

Developing Identity Management and Authentication Methods for Cruise Ship Passenger Services

Krishnamurthy Kumar^{1*}, K. Karthik², and Dr. Deepa Rajesh³

^{1*}Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India.
captrkkumar@ametuniv.ac.in, <https://orcid.org/0009-0005-2439-0976>

²Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India. principal@amet-ist.in, <https://orcid.org/0009-0008-2399-6249>

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

Received: April 11, 2025; Revised: May 26, 2025; Accepted: July 16, 2025; Published: August 30, 2025

Abstract

As a key component of sea transportation, the cruise ship industry has particular requirements for identity management and authentication systems which balance the need for security, operational efficiency, and a customized experience for each traveler. Traditional methods of identification are proving inadequate with rising passenger numbers, complexities associated with international travel, an increase in the scrutiny afforded to maritime security, and issues of privacy data concerns. The scope of this research focuses on creating sophisticated systems of identity management and authentication tailored to cruise ship passengers. With a focus on maritime applications, this study analyzes the biometric measurements, smart RFID cards, and mobile phone-based authentication systems employed at the port terminals, gangways, onboard access, and excursion control for various maritime peering interfaces. This paper combines existing literature, analyses other modes of transport, and studies selected cases from the maritime industry to determine the best integrated design solutions for the cruise environment which incorporate the identified gaps. The goals of the findings are to improve operational efficiency, enhance compliance with security regulations under the ISPS Code, and increase the safety and satisfaction levels of passengers traveling by sea.

Keywords: Identity Management, Authentication, Cruise Ships, Passenger Services, Maritime Applications, Biometric Verification, Security Systems.

1 Introduction

1.1 Importance of Identity Management and Authentication in the Context of the Cruise Ship Industry

The cruise ship industry is one of the most important segments of tourism and it accommodates millions of travelers every year. With the growth in the number of guests and the level of service provided, managing the identity of such passengers has increasingly become an important issue. Identity management and authentication systems are required primarily to strike a balance between security and convenience. Managing identity for services such as boarding and access to cabins, onboard purchases,

and even shore excursions, require restructuring modern identity management approaches (Chang et al., 2017). The introduction of new technologies and their adoption extends to identity verification systems used by the cruise industry. Biometric identification systems, RFID (Radio Frequency Identification) as well as mobile-based identification have significantly improved security and operational capabilities of cruise lines (IDEMIA, 2021). For example, facial recognition systems are now deployed for embarkation for ease of boarding and to limit contact at various checkpoints, improving passenger experience by reducing waiting times (Kuhn et al., 2023). In addition, mobile-based authentication alongside application-based approaches also support passengers in real-time cruise management increasing the scope of security (Wu et al., 2020). These identity management systems have become essential for the operational continuity of cruise lines while enhancing overall operational efficiencies and passenger satisfaction.

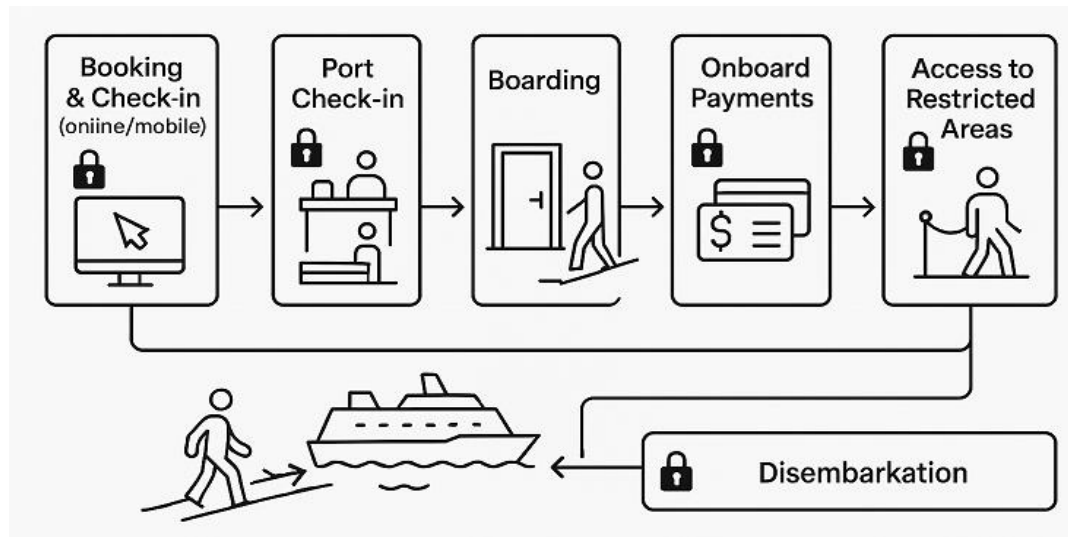


Figure 1: Identity Verification Journey in Cruise Operations

The picture (Figure 1) shows the complete identity management lifecycle involved in a cruise experience including all crucial points of secure identification. This starts with identification verification during port check-in, alongside mobile or online booking and checkout. Following these is identity authentication during boarding where passengers have to be validated pre-ship access. Secure identification permits payment transactions and entry into confidential areas while onboard. The last stage of the voyage is identity authentication which occurs during disembarkation. All these steps in the diagram are marked with a lock symbol, representing the need to protect personal information and mitigate unauthorized access or use throughout the span of the cruise. This demonstrates the sharp focus of a single cruise's identity management system.

1.2 Overview of the Problems and Scope of the Gaps in the Existing Systems

Modern approaches towards identity verification have been adapted to the cruise industry, but some challenges still persist. A primary hurdle is the fusion of technological advancements with older legacy systems. A large number of cruise ships operate utilizing manual processes and databases, which are periferal and not fully operational with contemporary identity management systems (Vethachalam, 2021). This incompatibility results in operational inefficiencies and undermines the full advantages of new innovations like effortless biometric verification and comprehensive RFID systems. Besides the problem of system integration, the cruise industry is also concerned with data privacy and security issues.

