomizes intellectual prowess and leadership. Her unparalleled contributions continue to inspire and redefine maritime education on a global scale, reflecting her relentless pursuit of excellence and commitment to shaping future generations. A prolific researcher and thought leader, Dr. Deepa Rajesh has an illustrious record of publications in prestigious Scopus, UGC-CARE, and high-impact factor journals. Her thought-provoking research papers have graced numerous national and international conferences, further solidifying her standing in the academic community. Her two published books stand as a testament to her dedication to knowledge dissemination. Moreover, her successful completion of funded research projects underscores her ability to secure grants and contribute significantly to scholarly advancements. Serving as an editorial board member for reputed journals, she continues to shape the academic discourse with her insightful perspectives.