Advances in Cybersecurity Risk Mitigation for Autonomous Systems in Maritime and Intermodal Transport Infrastructure

FRANCESS CHINYERE OKOLO[1], EMMANUEL AUGUSTINE ETUKUDOH[2], OLUFUNMILAYO OGUNWOLE[3], GRACE OMOTUNDE OSHO[4], JOSEPH OZIGI BASIRU[5]
[1]*Texas Southern University, USA*
[2]*Fleet Manager, Nigeria*
[3]*SAKL, Lagos Nigeria*
[4]*Guinness Nig.Plc*
[5]*S. C. C. Nigeria Limited*

Abstract- ***The rapid integration of autonomous systems in maritime and intermodal transport infrastructure has revolutionized operational efficiency, navigation precision, and logistics management. However, the growing dependence on digital technologies and interconnected systems exposes these critical infrastructures to escalating cybersecurity threats. This paper explores recent advances in cybersecurity risk mitigation tailored for autonomous maritime vessels and intermodal transport systems, including ports, railways, and logistics hubs. It provides a critical assessment of threat vectors such as GPS spoofing, sensor manipulation, communication jamming, and malware attacks targeting navigation and control systems. Additionally, the paper examines the role of advanced encryption, intrusion detection systems (IDS), blockchain technology, and AI-driven threat analytics in enhancing the security posture of these infrastructures. Real-world case studies and regulatory frameworks, such as the IMO's cybersecurity guidelines and EU cybersecurity directives, are analyzed to demonstrate practical applications and policy implications. The paper concludes by identifying key challenges, including system interoperability, legacy vulnerabilities, and the need for standardized cybersecurity protocols, and recommends a multidisciplinary approach combining technical innovation, regulatory compliance, and continuous risk assessment to safeguard autonomous transport systems in an increasingly digital maritime and intermodal ecosystem.***

Indexed Terms- ***Transport infrastructure, cyber threat analytics, digital twins security, critical infrastructure protection, maritime navigation security***

I. INTRODUCTION

The global transportation landscape is undergoing a significant transformation, driven by rapid advances in automation, digitization, and smart infrastructure. Among the most transformative developments are autonomous systems, which are increasingly being integrated into maritime and intermodal transport networks to enhance operational efficiency, reduce human error, and optimize supply chain performance [1]. Autonomous ships, smart ports, and connected intermodal hubs are now pivotal elements of modern logistics ecosystems. However, as these systems become more reliant on complex software, sensors, and networked communication technologies, they also present a broader and more intricate cybersecurity threat surface. Maritime and intermodal transport systems operate in environments where safety, continuity, and reliability are paramount [2]. The integration of autonomous technologies introduces vulnerabilities that, if exploited, could lead to significant disruptions, financial losses, environmental damage, or even threats to human life [3]. Attacks on navigation systems, manipulation of cargo management platforms, or breaches in communication protocols between autonomous vehicles and central control stations are examples of critical risks faced in this domain. Unlike traditional cyber-physical systems, those used in maritime and intermodal contexts often involve legacy systems, distributed stakeholders, and international regulations, making cybersecurity both technically and logistically challenging [4]- [6].

Recent advances in cybersecurity for these sectors have focused on enhancing threat detection, real-time monitoring, and incident response mechanisms tailored to the specific needs of autonomous operations. Techniques such as artificial intelligence (AI)-driven anomaly detection, blockchain for secure data sharing, and zero-trust architectures are being explored to fortify systems against both internal and external threats [7]. Additionally, simulation-based testing environments, digital twins, and standardized cybersecurity frameworks are emerging as critical tools for resilience-building. These technologies not only aim to detect and prevent cyber incidents but also ensure that systems can recover rapidly with minimal disruption [8]. Equally important is the alignment of technological measures with regulatory and organizational strategies. Industry stakeholders, including port authorities, shipping companies, logistics providers, and government agencies, are increasingly collaborating to define cybersecurity best practices, compliance requirements, and coordinated response strategies [9]. Global maritime regulatory bodies such as the International Maritime Organization (IMO) have issued guidelines addressing cybersecurity in maritime operations, urging stakeholders to implement risk-based approaches tailored to their operational realities [10].

In light of these developments, this study explores the latest advances in cybersecurity risk mitigation specifically for autonomous systems in maritime and intermodal transport infrastructure. It examines the evolving threat landscape, evaluates state-of-the-art mitigation techniques, and discusses the regulatory, organizational, and technical frameworks that are shaping a secure future for autonomous transport [11]. The findings underscore the urgency of adopting proactive and adaptive cybersecurity strategies as digital transformation continues to redefine global transport infrastructure.