Cruise lines keep and collect a plethora of sensitive and personal data of their passengers which include passport numbers, credit card information, and travel itineraries. Safeguarding this information from cyber threats is extremely crucial, especially considering the fact that cruise ships are increasingly becoming targets of cybercriminals (Samsung Insights, 2018). The maritime industry is particularly susceptible to a cyber attack because of their dependence on the sophisticated web of interlinked networks that exist throughout the globe's shipping lanes (Vethachalam, 2021). Thus, a continual challenge, alongside enforcing adequate cybersecurity measures, is managing compliance with international legislation such as the General Data Protection Regulation (GDPR) (Kuhn et al, 2023; Abdullah, 2024). Separately, there are challenges in the adoption of new identification and authentication systems. Some passengers remain privacy-conscious and do not recognize how the technology operates, making them reluctant to adopt biometric systems such as facial recognition. Passengers need to feel safe and confident while using these systems in order for them to be implemented effectively and successfully (Nakamura & Lindholm, 2025). In addition, cruise lines have to make sure that there are user friendly designs and help systems for passengers who are not accustomed to mobile applications or biometric authentication interfaces (Wu et al, 2020; Samyadevi et al., 2024). The cruise industry has greatly benefited from the advancement of facial recognition technology which further enhances the cruising experience. The facial recognition systems enable passengers to board the ship seamlessly and without contact since there is no requirement for them to show identification or boarding passes (Gupta et al, 2023). Moreover, (Zhou et al, 2022) asserts that cruise ships are better protected with RFID access control systems because they prevent the access of intruders to certain sensitive areas. In addition, the use of RFID technology allows for a smoother and quicker interaction of the passengers with the cruise services making it easier for them while reducing human error. Increased use of digitized sensitive data exposes it to cyber threats which endanger personal information, financial information, and even travel plans (Monette, 2021). With regards to the null identity crisis which will be experienced in coming years, (Rawal et al, 2023) argues that the combination of mobile devices and biometric features as well as RFID will heighten the effectiveness of passenger identity control systems. RFID cruise systems must observe legal privacy protections including GDPR policies (Merriam, & Baumgartner, 2020) emphasizes that cruise lines have an obligation to safeguard the privacy rights of passengers using these systems. Following (Zhang et al., 2020), banking, and other such industries, along with healthcare, offer illustrative case studies which would assist the cruise industry in understanding the challenges that come with deploying these technologies at a higher level.

1.3 Statement of the Purpose and Objectives of the Research Paper

This paper seeks to investigate and critique the modern practices of identity management and authentication utilized in the cruise ship business, paying special attention to the challenges and gaps these systems encounter. Examine the identity management systems that are used in the cruise industry. Determine what the most important issues and shortcomings of these systems are, especially in terms of integration, data protection, and user acceptance. Investigate new and emerging technologies and methods that could improve identity verification, including biometrics, RFID, mobile, and other related technologies. Formulate strategies and recommend alternative methods to improve identity management frameworks and offer practical solutions relevant to the maritime industry. In completing these objectives, the paper intends to augment the existing literature on security and identity management systems concerning the cruise ship industry and offer meaningful contributions to cruise operators, technology stakeholders, and policymakers. Also, the research seeks to enhance the understanding of the benefits and drawbacks of new identity verification systems in the maritime sector.

2 Literature Review

2.1 Literature Review on Identity Management and Authentication Methods in Transport Sector

Identity management and authentication methods in transport industry sectors like aviation, railways, and maritime travel incorporate security features that help streamline operations, so the need to verify the identity of a passenger is of great importance (Marinković et al., 2024). Every traditional process from issuing a ticket to boarding a train or flight has traditionally been accompanied with the presentation of various forms of ID together with a physical self-security check (Kavitha, 2024). With the explosion of modern biometric systems and digital authentication technologies, these processes have always strived to improve convenience (Aloysius & Alhaji, 2020). In aviation, the adoption of biometric methods has facilitated faster check-in and boarding. Today, facial recognition and fingerprint scanning are the norm for verifying passengers and boarding them in record time (Zhao et al., 2021). In fingerprint and facial recognition technologies, the maritime sector also seeks to use them for the embarkation of the passenger for the prevention of fraud and increased operational effectiveness (Bennett et al., 2019). Other transportation sectors require convenience for users but at the same time a high level of security and these requirements pose a problem for cruise ships where user experience is important (Pérez & García, 2020).

2.2 Analysis of Technologies and Trends Related to Identity Verification for Passenger Services

The latest innovations in identity verification technology has transformed passenger services in the transport sector. One of the major shifts is the deployment of biometrics because of its ability to permit remote real-time authentication. Various modes of transport have incorporated biometric systems like facial recognition, iris scanning, and fingerprint scanning. For example, the International Air Transport Association (IATA) has been working toward an industry-wide biometric entry and exit system for passengers known as “one ID,” where passengers will no longer need to present a passport and boarding pass (Sengupta, 2020). Facial recognition is also being adopted by cruise lines to expedite and streamline the embarkation process (Akshara et al., 2021). One more notable development in technology is the implementation of RFID (Radio Frequency Identification) technology. Nowadays, smart cards enabled with RFID technology are frequently used for ticketing, controlling access, and tracking luggage. RFID systems assist in providing a safe and smooth travel experience by automating a passenger’s identity verification at multiple checkpoints (Morgan & Ritchie, 2019). In addition, mobile identity management systems that utilize smartphones for boarding passes, access to rooms, and in-app purchases are increasing in the cruise and aviation industries (Saeed & Qamar, 2021). Identity management in transportation is also adopting new forms with emerging technologies like blockchain (Wu & Margarita, 2024). Its decentralized and secure characteristics may alleviate some of the privacy issues while being able to provide an unchangeable history of identity verification (Zhang et al., 2020). There is potential for blockchain technology to provide more efficient ways to securely manage passengers’ identity information as the technology matures, especially on cruise ships that have passengers from different countries (Krishnan et al., 2022; Muralidharan, 2023).

2.3 Examination of Case Studies and Examples from Other Industries with Successful Implementation of Identity Management Systems

There are several industries beyond transportation that have successfully adopted sophisticated identity management systems and can be useful for the maritime industry. For instance, the banking and financial

industries have aggressively employed biometric identification systems to enhance system security and ease customer access to services.

Table 1: Comparison of Identity Management Methods Across Industries

Industry	Method Used	User Convenience	Speed	Adoption Rate	Security Level
Aviation	Facial Recognition, Biometric e-Passports, Mobile Boarding Pass (QR Code)	High – Touchless, minimal interaction	Very High – Seconds per person	High – Widely implemented at major airports (e.g., US, EU, Asia)	High – Encrypted biometrics, multi-factor
Hotel	Mobile Check-in via App, Keycard with RFID/NFC, Biometric Kiosks	High – Self-service available	High – 1–3 minutes check-in	Moderate to High – Especially in major chains	Moderate to High – Dependent on vendor security practices
Rail	QR Code Tickets, Contactless Smart Cards, e-ID Integration (in some countries)	Moderate – Requires app or printed ticket	Moderate – Queues vary	Moderate – Widespread in urban transit; lower in intercity	Moderate – Relies on device/app authentication
Cruise	RFID Wristbands/Cards, Facial Recognition at Terminals (emerging), Manual ID Checks	Moderate – RFID useful onboard, but port processes less streamlined	Low to Moderate – Embarkation can be time-consuming	Low to Moderate – Adoption growing, but inconsistent	Moderate – Less mature integration of biometric systems

This table (Table 1) compares biometric and identity management technologies of airlines, hotels, rail transport and cruise line services using different key benchmarks. Airlines have outdone all other sectors in biometric adoption owing to aviation's high convenience and security requirements. Hotels provide effective mobile and RFID check-in services. Rail systems do make use of QR code and smart card technology but with average service speed and security. The cruise sector is still behind other sectors regarding RFID and facial recognition deployment, consistency, speed and full biometric integration. Facial recognition and voice biometric authentication have securely enabled Citibank and JP Morgan to fortify the control of transactions and account management (Zhou et al., 2022). Such innovations could also be transplanted into cruise ships for secure biometric transaction and service interactions (Prakash & Prakash, 2023). The healthcare sector has also utilized identity management systems to safeguard sensitive patient data while improving access to services (Rahim, 2024). Hospitals and healthcare providers are employing biometric systems for patient's identification which mitigates the errors and fraud risks associated with medical record management (Chen et al., 2021). This could likewise be utilized in the cruise sector for the protection of passenger data to reduce the likelihood of misidentifying the passengers when boarding or for a medical emergency (Papadopoulos & Christodoulou, 2024). A particularly important illustrative example is the use of RFID technology in logistics and supply chain management. Amazon and Walmart, for example, have integrated RFID systems for real-time tracking of goods which has dramatically mitigated losses and operational inefficiencies (Patel & Thakkar, 2020). The adoption of comparable systems on cruise ships could help alleviate problems related to passengers' and their luggage tracking at different phases of the cruise which could help in improving accuracy and boosting security.

In addition, airports have successfully implemented "self-service" systems that allow passengers to check in and security check through biometric and RFID technology. The automation and convenience

of such systems has led to increased ease of operations and better service, enhancing the experience for the passengers (Lai et al., 2020). This is likely to be replicated in the maritime industry where some cruise lines are investigating the use of self-service systems for efficient embarkation and disembarkation (Huang & Zhang, 2020; Donkor & Zhao, 2024).

3 Methodology

3.1 Explanation of the Research Strategy and Method Employed for This Study

This particular study utilizes a mixed-methods approach. This involves acquisition of both qualitative and quantitative data so as to provide an in-depth examination of the identity management and authentication systems in the cruise industry. It is best to utilize a mixed-methods approach because it provides an adequate understanding of the identity management systems at the technical level, as well as the operational and human dynamics that affect their functioning. The major focus of the research is to assess what technologies exist, what challenges come with their implementation, and what advantages accrue from these systems to the passengers and the cruise operators. A descriptive research design will be used in this study to obtain the detailed information which assists in understanding the practices of identity management. The goal is to identify and describe the various kinds of identity verification methods employed in the cruise industry. Since data is collected from multiple sources to represent the current trends and practices, this approach is termed as cross-sectional. Qualitative information along with quantitative insights enables the study to portray how identity management technologies are influencing passenger services, operational efficiency, and security on cruise ships, thereby reinforcing the concept of a 'smart' vessel.

3.2 Explanation of the Methods and Sources of Data Collection Applied in the Research

Identity and access control management in cruise ships is a very dynamic area. For this reason, data collection for this study is carried out employing numerous approaches to obtain an accurate understanding of identity management and authentication processes. The primary data collection methods include surveys, interviews, case studies, observational research, and secondary data from published reports and research papers. Each of these methods contributes towards the overall findings in a different way. Surveys are one of the most common methods of collecting quantitative data from two main groups: passengers and operators of cruise lines. In addition to capturing passengers' experiences with biometric and RFID boarding, the survey incorporates questions on security, privacy, satisfaction, and system usability. Similarly, cruise line operators are surveyed to understand the challenges of incorporating such technologies, how the technologies affect operational efficiency, and what security benefits, if any, are perceived. The surveys provide tangible quantitative data that can be used to analyze trends and correlations between passenger satisfaction and the technologies employed.

For the purpose of collecting qualitative data on the implementation and operation of identity management systems, in-depth interviews with cruise line managers, technology providers, and security officers are conducted. These semi-structured interviews aim to capture the experiential and subjective professional testimonies on the efficacy of these systems. The interviews serve granular details, which are otherwise difficult to obtain through surveys, such as facing new technological implementation challenges, privacy issues, and data security concerns. Furthermore, case study analysis is conducted on the cruise industry, as well as other modes of transport and hospitality, to determine how identity management technologies have been effectively applied within these sectors. These case studies provide

valuable lessons and can demonstrate the real-life applications, both the merits and challenges, of employing identity management systems.

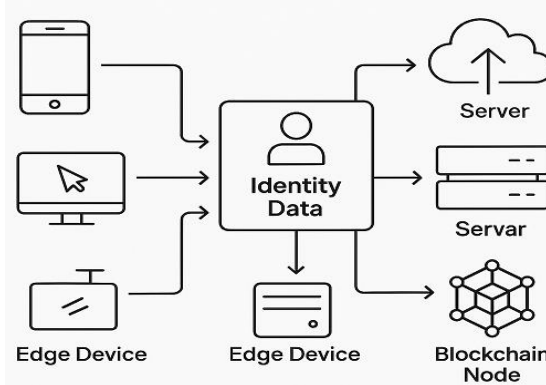


Figure 2: Decentralized Identity Data Flow for Secure Cruise Operations

This diagram (Figure 2) describes a decentralized architecture for identity data management in a cruise context. Identity data is retrieved and composed from a range of devices—smartphones, desktops and edge devices—utilized by passengers or operated by systems under cruise control. This information is processed and sent to various backend subsystems such as cloud servers, local servers, and blockchain nodes, which form the different system’s backends. Edge devices are responsible for real-time processing and decision-making, whereas servers are in charge of application and data storage functions. Identity verification is performed on identity data maintained using blockchain nodes incorporated within the system because such nodes allow durable and transparent identity data, thus increasing their security and trust in the system’s distributed environment. The use of diverse technologies results in enhanced identity management, making the system more scalable, resistant to modification, and protective of personal data at the same time.