II. LITERATURE REVIEW

The increasing reliance on autonomous systems in maritime and intermodal transport infrastructure has ushered in significant operational efficiencies and improvements in safety [12]. However, these benefits are accompanied by growing vulnerabilities to cyber threats, raising critical concerns about cybersecurity risk mitigation. As digitalization deepens in the transport sector, especially with the proliferation of artificial intelligence (AI), Internet of Things (IoT), and machine-to-machine (M2M) communications, there is an urgent need to understand the evolving threat landscape and develop robust cybersecurity frameworks tailored to the unique characteristics of maritime and intermodal systems [13]- [15]. The maritime domain, traditionally reliant on mechanical systems and human operation, is undergoing a transformation with the integration of Maritime Autonomous Surface Ships (MASS), automated port operations, and interconnected logistics networks [16]. These systems, while enhancing navigational precision and operational reliability, also present an expanded attack surface. Cyberattacks targeting Global Navigation Satellite Systems (GNSS), Automatic Identification Systems (AIS), and Electronic Chart Display and Information Systems (ECDIS) have been documented, demonstrating the real-world implications of compromised maritime cybersecurity [17]. Research by Tam and Jones (2019) highlighted vulnerabilities in AIS, which could be exploited to spoof ship positions, disrupt maritime traffic, or facilitate smuggling and piracy. The potential for such cyber threats to disrupt international trade and logistics necessitates a coordinated response [18].

In response to these emerging risks, several frameworks and technologies have been proposed to enhance the cybersecurity posture of autonomous maritime systems [19]. One notable approach involves the adoption of risk-based methodologies, such as the Maritime Risk Assessment and Mitigation (MRAM) model, which evaluates the likelihood and impact of cyber incidents across shipboard and shore-based systems [20]. The MRAM framework, built on the ISO/IEC 27001 standard, integrates threat modeling, vulnerability assessment, and impact analysis to guide security policy development [21]. Moreover, regulatory efforts by the International Maritime Organization (IMO), including the inclusion of cyber risk management in the International Safety Management (ISM) Code, underscore the growing recognition of cybersecurity as a critical component of maritime safety. Autonomous systems in intermodal transport infrastructure—where cargo is moved across

various modes such as ships, trains, and trucks—introduce additional complexity [22]. These systems require secure and seamless data exchanges across heterogeneous networks and organizational boundaries. Cyber-physical systems (CPS) and digital twins have been employed to manage and simulate these logistics operations, but they too are vulnerable to cyber threats such as data manipulation, ransomware attacks, and denial-of-service (DoS) disruptions [23]. A study by [24] emphasized the importance of secure-by-design principles in the architecture of smart transport infrastructure, recommending the use of zero-trust architectures, strong identity management, and end-to-end encryption to mitigate cyber risks [24].

Artificial Intelligence (AI) and Machine Learning (ML) have shown promise in enhancing anomaly detection and predictive analytics within autonomous transport systems [25]. These technologies can identify deviations from normal patterns in real-time, allowing for rapid incident response. For instance, AI-driven intrusion detection systems (IDS) have been applied in port cybersecurity to monitor network traffic and detect suspicious activity, significantly reducing response times to potential threats. However, AI systems themselves can become targets of adversarial attacks, raising concerns about their reliability and trustworthiness in critical applications. Research by [26] warns of the vulnerability of ML algorithms to data poisoning and model inversion attacks, which can compromise decision-making processes in autonomous systems. Blockchain technology has also emerged as a potential solution for enhancing the integrity and transparency of data flows in intermodal logistics. By decentralizing data storage and verification, blockchain can reduce the risk of single points of failure and unauthorized data alterations [27]. Pilots such as TradeLens and the Digital Container Shipping Association (DCSA) have explored blockchain for secure documentation and cargo tracking. Despite these advances, challenges remain in scaling blockchain solutions, ensuring interoperability, and addressing regulatory uncertainties.

Human factors and organizational readiness continue to play a significant role in cybersecurity risk mitigation. Training programs, awareness campaigns, and cybersecurity drills are essential to prepare crew members and logistics personnel for cyber incidents [28]. Moreover, the establishment of incident response teams and the integration of cybersecurity into broader safety management systems are critical steps in building resilient infrastructure. The concept of a cybersecurity culture, promoted by the European Union Agency for Cybersecurity (ENISA), emphasizes the need for an organization-wide commitment to cybersecurity practices, particularly in environments where human-machine collaboration is prevalent [29]. Collaborative initiatives and public-private partnerships have gained momentum as a strategy to address cybersecurity risks across the transport sector. Programs such as the Maritime Cyber Risk Assessment (MaCRA), NATO's Cyber Maritime Strategy, and the EU's Cybersecurity Act aim to foster information sharing, harmonize security standards, and promote the development of secure technologies [30]. Additionally, cyber threat intelligence (CTI) platforms enable stakeholders to exchange real-time information on emerging threats and vulnerabilities, enhancing collective situational awareness.

Despite the progress, several research gaps remain [31]. The integration of cybersecurity into the design phase of autonomous systems is still limited, often treated as an afterthought. There is also a need for standardized metrics to assess cybersecurity resilience across different transport domains [32]. Future research should explore the convergence of cybersecurity and safety assurance, particularly in scenarios involving mixed-initiative systems where human and autonomous agents coexist. Furthermore, the legal and ethical implications of cyber incidents in autonomous transport—such as liability attribution and compliance with international regulations—require thorough investigation. The advancement of autonomous systems in maritime and intermodal transport offers transformative benefits, but it also amplifies cybersecurity challenges that must be proactively addressed [33]. A multifaceted approach encompassing technical, organizational, regulatory, and collaborative measures is essential to safeguard these critical infrastructures. The continued evolution of threat landscapes demands adaptive and resilient cybersecurity strategies, informed by interdisciplinary research and global cooperation [34]. As autonomy becomes the new norm in transport, cybersecurity

must evolve in parallel to ensure the safe, secure, and sustainable movement of goods and people across the globe.