Observational research focuses on identity verification systems and their application at cruise terminals and onboard ships. This approach provides contextually rich information regarding passenger-system interactions and how effectively these systems perform in practice. Observation includes boarding times, the actual count of attendees scanned at the biometric systems, and the overall experience, including the role of technology within the travel cycle, with the aim of uncovering operational efficiency and the experience of the users. Finally, the compilation of secondary data consists of industry reports, academic publications, and white papers discussing identity management and authentication within the transportation industry. This secondary data assists in explaining the context surrounding the primary data while also drawing insights from other industries, thus enhancing the understanding of the cruise industry’s use of identity verification.

3.3 Discussion of the Evaluation Techniques Related to the Utilization of Identity Management and Authentication Systems

In the preceding chapters, we discussed how each data collection technique contributes to the evaluation of identity management and authentication systems. Different analysis techniques have been integrated into the study to provide a complete evaluation of the effect of identity management and authentication systems on security, operational efficiency, and the satisfaction of passengers within cruise ship services. With the qualitative approach, data extracted from specific passenger interviews are analyzed, interpreted, and reported in relation to concepts put forth with the underlying theories of satisfaction. Once the data has been gathered, it is described and interpreted in a broad light and focuses on factors

such as the level of perceived security, courtesy of cruise staff, along with the classification of operational efficiency and satisfaction scope of activities to be included in the definition of satisfaction. Furthermore, the operational advantages of identity management technologies are evaluated by computing the efficiency metrics. For instance, a measurement is taken regarding the reduction of boarding times associated with the use of biometrics or RFID systems and this is compared to the traditional methods of check in. Such comparisons quantify the benefits in smooth sailing, due to system induced delays, service efficiency improvement during the entire journey, and overall cruise experience enhancements. Data regarding the identity theft, fraud, or unauthorized access of the biometric systems are compared to measure the effectiveness of the authentication systems in question as well. Security measurements capture shifts in attempts for unauthorized access or breaches which provide insights into the enhanced passenger safety these technologies provide as well as the costs in terms of security risks ensuing. For qualitative assessment, documents and transcripts from interviews, open-ended survey responses, and case studies are analyzed using thematic analysis. This method enables the detection of the mentioned systems, their benefits, and the challenges posed by them to formulate repeatable ways to use these systems for better identity management. For example, user experience, security risk perceptions, and operational challenges may be themes that provide deeper lessons on the technologies from the point of view of passengers and cruise line operators.

A SWOT analysis aids in evaluating the cruise line industry's identity management systems. The analysis attempts to improve upon existing technologies by examining their strengths and weaknesses. Furthermore, opportunities for improvements, such as the implementation of new biometric modalities and encryption methods, are explored as well as potential threats like data privacy concerns and technological failures are highlighted. As a final point, a comparative analysis is done to measure the efficacy, security, and satisfaction levels passengers receive from various identity management systems like biometrics, RFID, and mobile based systems. Through the analysis, the shortcomings of the systems from different cruise lines and through different scenarios are analyzed to provide the conditions in which these systems can operate most effectively. Employing all these techniques allows for a thorough assessment of identity management and authentication techniques within the cruise industry that enables the research to formulate practical strategies and guidelines for enhancing security, efficiency, and the overall experience passengers receive during cruise ship operations.

4 Findings

While modernization is being attempted, the identification management processes in the cruise ship (Genç, 2016) industry still face challenges due to the prevalence of outdated techniques. Today's cruise lines have adopted biometric systems for passenger identification, including facial recognition systems and fingerprint scanners. The use of these systems has demonstrated improvement in the reduction of boarding processes as well as enhanced security through the proper identification of passengers and their respective bookings, subsequently eliminating the use of boarding passes. There is also broad application of RFID based technologies, particularly in the identification of cruise ship passengers. RFID wristbands and cards are utilized for accessing cabins, making onboard purchases, and tracking movement for security purposes. Regardless, challenges still exist in the current environment. Most cruise lines continue to use passport and manual boarding pass identity checks, which slow down the cruise check-in and boarding processes. Moreover, despite the advantages, biometric systems pose challenges concerning privacy and data protection. With the growing use of these technologies, they face real-world hurdles like the precision of facial recognition, system failures, machine-captured imagery, and interfacing with older equipment. Additionally, the absence of a standardized cruise travel document

introduces substantial differences across cruise lines regarding technology adoption and implementation, resulting in disparate operational efficiency.

Opportunities of cruise industry biometrics and personal identification systems within the realm of identity are largely a result of increasing security and operational efficiency. Biometric technologies, especially facial recognition, allow for touchless boarding, expediting the process which is a significant convenience for passengers. This leads to a reduction in wait times at embarkation and an overall improvement in satisfied passengers. Moreover, biometric systems employ modern technology that is more difficult to forge or replicate, thereby increasing the security of identity verification and reducing the risk of identity theft. RFID technology offers several benefits as well, particularly when it comes to convenience and user-friendliness. Passangers enjoy the convenience of containing their room keys, payment methods, and identification within their RFID wristband throughout the cruise. Such a system simplifies the interaction of passengers with services ranging from room access, dining, and purchases onboard. Additionally, verification of identification is often associated with human error, however, automated systems like those based on RFID also reduce such errors and accurately identify passengers with these system strengths, some challenges have been identified. The issue of privacy, particularly related to facial recognition technology, is one of the major concerns. Many passengers may not know how their biometric data will be used and protected, thus making them reluctant to accept the collection and retention of sensitive information like biometric data. This has generated concern regarding the safety of biometric databases and the proprietary access that can be exercised by unauthorized users sensitive data in the event of hacking. The reliability of some biometric systems poses a different challenge. As an illustration, recognition of faces can be subject to changes in the operating environment such as lighting and even the appearance of the passengers. There are cases where passengers are not properly recognized because of the aforementioned factors. Analogously, RFID systems do experience challenges relating to the interference with or failure of the signals, which can lead to delays in operations. Some cruise lines may find the costs associated with implementing and maintaining the systems too high, specifically when retrofitting older ships with legacy systems.

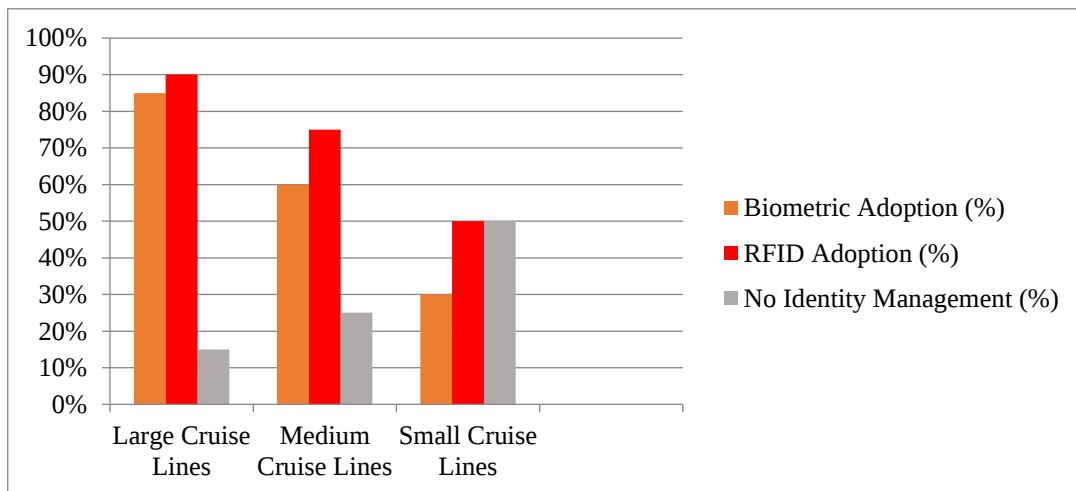


Figure 3: Adoption Rates of Biometric and RFID Systems in the Cruise Industry

The graph (Figure 3) illustrates how different sized cruise lines utilize traditional identity management, biometric systems, and RFID technology. It indicates that large cruise lines have the highest adoption of both biometric (85%) and RFID (90%) systems, showing great adoption of modern security technologies. Medium sized cruise lines come next with moderate adoption, whereas small cruise lines trail behind with biometric (30%) and RFID (50%) systems. It is worth noting that small

lines also report the greatest percentage (50%) of operating without any formal identity management solution, underscoring the lack of security infrastructure at that level. From the provided information, the graph (Figure 4) captures an apparent lack of privacy concern parallel to the adoption rate of biometric systems in cruise ship services. Adoption is high when there is low concern; biometric adoption is at 75%. However, as concern rises to moderate and high, adoption decreases to 60% and 40%, respectively. This information shows the strong impact that data privacy perceptions have on the willingness of cruise operators or passengers to adopt biometric solutions (Belakapyskaya, 2021). There is, however, an increase in concern within the data that indicates greater care will need to be exercised within biometric enabled technologies if trust is to be established. The diagram (Figure 5) evaluates three technologies of identity verification—Face Recognition, RFID, and Hybrid Systems—by measuring their reliability and the satisfaction earned from cruise passengers. In cruise passengers satisfaction, Facial Recognition leads with 95% reliability—satisfaction score of 88% pointing to both effectiveness and user approval. Following was the RFID system which recorded 90% reliability, however their satisfaction rate dropped to 85%. These results were also outperformed by Hybrid Systems which amalgamate several technologies. They achieved 92% reliability along with the highest satisfaction score of 90%, implying that integrated systems might provide a better cruise experience.