2.1 Proposed Conceptual Model

The increasing integration of autonomous systems within maritime and intermodal transport infrastructures represents a significant advancement in global logistics, navigation efficiency, and safety optimization. However, this evolution simultaneously introduces a new dimension of vulnerabilities, particularly in the realm of cybersecurity [35]. As these systems become increasingly reliant on interconnected digital technologies—ranging from artificial intelligence (AI) to the Internet of Things (IoT)—they also become attractive targets for cyber threats. Addressing these concerns necessitates a comprehensive and adaptive conceptual model that encapsulates technological, organizational, and regulatory dimensions for mitigating cybersecurity risks [36]. At the core of the proposed model lies the principle of resilience through layered cybersecurity. This framework integrates multiple defense mechanisms—preventive, detective, and responsive—in an interdependent architecture that is contextually aware of the operational environment. The foundational layer of the model comprises robust hardware and software security protocols, including embedded encryption, secure boot processes, and real-time threat detection capabilities using AI-driven anomaly detection systems [37]. In the case of autonomous vessels or smart port systems, these technologies must be capable of detecting subtle deviations in network traffic, sensor data, and command pathways that might indicate a cyber intrusion or a system anomaly.

The second layer involves intelligent communication security, focusing on securing data flows between autonomous vehicles, port infrastructure, cargo systems, and centralized monitoring units [38]. Secure communication protocols such as quantum-resistant cryptography and blockchain-enhanced transmission systems ensure the integrity and non-repudiation of data in transit. Blockchain, in particular, plays a dual role: first, as a decentralized trust mechanism for authenticating devices and operators; and second, as an immutable ledger for operational data, enabling traceability and forensic analysis in the event of a cyber breach [39]. In intermodal transport, where cargo may shift between autonomous ships, smart rail systems, and automated road transport, maintaining seamless and secure data continuity is paramount.

The third layer incorporates autonomous cyber response and recovery mechanisms, where systems are capable of not only detecting but also dynamically responding to cyber incidents. This involves the implementation of machine learning-based predictive analytics to assess potential threats and initiate automatic containment protocols [40]. In a smart port scenario, for example, if abnormal behavior is detected in a container tracking subsystem, the system may automatically isolate that subsystem, reroute operations, and notify human operators. This kind of built-in cyber resilience minimizes operational disruptions and allows for graceful degradation instead of total system failure. A critical aspect of the model is the human-in-the-loop (HITL) integration, which ensures that while systems operate autonomously, human oversight and intervention remain possible and effective [41]. This is particularly important in high-stakes maritime environments where decisions must balance safety, legality, and commercial priorities. Training operators using digital twins and cybersecurity simulation platforms allows stakeholders to rehearse response strategies in virtual environments, building familiarity with emerging threats and appropriate mitigation actions [42].

In terms of governance, the model emphasizes compliance with international cybersecurity frameworks such as the International Maritime Organization's (IMO) guidelines on maritime cyber risk management and the European Union Agency for Cybersecurity (ENISA) recommendations. These regulatory frameworks must be embedded into the operational algorithms and decision-making processes of autonomous systems, ensuring continuous alignment with evolving legal and ethical standards [43]. Furthermore, the proposed model advocates for real-time auditability and transparency through integrated compliance dashboards powered by AI-driven monitoring systems. These dashboards aggregate threat intelligence data, system logs, and compliance metrics to offer a comprehensive view of

the cybersecurity posture across the entire intermodal transport network [44]. The conceptual model also prioritizes collaborative risk intelligence sharing, recognizing that cybersecurity is not a siloed responsibility but a collective enterprise. Secure, anonymized data-sharing protocols between shipping companies, port authorities, transport operators, and governmental agencies are necessary for building a federated threat intelligence ecosystem. This ecosystem uses data fusion and pattern recognition to identify emerging attack vectors and disseminate warnings across the network before attacks can propagate [46]. In this sense, the model supports a shift from reactive to proactive cybersecurity through community-based situational awareness.

On a technological innovation front, the model envisions the use of edge computing and federated learning to bring computational intelligence closer to the operational endpoints—autonomous vessels, cranes, trucks, etc.—without compromising data privacy. Federated learning allows AI models to be trained locally on encrypted data at the edge, and only the aggregated model parameters are shared, not the raw data itself. This ensures privacy-preserving machine learning while benefiting from the diverse data sources across the maritime and intermodal landscape. Combined with edge analytics, this approach enhances threat detection, predictive maintenance, and system optimization in real time, even in bandwidth-constrained environments. The model underscores the significance of cyber-physical systems (CPS) integration. In autonomous maritime and intermodal settings, the interplay between physical actions and cyber instructions is critical [47]. A cyberattack on a navigation system or cargo crane could translate into physical accidents, port congestion, or environmental disasters. Therefore, cybersecurity must not only protect data but also ensure the integrity of physical operations. This involves testing systems using fault injection, red-teaming, and formal verification methods to evaluate how cyber vulnerabilities could lead to real-world harm and how to prevent or contain such outcomes. The proposed conceptual model advocates a holistic, adaptive, and multi-layered approach to mitigating cybersecurity risks in autonomous systems within maritime and intermodal transport infrastructures. By combining technological innovation with strategic governance, human oversight, and collaborative intelligence, this model positions cybersecurity not as an afterthought, but as a core enabler of safe, efficient, and resilient autonomous transportation systems [48].

2.2 Implementation Approach

The rapid evolution of autonomous systems within maritime and intermodal transport infrastructure presents both groundbreaking opportunities and unprecedented cybersecurity risks. As these infrastructures grow increasingly digitized and interconnected, safeguarding them against emerging cyber threats becomes a mission-critical priority [49]. The implementation of advanced cybersecurity risk mitigation strategies in this domain demands a multifaceted approach—one that encompasses technological, procedural, and organizational advancements tailored to the unique nature of transport and logistics ecosystems. Implementing effective cybersecurity measures begins with a comprehensive risk assessment, designed to identify vulnerabilities across physical, cyber, and human layers of maritime and intermodal operations. The initial step involves mapping all digital assets and communication channels across autonomous vessels, smart ports, intermodal hubs, and control centers. This includes Internet of Things (IoT) sensors, industrial control systems (ICS), global navigation satellite systems (GNSS), and AI-driven decision-support systems [50]. Advanced threat modeling must then be employed to anticipate potential attack vectors such as GPS spoofing, jamming, ransomware, insider threats, and zero-day vulnerabilities. These assessments must be dynamic and iterative, continuously updated to reflect changes in infrastructure, threat landscapes, and technology stacks. Following the risk identification phase, the implementation of robust cybersecurity frameworks grounded in international standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and the International Maritime Organization (IMO) guidelines is critical. These frameworks provide structured methodologies for establishing and maintaining information security management systems (ISMS), tailored to both operational technology (OT) and information technology (IT) environments. Leveraging these standards allows for consistency and interoperability across maritime and land-based intermodal transport

infrastructures, fostering global alignment in cybersecurity postures.

A key aspect of implementation is the deployment of secure communication protocols and encrypted data exchange mechanisms to protect the integrity and confidentiality of operational data. Transport Layer Security (TLS), secure application programming interfaces (APIs), and blockchain-based data logging can provide traceable, tamper-proof audit trails across decentralized systems. In particular, blockchain technology holds promise in safeguarding logistics records, ensuring trusted cargo provenance, and validating autonomous vehicle routing data. For autonomous maritime vessels, secure onboard communication systems integrated with shore-based command centers should incorporate multi-factor authentication, real-time anomaly detection, and fail-safe backup protocols in case of cyber incidents. Artificial Intelligence (AI) and Machine Learning (ML) techniques also play a pivotal role in real-time threat detection and response. Implementing AI-driven Security Information and Event Management (SIEM) systems enables predictive analytics, facilitating the identification of abnormal patterns that may indicate cyber intrusions. These systems should be integrated with intrusion detection and prevention systems (IDPS) capable of operating in both IT and OT environments. For example, anomaly detection algorithms can be trained to recognize deviations in vessel trajectory, system behavior, or communications, prompting immediate automated or human-initiated countermeasures. Furthermore, digital twin technology can be used to simulate cyberattacks in a risk-free environment, allowing organizations to test response strategies and improve system resilience without compromising operational continuity.

Cybersecurity mitigation also demands strong governance and organizational coordination. Establishing a cross-functional cybersecurity operations center (CSOC) that monitors threats across maritime and intermodal nodes ensures unified oversight and rapid incident response. Such a center must collaborate with port authorities, shipping companies, inland terminal operators, and national cybersecurity agencies to promote coordinated defense measures. This collaboration can be reinforced by sharing threat intelligence and adhering to a common operational language and protocols. Additionally, cybersecurity training and awareness programs must be developed for personnel at all levels, ensuring that even non-technical staff understand the importance of cyber hygiene and their role in preventing breaches. To further support implementation, governments and regulatory bodies must introduce incentive structures and enforce compliance through regular audits and certifications. Funding mechanisms for cybersecurity innovation, public-private partnerships for threat intelligence sharing, and legal frameworks for liability and data protection are essential components of a broader strategic implementation approach. The regulation must be agile enough to adapt to rapid technological change while remaining stringent enough to deter negligence and non-compliance.

Resilience engineering should be embedded into the design of autonomous systems to ensure continuity in the event of cyber disruptions. This includes redundant systems, robust failover mechanisms, and contingency planning. Cybersecurity-by-design principles must guide the development of autonomous vessels and intermodal systems from the outset, rather than being retrofitted as an afterthought. Additionally, post-incident forensics capabilities should be built into system architecture to facilitate rapid recovery and compliance with reporting obligations. The successful implementation of cybersecurity risk mitigation for autonomous systems in maritime and intermodal transport infrastructure hinges on an ecosystem-wide transformation. It requires the convergence of innovative technology, robust governance, skilled personnel, and proactive collaboration between the public and private sectors. As the lines between physical and digital domains blur, cybersecurity must be viewed not merely as a protective function but as a core enabler of trust, safety, and efficiency in the future of autonomous transport.