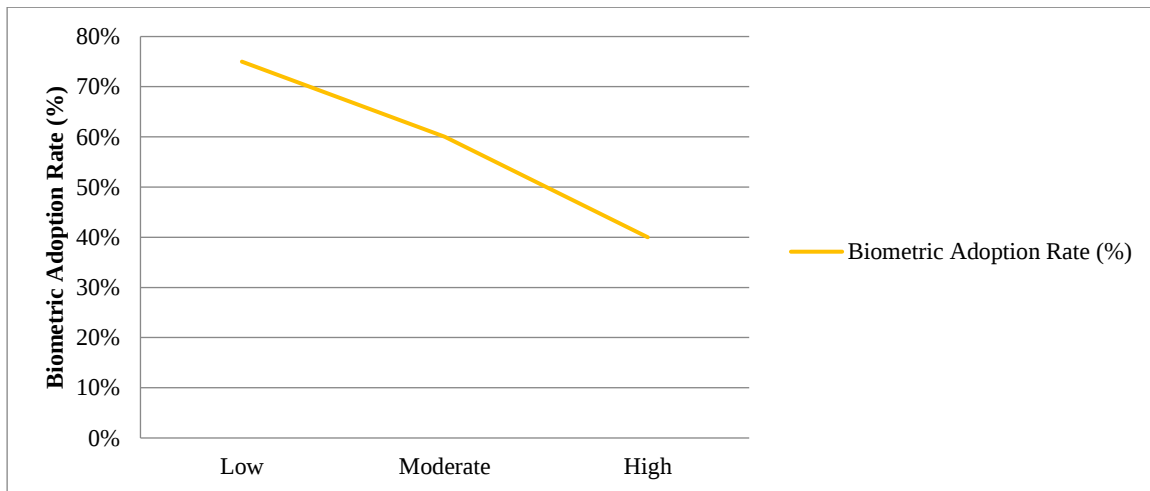


Figure 4: Privacy concerns vs. adoption of biometric technology

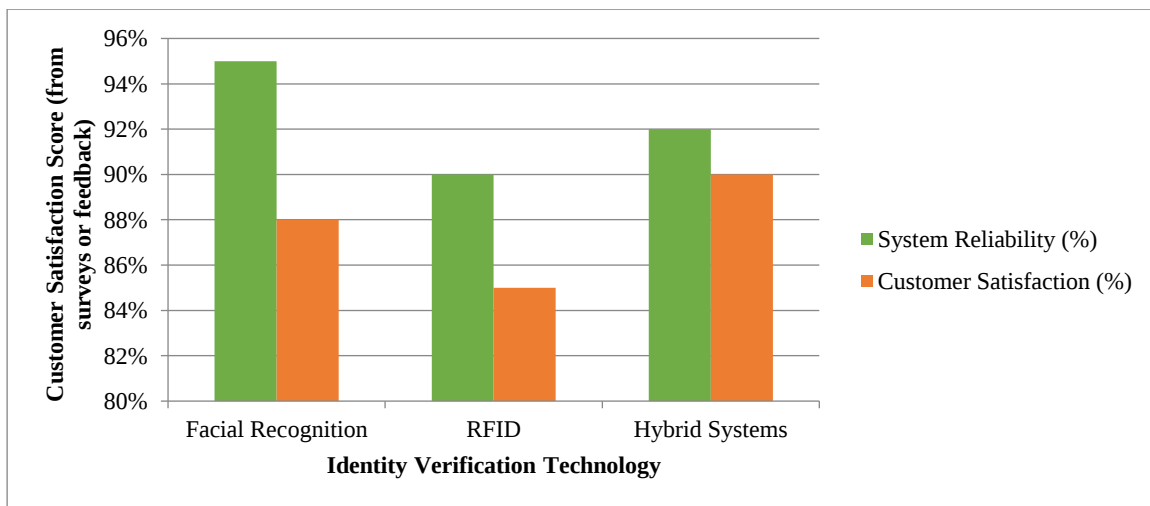


Figure 5: System Reliability and Customer Satisfaction

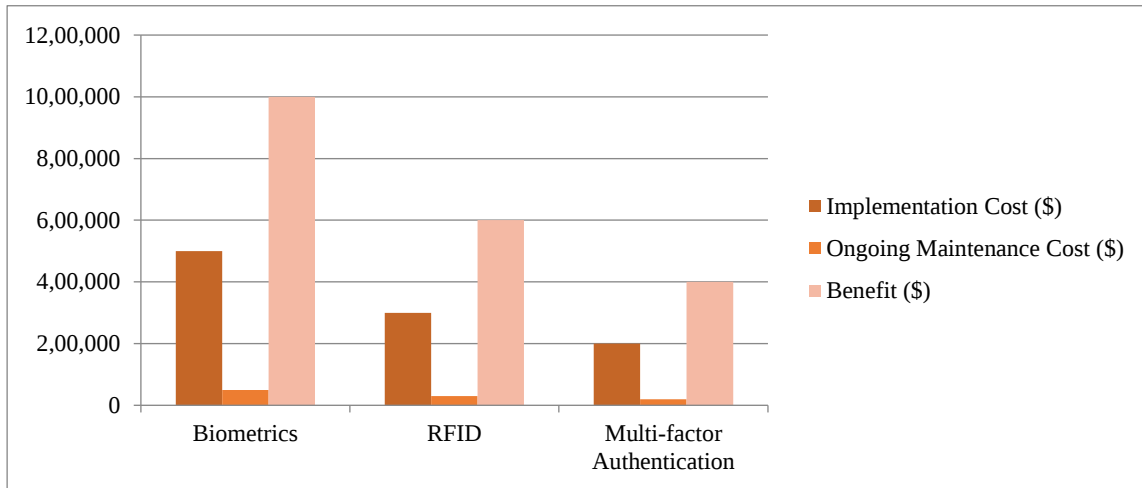


Figure 6: Cost vs. Benefit of Implementing Identity Management Systems

The capital expenditure and operational expense analysis of the cruise industry's three identity technologies, illustrated in the graph (Figure 6) depicts the balance between expected benefits and the implementation as well as maintenance costs incurred. Biometric systems offer the highest benefits, achieving a return of \$10 million despite undergoing the most expensive initial cost involving implementation, approximately \$5 million, indicating a strong return on investment. In terms of cost-benefit ratio, RFID technologies present a moderate profile with implementation costs of \$3 million and benefits of \$6 million. Multi-factor authentication presents the lowest costs and benefits, thus being economically appealing but less impactful. In summary, the graph validates the economic rationale behind the adoption of sophisticated identity management systems.

The current gaps in processes based on existing systems of identity verification, need to be improved and addressed. The uppermost challenge in the fusion of privacy and identity verification technologies is one of the privacy. Cruise operators need to have the correct policies to tell their patrons concerning the storage, usage and protecting of personal biometric data. Proper handling of privacy and consent issues guarantees that sensitive data is encrypted and that biometric information is either entirely stripped of identifying characteristics, dormant erasure or locked away in data vaults, thereby ensuring security against unauthorized access and breach. Moreover, clear consent agreements with passengers and the escape clause of opting out would strengthen confidence to trust such systems. Investing in more precise and dependable biometric technologies is one way to improve identity verification systems. As an example, facial recognition could be fused with iris scans or voice recognition for more advanced multi-modal biometric identification systems. The accuracy of identity verification would be improved, and extra security would be added by requiring multiple verifications before access is granted to restricted areas or services in the ship. Reliability of the systems is another area that requires focus. Cruise lines need to purchase quality hardware and software to reduce technical faults. Routine servicing and updates to the biometric and RFID systems are needed to ensure they work under different conditions. Systems should also be tested in different environmental scenarios. Changes in lighting and crowd density are some of the conditions that may affect the performance of the system. Passengers should not be affected by the issues arising from changes in these conditions. The incorporation of multi-factor authentication (MFA) could provide even more fortification for the identity verification procedures. For instance, mobile authentication through QR codes or apps can be paired with biometric verification for added protection. Even if one of the authentication methods is compromised, fraudulent access would still be incredibly difficult to obtain. MFA serves as a crucial asset for sensitive transactions involving access

to personal information or purchases made onboard. In the end, heightened education and awareness of the biometric and RFID security features would alleviate concerns for passengers. Effective communication detailing the functioning of these technologies, their benefits, and the protective measures employed concerning passenger privacy will cultivate trust and increase acceptance of these systems. To summarize, the cruise industry has succeeded in incorporating sophisticated identity management technologies, but there remains room for improvement. Attention to privacy concerns, system dependability, and integration collaboration would greatly advance identity verification systems in the cruise industry. A balance of sophisticated technologies with clear data handling, heightened passenger education, and advanced data management will uphold security and operational efficiency while delivering a streamlined and safeguarded experience for passengers.

5 Implications

The application of modern identity management systems and advanced authentication techniques in the cruise ship business marks a new era in operational efficiency, passenger service experience, and compliance with laws and policies. With cruise ships transporting thousands of passengers and crew members across international borders, identification systems have to be secure, accurate, and immediate. Modern technology such as biometric facial recognition, RFID access cards, and multi-factor authentication systems let cruise lines refine their processes, heighten security, and improve the quality of service delivery. In relation to operational processes, these technologies can substantially alleviate the amount of time needed to check-in and board. As an illustration, biometric facial recognition systems can replace identity checks done by staff with automated processes. This serves to speed up boarding and reduce human error as well as increase throughput at ports during peak exodus and surging claustrophobia disembarkation hours. Moreover, sophisticated authentication systems can be implemented in the cabin, dining areas, and entertainment domains which can grant attendees entry without the physical keys or cards which are often mislaid or traded.