2.3 Case study applications

The maritime industry, traditionally reliant on manual operations, has been quick to adopt automation in navigational systems, cargo handling, and port operations. Autonomous vessels and smart ports use GPS, sensor networks, communication systems, and

control algorithms to perform complex tasks with minimal human intervention. Similarly, intermodal transport, which involves the seamless integration of multiple transport modes such as rail, truck, and sea, now depends heavily on automated scheduling, tracking, and coordination systems. As these systems become more digitized, the threat landscape expands to include cyberattacks targeting vessel navigation systems, port logistics platforms, data communication links, and even industrial control systems (ICS) managing cranes and freight terminals. A prominent example of cybersecurity risk mitigation in this context is the use of AI-powered threat detection and response platforms deployed across port infrastructures. For instance, the Port of Los Angeles, one of the busiest in the United States, has partnered with private cybersecurity firms to develop a Cyber Resilience Center (CRC). This platform acts as a centralized hub for real-time monitoring, incident reporting, and collaborative defense against cyber threats. By aggregating data from different stakeholders — including shipping lines, terminal operators, and trucking companies — the CRC uses machine learning algorithms to detect anomalies and potential intrusions, allowing for a proactive defense strategy. Such collaboration and intelligence sharing are crucial to mitigating systemic risks in highly interdependent environments.

Autonomous vessels are particularly vulnerable to GPS spoofing, electronic jamming, and onboard system intrusions. In 2017, a cybersecurity researcher demonstrated how a GPS spoofing device could mislead an autonomous yacht, diverting its path without alerting onboard systems. Since then, several cybersecurity solutions have emerged to harden autonomous navigation systems. These include multi-layered authentication protocols, blockchain-based data integrity checks, and hybrid navigation systems that cross-verify positional data using inertial measurement units (IMUs), radar, and optical sensors. By using redundant data sources and cryptographic verification, autonomous vessels can now better validate their position and mission-critical data, significantly reducing the risk of undetected cyber manipulation. Cybersecurity for intermodal transport hubs also involves securing IoT devices and sensor networks, which are integral to real-time logistics coordination. Smart terminals use automated gantry cranes, RFID-based cargo tracking, and edge computing devices to manage freight flows. These endpoints, if left unsecured, present easy targets for attackers seeking to disrupt operations or exfiltrate sensitive logistics data. To address this, modern cybersecurity frameworks now emphasize zero-trust architectures, continuous authentication, and encryption of all data in motion and at rest. Furthermore, endpoint detection and response (EDR) systems are now embedded in the ICS environment to detect and isolate anomalous behaviors before they propagate through the network.

One of the most innovative cybersecurity advancements involves the application of blockchain technology to ensure data integrity and traceability across the transport ecosystem. In the maritime and intermodal context, blockchain is used to create tamper-proof records of cargo manifests, maintenance logs, and transaction histories. By decentralizing the data ledger, blockchain prevents single points of failure and ensures that any unauthorized changes to data are immediately detectable. Several pilot projects, such as the IBM-Maersk TradeLens platform, have demonstrated how distributed ledgers can enhance both operational transparency and cyber resilience. Although TradeLens was recently discontinued, it laid the groundwork for future decentralized digital logistics ecosystems. Cybersecurity risk mitigation also requires robust regulatory frameworks and industry-wide standards. The International Maritime Organization (IMO) has mandated that all shipping companies incorporate cybersecurity into their Safety Management Systems (SMS) under IMO 2021 guidelines. Similarly, organizations such as the European Union Agency for Cybersecurity (ENISA) and the U.S. Department of Homeland Security have issued guidelines and conducted risk assessments specifically tailored for maritime and intermodal systems. Compliance with these frameworks ensures a minimum baseline of cybersecurity hygiene and provides structured methodologies for risk assessment, incident response planning, and system hardening.

Despite these advances, significant challenges remain. Many legacy systems still operate in maritime and rail networks, lacking the security features required in modern digital infrastructures. Interoperability

between different platforms, varying cybersecurity maturity levels among stakeholders, and the increasing sophistication of threat actors — including state-sponsored groups — demand continuous innovation and investment in cybersecurity. Additionally, the rise of quantum computing poses future risks to current encryption standards, necessitating the development of quantum-resistant algorithms. The future of autonomous maritime and intermodal transport hinges not only on technological sophistication but also on the robustness of cybersecurity frameworks that protect them. The increasing integration of AI, IoT, and blockchain technologies provides both new attack vectors and innovative defense mechanisms. By embracing a defense-in-depth strategy, investing in cyber resilience centers, adopting decentralized data integrity solutions, and fostering international collaboration, the industry is taking vital steps to secure the backbone of global trade against evolving cyber threats. The path forward must continue to be driven by both technological advances and a shared commitment to cybersecurity as a core element of operational safety and reliability.

2.4 Discussions

The rapid evolution of autonomous systems has transformed the maritime and intermodal transport infrastructure landscape, introducing increased efficiency, safety, and operational optimization. However, this transformation comes with a heightened exposure to cybersecurity threats, making the mitigation of associated risks a pressing concern. As critical sectors become increasingly interconnected and dependent on digital technologies, the importance of securing these infrastructures cannot be overstated. Advances in cybersecurity risk mitigation are therefore central to ensuring the resilience, reliability, and integrity of autonomous systems in this domain. Autonomous maritime vessels, port operations, and intermodal transport platforms are now heavily reliant on a variety of digital components such as AI-powered navigation systems, satellite communication networks, IoT sensors, and cloud-based data exchange platforms. While these technologies significantly enhance operational capability, they simultaneously create a complex cyber-physical system that is vulnerable to sophisticated cyberattacks. Incidents such as GPS spoofing, ransomware, denial-of-service attacks, and unauthorized data access have already demonstrated their potential to disrupt operations, jeopardize safety, and result in substantial economic losses. Consequently, cybersecurity risk mitigation strategies must evolve in parallel with technological advancements.

One of the major advances in cybersecurity for these systems is the integration of Artificial Intelligence (AI) and Machine Learning (ML) for predictive threat analysis and automated threat response. These technologies enable the real-time analysis of vast data streams, identifying anomalies and patterns indicative of cyber threats before they escalate into full-scale incidents. By leveraging adaptive learning, ML algorithms can enhance detection capabilities, reduce false positives, and provide timely alerts to operators. In maritime environments, AI is being deployed in vessel traffic monitoring systems and cargo tracking platforms to detect unauthorized access attempts, route deviations, and suspicious data transmission patterns. Another critical advancement is the deployment of blockchain technology for securing data integrity and access control in intermodal transport systems. Blockchain's decentralized ledger system offers a tamper-proof environment for logging events, transactions, and system changes, making it particularly useful in multi-stakeholder environments such as global shipping and port management. This ensures transparency, enhances trust among stakeholders, and significantly reduces the potential for internal threats and data manipulation. For instance, in container tracking and documentation, blockchain allows for secure data sharing across the supply chain, from customs to logistics providers, minimizing the risk of forgery or unauthorized data access.

Additionally, the adoption of Zero Trust Architecture (ZTA) is redefining access control mechanisms across maritime and intermodal infrastructures. Unlike traditional security models that assume trust within a network perimeter, ZTA enforces strict identity verification and continuous monitoring regardless of location or device. This approach significantly limits lateral movement within systems in case of a breach, containing potential threats before they cause systemic damage. ZTA is particularly suited to autonomous operations, where remote access and distributed

computing are common. Moreover, cyber-resilience is being enhanced through simulation-based training and digital twin technologies. Digital twins, virtual replicas of physical systems, enable operators and security analysts to simulate potential attack scenarios and test mitigation strategies in a controlled environment. This proactive approach facilitates the development of robust incident response protocols, identifies system vulnerabilities, and aids in optimizing cybersecurity investments. In port operations, digital twins are increasingly used to model terminal operations and logistics flows, helping operators understand the ripple effects of cyber incidents and implement contingency planning more effectively.

Regulatory frameworks and international cooperation have also advanced as critical enablers of cybersecurity in autonomous transport. Initiatives by the International Maritime Organization (IMO) and regional entities have led to the development of cybersecurity guidelines and compliance requirements for autonomous systems. The IMO's resolution MSC.428(98), which mandates the integration of cybersecurity into the Safety Management Systems (SMS) of maritime operators, is a significant step in institutionalizing cybersecurity. Collaborative efforts such as information sharing platforms and joint cyber incident response teams are promoting a more unified defense approach, especially against transnational threats targeting critical infrastructure. However, the dynamic nature of cyber threats necessitates continuous innovation and adaptability in defense strategies. Cyber attackers are increasingly exploiting vulnerabilities in third-party software, open-source platforms, and legacy systems that are often embedded in transport infrastructure. To address this, there is a growing emphasis on secure software development practices, vulnerability disclosure programs, and robust supply chain risk management protocols. Furthermore, enhanced endpoint protection through the use of multi-factor authentication, encrypted communications, and secure firmware updates is becoming standard practice.

Human factors also remain a significant vector of cyber risk. Advances in cybersecurity awareness and training programs tailored for maritime and transport personnel are essential. These programs emphasize phishing detection, safe device usage, and incident reporting, fostering a culture of cybersecurity across all levels of operation. As automation reduces human involvement in physical tasks, it paradoxically increases the reliance on human oversight in digital domains, underscoring the need for continuous education and skill development. The cybersecurity landscape for autonomous maritime and intermodal transport infrastructure is rapidly evolving in response to growing digital integration and sophisticated threat environments. Advances in AI, blockchain, Zero Trust Architecture, digital twin technology, and regulatory frameworks are collectively strengthening the sector's ability to mitigate cyber risks. However, the success of these measures depends on sustained investment, cross-sector collaboration, and a proactive security mindset that anticipates and adapts to emerging challenges. As autonomy continues to redefine transport infrastructure, cybersecurity must remain a foundational pillar of its evolution.

CONCLUSION

The evolution of autonomous systems in maritime and intermodal transport infrastructure represents a transformative leap towards greater efficiency, safety, and operational optimization. However, this technological advancement comes with an equally significant escalation in cybersecurity vulnerabilities, which, if unaddressed, pose severe risks to operational continuity, safety, and national security. As these systems increasingly rely on interconnected networks, sensors, and AI-driven decision-making, the attack surface for malicious cyber activities expands dramatically, necessitating robust and forward-thinking cybersecurity strategies. Recent advances in cybersecurity risk mitigation underscore a multidisciplinary approach that blends technological innovation with policy development, stakeholder collaboration, and regulatory oversight. Techniques such as AI-based anomaly detection, blockchain for secure data exchange, zero-trust architecture, and digital twin technologies are being progressively integrated into transport infrastructures to fortify their defenses. These innovations not only enhance threat detection and response capabilities but also promote resilience through predictive analytics and real-time monitoring. Furthermore, cybersecurity frameworks are being redefined to accommodate the specific