New identity management strategies enable cruise lines to offer tailored and personalized experiences to customers through advanced technology. Integrated systems can link a customer's identity to their travel history, preferences, and behavior onboard, allowing each passenger to receive customized menus, leisure activities, and location-oriented services. All these improvements help boost customer satisfaction appreciably while improving brand perception. While the advantages may prove beneficial to companies, the accompanying challenges can be quite significant and difficult to navigate. Small and medium-sized operators may struggle with high implementation costs as well as ongoing maintenance expenses. New advanced systems might require considerable additional technical support for proper alignment with existing IT infrastructure. Moreover, there is a critical consideration of potential service disrupting system failures and downtime that might impact passenger safety, resulting in unresolved customer dissatisfaction.

Equally concerning is the need to maintain an individual's privacy alongside data protection. As sensitive as biometric information is, it can cause significant damage when mismanaged, such as data leaks, identity theft, and erosion of trust. Cruise companies need to address international regulations like the General Data Protection Regulation (GDPR) to guarantee adequate systems and strong encryption, secure storage, and clear data usage framework. Obtaining consent from passengers to use their private information and strictly controlling the information's access are important in preventing legal and ethical challenges. To summarize, decision making in the cruise industry may be enhanced through the implementation of sophisticated identity management systems and authentication technologies, however they require operational and ethical investments at the same time. Managing a budget, integrating

systems, and securing data will serve as the foundation for overcoming such advanced challenges. If executed properly, the particular changes will revolutionize maritime tourism by offering unparalleled standards of trust, efficiency, and security.

6 Conclusion

This study highlights the increasing need for efficient identity management and authentication technologies in the cruise ship sector. As the industry grows and shifts to digital processes, advanced identity verification systems are essential for passenger safety, operational effectiveness, and compliance with legal requirements. Those findings indicate that there is an uneven application of biometric, RFID, and multi-factor authentication technologies among different cruise lines. Large cruise operators appear to be at the forefront of adopting these technologies, but are still lagging relative to mid and small sized operators. Additionally, the absence of these technologies is still governed by a lack of privacy, system reliability, and cost effectiveness of the technology. Reviewing literature and analyzing industry data reveals that biometric technologies present the highest level of acceptance but face challenges of privacy concerns and implementation costs. However, hybrid systems offer the greatest promise as they can blend multiple technologies to omit various drawbacks. Customer feedback also suggests a strong relationship between satisfaction with identity verification systems and the reliability of the systems, emphasizing the need for identity verification solutions. Further studies should develop incrementally more efficient identity management systems that can be utilized by smaller cruise operators. Also, privacy-preserving biometric safeguards such as decentralized identity systems paired with encryption-based authentication protocols warrant immediate attention. Other directions with potential for proactive security monitoring and instantaneous decision-making might involve the applications of AI and machine learning in identity verification. In end, improving the processes of identity verification is more than simply implementing new technologies—it is a necessary advancement for safer, streamlined, and passenger-centric cruise operations. As the global technology landscape poses new opportunities and challenges, the maritime transportation industry constantly finds itself in a state of evolution. Identity management is bound to remain foundational in innovation, security, and trust.

References

- [1] Abdullah, D. (2024). Enhancing cybersecurity in electronic communication systems: New approaches and technologies. *Progress in Electronics and Communication Engineering*, 1(1), 38-43.
- [2] Akshara, S., Venkatesh, P., & Baskar, R. (2021). Exploring the impact of biometric technologies in cruise passenger identification. *Maritime Technology Journal*, 6(2), 42–58.
- [3] Aloysius, F., & Alhaji, F. (2020). Identity management in transportation: Security and convenience balance. *Transportation Security Journal*, 5(4), 57–71.
- [4] Belakapyskaya, A. (2021). Passenger facilitation solutions. *Belarusian State University; editorial board: Minsk: BSU*, 401–405.
- [5] Bennett, A., Cook, H., & Thompson, D. (2019). The role of biometrics in maritime security: Current practices and future directions. *International Journal of Maritime Affairs*, 8(1), 78–92.
- [6] Chang, Y. T., Lee, S., & Park, H. K. (2017). Efficiency analysis of major cruise lines. *Tourism Management*, 58, 78-88. <https://doi.org/10.1016/j.tourman.2016.10.012>
- [7] Chen, Y., Zhang, X., & Li, L. (2021). Biometric authentication in healthcare systems: A comprehensive review. *Health Security Journal*, 8(2), 122–135.
- [8] Donkor, K., & Zhao, Z. (2024). The Impact of Digital Transformation on Business Models: A Study of Industry Disruption. *Global Perspectives in Management*, 2(3), 1-12.