operational demands of autonomous maritime and intermodal environments. Standards such as the NIST Cybersecurity Framework and the IMO's guidelines on maritime cybersecurity are being adapted and expanded to align with autonomous functionalities. Collaborative initiatives between public and private sectors, including information sharing and joint threat intelligence, are proving vital in identifying vulnerabilities and fortifying defenses across critical infrastructure. Despite these strides, challenges persist. The complexity of securing legacy systems, ensuring interoperability across diverse platforms, addressing human factors, and navigating regulatory discrepancies between jurisdictions remain significant hurdles. Moreover, the rapid pace of technological change often outstrips the development of adequate cybersecurity policies and training, leaving gaps in preparedness. The advancement of cybersecurity risk mitigation strategies is crucial to the sustainable deployment of autonomous systems in maritime and intermodal transport. A proactive, layered, and adaptive cybersecurity approach—grounded in cutting-edge technologies and supported by cohesive regulatory frameworks—is essential to protect these critical infrastructures from ever-evolving cyber threats. Continued investment in research, international collaboration, and workforce development will be pivotal in ensuring that cybersecurity evolves in lockstep with automation, thereby enabling a secure and resilient future for global transport systems.

REFERENCES

[1] Okolie, C.I., Hamza, O., Eweje, A., Collins, A., Babatunde, G.O., & Ubamadu, B.C., 2021. Leveraging Digital Transformation and Business Analysis to Improve Healthcare Provider Portal. ICONIC RESEARCH AND ENGINEERING JOURNALS, 4(10), pp.253-257.

[2] Austin-Gabriel, B., Hussain, N.Y., Ige, A.B., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Research Journal of Engineering and Technology, 1(01), pp.047-055.

[3] Hussain, N.Y., Austin-Gabriel, B., Ige, A.B., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Research Journal of Science and Technology, 2(02), pp.006-015.

[4] Ike, C.C., Ige, A.B., Oladosu, S.A., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews, 2(1), pp.074-086.

[5] Oladosu, S.A., Ike, C.C., Adepoju, P.A., Afolabi, A.I., Ige, A.B. and Amoo, O.O., 2021. The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. Magna Scientia Advanced Research and Reviews.

[6] Akinade, A.O., Adepoju, P.A., Ige, A.B., Afolabi, A.I. and Amoo, O.O., 2021. A conceptual model for network security automation: Leveraging AI-driven frameworks to enhance multi-vendor infrastructure resilience. International Journal of Science and Technology Research Archive, 1(1), pp.39-59.

[7] Oladosu, S.A., Ike, C.C., Adepoju, P.A., Afolabi, A.I., Ige, A.B. and Amoo, O.O., 2021. Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. Magna Scientia Advanced Research and Reviews.

[8] Ajayi, A. and Akerele, J.I., 2021. A high-impact data-driven decision making model for integrating cutting-edge cybersecurity strategies into public policy, governance, and organizational frameworks. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), pp.623-637.

[9] Elujide, I., Fashoto, S.G., Fashoto, B., Mbunge, E., Folorunso, S.O. and Olamijuwon, J.O., 2021. Application of deep and machine learning techniques for multi-label classification performance on psychotic disorder diseases. Informatics in Medicine Unlocked, 23, p.100545.

[10] Olamijuwon, O.J., 2020. Real-time Vision-based Driver Alertness Monitoring using Deep Neural

Network Architectures (Master's thesis, University of the Witwatersrand, Johannesburg (South Africa)).

[11] Ogungbenle, H.N. and Omowole, B.M., 2012. Chemical, functional and amino acid composition of periwinkle (Tympanotonus fuscatus var radula) meat. Int J Pharm Sci Rev Res, 13(2), pp.128-132.

[12] Elumilade, O.O., Ogundeji, I.A., Achumie, G.O., Omokhoa, H.E. and Omowole, B.M., 2021. Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. Journal of Advanced Education and Sciences, 1(2), pp.55-63.

[13] Otokiti, B.O., Igwe, A.N., Ewim, C.P.M. and Ibeh, A.I., 2021. Developing a framework for leveraging social media as a strategic tool for growth in Nigerian women entrepreneurs. Int J Multidiscip Res Growth Eval, 2(1), pp.597-607.

[14] Egbuhuzor, N.S., Ajayi, A.J., Akhigbe, E.E., Agbede, O.O., Ewim, C.P.M. and Ajiga, D.I., 2021. Cloud-based CRM systems: Revolutionizing customer engagement in the financial sector with artificial intelligence. International Journal of Science and Research Archive, 3(1), pp.215-234.

[15] Ewim, C.P.M., Omokhoa, H.E., Ogundeji, I.A. and Ibeh, A.I., 2021. Future of Work in Banking: Adapting Workforce Skills to Digital Transformation Challenges. Future, 2(1).

[16] Hassan, Y.G., Collins, A., Babatunde, G.O., Alabi, A.A. and Mustapha, S.D., 2021. AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. Artificial intelligence (AI), p.16.

[17] Okolie, C.I., Hamza, O., Eweje, A., Collins, A. and Babatunde, G.O., Leveraging digital transformation and business analysis to improve healthcare provider portal. IRE Journals. 2021; 4 (10): 253-254

[18] Oyegbade, I.K., Igwe, A.N., Ofodile, O.C. and Azubuike, C., 2021. Innovative financial planning and governance models for emerging markets: Insights from startups and banking audits. Open Access Research Journal of Multidisciplinary Studies, 1(2), pp.108-16.