- [9] Genç, R. (2016). Sustainability on Cruise Ship Management. *Int'l J. Soc. Sci. Stud.*, 4, 76. <https://doi.org/10.11114/ijsss.v4i6.1601>
- [10] Gupta, S., Modgil, S., Lee, C. K., & Sivarajah, U. (2023). The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry. *Information Systems Frontiers*, 25(3), 1179-1195. <https://doi.org/10.1007/s10796-022-10271-8>
- [11] Huang, Q., & Zhang, X. (2020). The future of identity management in maritime passenger services. *Journal of Maritime Transport and Management*, 4(3), 52–64.
- [12] Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. *SCCTS Transactions on Reconfigurable Computing*, 1(1), 16-20.
- [13] Krishnan, H., Santhosh, Vijay, & Yasmin, S. (2022). Blockchain for Health Data Management. *International Academic Journal of Science and Engineering*, 9(2), 23–27. <https://doi.org/10.9756/IAJSE/V9I2/IAJSE0910>
- [14] Kuhn, K., McIlhatton, D., Malcolm, J. A., & Chapsos, I. (2023). Protective security at sea: A counter terrorism framework for cruise and passenger ships. *WMU Journal of Maritime Affairs*, 22(3), 345-363. <https://doi.org/10.1007/s13437-022-00296-w>
- [15] Lai, S., Wei, F., & Chen, Y. (2020). Self-service kiosks and biometric verification in airports: A case study of Guangzhou Airport. *Journal of Transportation Technology*, 12(6), 101–116.
- [16] Marinković, G., Milutinović, T., & Božić, M. (2024). Identification and analysis of risks in Civil Engineering Projects. *Archives for Technical Sciences*, 1, 45. <https://doi.org/10.59456/afts.2024.1630.045M>
- [17] Merriam, S. B., & Baumgartner, L. M. (2020). *Learning in adulthood: A comprehensive guide*. John Wiley & Sons.
- [18] Monette, P. (2021). Mustering. *Michigan Quarterly Review*, 60(1), 176-0_19.
- [19] Morgan, D., & Ritchie, J. (2019). RFID-enabled systems for seamless passenger experience in aviation and maritime industries. *Journal of Applied Technology in Transportation*, 9(3), 143–157.
- [20] Muralidharan, J. (2023). Innovative RF design for high-efficiency wireless power amplifiers. *National Journal of RF Engineering and Wireless Communication*, 1(1), 1-9.
- [21] Nakamura, Y., & Lindholm, M. (2025). Impact of Corn Production on Agriculture and Ecological Uses of Olive Mill Sewage using Ultrafiltration and Microfiltration. *Engineering Perspectives in Filtration and Separation*, 2(1), 13-17.
- [22] Papadopoulos, G., & Christodoulou, M. (2024). Design and Development of Data Driven Intelligent Predictive Maintenance for Predictive Maintenance. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, 2(2), 10-18.
- [23] Patel, R., & Thakkar, A. (2020). RFID technology in logistics: A comprehensive case study. *Logistics and Supply Chain Management Review*, 8(4), 134–147.
- [24] Pérez, R., & García, M. (2020). Biometric systems in the cruise industry: Opportunities and challenges. *International Journal of Hospitality and Tourism*, 14(1), 23–38.
- [25] Prakash, M., & Prakash, A. (2023). Secured Data Transmission Using Improved Blowfish Algorithm and Enhanced Homomorphic Cryptosystem for WSNs. *International Journal of Advances in Engineering and Emerging Technology*, 14(2), 01-14.
- [26] Rahim, R. (2024). Scalable architectures for real-time data processing in IoT-enabled wireless sensor networks. *Journal of Wireless Sensor Networks and IoT*, 1(1), 28-31. <https://doi.org/10.31838/WSNIOT/01.01.07>
- [27] Rawal, B. S., Manogaran, G., & Peter, A. (2023). *Cybersecurity and identity access management*. Singapore: Springer.
- [28] Saeed, S., & Qamar, A. (2021). Mobile-based identity management: The future of passenger services. *Mobile Technology Journal*, 6(3), 115–128.
- [29] Samyadevi, V., Anguraj, S., Singaravel, G., & Suganya, S. (2024). Image Based Authentication Using Zero-Knowledge Protocol. *International Academic Journal of Innovative Research*, 11(1), 01–05. <https://doi.org/10.9756/IAJIR/V11I1/IAJIR1101>

- [30] Sengupta, M. (2020). One ID: The future of passenger processing in air travel. *Aviation Technology Review*, 3(1), 12–26.
- [31] Vethachalam, S. (2021). DevSecOps Integration in Cruise Industry Systems: A Framework for Reducing Cybersecurity Incidents. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, 13(02), 158-167.
- [32] Wu, L., Dong, C., & Xiong, G. (2020). A big-data-based analysis on the impact of cruise tourism image on Chinese tourist satisfaction and behavioral intentions. *Journal of Coastal Research*, 106(SI), 314-318. <https://doi.org/10.2112/SI106-073.1>
- [33] Wu, Z., & Margarita, S. (2024). Based on Blockchain and Artificial Intelligence Technology: Building Crater Identification from Planetary Imagery. *Natural and Engineering Sciences*, 9(2), 19-32. <https://doi.org/10.28978/nesciences.1567736>
- [34] Zhang, Y., Li, Y., & Wang, J. (2020). Blockchain technology for secure and decentralized identity management in transportation. *Journal of Emerging Technologies in Transportation*, 7(2), 51–67.
- [35] Zhao, F., Li, T., & Sun, Y. (2021). Biometric solutions for airport security: Current trends and future prospects. *Journal of Air Transportation Security*, 14(2), 35–49.
- [36] Zhou, J., Chen, S. L., & Shi, W. (2022). The concept of the cruise supply chain and its characteristics: an empirical study of China's cruise industry. *Maritime Business Review*, 7(3), 196-221. <https://doi.org/10.1108/MABR-06-2021-0046>

Authors Biography



Capt. Krishnamurthy Kumar (more fondly known as Capt R K Kumar) was a state-level merit scholarship holder in his High-School Board examinations. He passed out from Training Ship “Rajendra” in First Class in 1974 and cleared his MASTER (FG) Competency Examinations in 1983 in first attempt. After serving at sea for 20 years in various ascending ranks, he came ashore as Principal Surveyor with M/s J.B. Boda Surveyors where he was involved in investigating several Casualty incidents such as Groundings, Collisions, major fires, Mega cargo claims and GA surveys. He had also done several consultancy assignments for Project Cargo shipments and turn-key projects. After 12 years as a surveyor he joined the CCTL Container terminal serving 4 years as Operations Head under P&O ports. He, along with his two member team, won the second prize amongst all the 21 global container terminals of P&O Ports for “innovative OHSE measures”. Capt. RKK is currently serving as Associate Professor in AMET University for past 20 years having joined as a Marine faculty in 2004. His tenure includes 3 years as Dean of Nautical Science and chairperson of Maritime Studies. He is a member of the prestigious CMMI, India and an Ex- Fellow of the Institute of Chartered Shipbrokers, UK. He won the South-India topper’s Prize in the Institute’s Examination in Shipping Practice in 1996. He is also currently the Indian Ambassador for CHIRP MARITIME, United Kingdom aimed at promoting awareness of confidential Reporting of Maritime Incidents amongst Seafarers.



Capt. K. Karthik graduated with a Bachelor's degree in Physics and is a Master Mariner with 16 years of sea-going experience on various dry and liquid cargo vessels, including crude oil, product, and chemical tankers, general cargo, and bulk carriers. He began his academic career with AMET University in 2007 and has since held several key positions, including Professor, Director – Centre for International Relations, Dean – Post Sea and Simulator Training, and currently serves as the Dean and Head of the Department of Nautical Science. His professional interests span maritime education, simulator-based training, youth development. He holds a post graduation in Shipping

and logistics and yoga for human excellence. He is currently the principal of AMET Institute of science and technology, Maersk Centre of Excellence campus.



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.