[19] Oyeniyi, L.D., Igwe, A.N., Ofodile, O.C. and Paul-Mikki, C., 2021. Optimizing risk management frameworks in banking: Strategies to enhance compliance and profitability amid regulatory challenges. Journal Name Missing.

[20] Paul, P.O., Abbey, A.B.N., Onukwulu, E.C., Agho, M.O. and Louis, N., 2021. Integrating procurement strategies for infectious disease control: Best practices from global programs. prevention, 7, p.9.

[21] Conz, E., Denicolai, S., & Zucchella, A. (2017). The resilience strategies of SMEs in mature clusters. Journal of Enterprising Communities: People and Places in the Global Economy, 11(1), 186-210.

[22] Meyer, E. L., Apeh, O. O., & Overen, O. K. (2020). Electrical and meteorological data acquisition system of a commercial and domestic microgrid for monitoring pv parameters. Applied Sciences, 10(24), 9092.

[23] Apeh, O. O., Meyer, E. L., & Overen, O. K. (2021). Modeling and experimental analysis of battery charge controllers for comparing three off-grid photovoltaic power plants. Heliyon, 7(11).

[24] Nwaozomudoh, M.O., Odio, P.E., Kokogho, E., Olorunfemi, T.A., Adeniji, I.E. and Sobowale, A., 2021. Developing a conceptual framework for enhancing interbank currency operation accuracy in Nigeria's banking sector. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), pp.481-494.

[25] Faith, D. O. (2018). A review of the effect of pricing strategies on the purchase of consumer goods. International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol, 2.

[26] Casalino, N., Żuchowski, I., Labrinos, N., Munoz Nieto, Á. L., & Martín, J. A. (2019). Digital strategies and organizational performances of SMEs in the age of Coronavirus: balancing digital transformation with an effective business resilience. Queen Mary School of Law Legal Studies Research Paper Forthcoming.

[27] Lusimbo, E. N. (2016). Relationship between financial literacy and the growth of micro and small enterprises in Kenya: A case of Kakamega Central sub-county (Doctoral dissertation, cohred, JKUAT).

[28] Lund, S., DC, W., & Manyika, J. (2020). Risk, resilience, and rebalancing in global value chains.

[29] Zekos, G. I., & Zekos, G. I. (2021). Risk management developments. Economics and Law of Artificial Intelligence: Finance, Economic Impacts, Risk Management and Governance, 147-232.

[30] Alberti, F. G., Ferrario, S., & Pizzurno, E. (2018). Resilience: resources and strategies of SMEs in a new theoretical framework. International journal of learning and intellectual capital, 15(2), 165-188.

[31] Guo, H., Yang, Z., Huang, R., & Guo, A. (2020). The digitalization and public crisis responses of small and medium enterprises: Implications from a COVID-19 survey. Frontiers of Business Research in China, 14, 1-25.

[32] Otokiti, B. O., Igwe, A. N., Ewim, C. P.-M., & Ibeh, A. I. (2021). Developing a framework for leveraging social media as a strategic tool for growth in Nigerian women entrepreneurs. International Journal of Multidisciplinary Research and Growth Evaluation, 1(1), 597-607.

[33] Južnik Rotar, L., Kontošić Pamić, R., & Bojnec, Š. (2019). Contributions of small and medium enterprises to employment in the European Union countries. Economic research-Ekonomska istraživanja, 32(1), 3296-3308

[34] Iborra, M., Safón, V., & Dolz, C. (2020). What explains the resilience of SMEs? Ambidexterity capability and strategic consistency. Long Range Planning, 53(6), 101947

[35] Apeh, O. O., Overen, O. K., & Meyer, E. L. (2021). Monthly, seasonal and yearly assessments of global solar radiation, clearness index and diffuse fractions in alice, South Africa. Sustainability, 13(4), 2135.

[36] Apeh, O.O., Chime, U.K., Agbo, S., Ezugwu, S., Taziwa, R., Meyer, E., Sutta, P., Maaza, M. and Ezema, F.I., (2019). Properties of nanostructured ZnO thin films synthesized using a modified aqueous chemical growth method. Materials Research Express, 6(5), p.056406.

[37] Agho, G., Ezeh, M.O., Isong, M., Iwe, D. and Oluseyi, K.A., Sustainable pore pressure prediction and its impact on geo-mechanical modelling for enhanced drilling operations. World J Adv Res Rev. 2021; 12 (1): 540–57

[38] Shaheen, R., Ağa, M., Rjoub, H., & Abualrub, A. (2020). Investigation of the pillars of sustainability risk management as an extension of enterprise risk management on palestinian insurance firms' profitability. Sustainability, 12(11), 4709

[39] Ferreira, J., & Coelho, A. (2020). Dynamic capabilities, innovation and branding capabilities and their impact on competitive advantage and SME's performance in Portugal: the moderating effects of entrepreneurial orientation. International Journal of Innovation Science, 12(3), 255-286.

[40] Adewale, T. T., Olorunyomi, T. D., & Odonkor, T. N. 2021. AI-powered financial forensic systems: A conceptual framework for fraud detection and prevention. Magna Sci Adv Res Rev, 2(2), 119-36.

[41] Adewale, T. T., Olorunyomi, T. D., & Odonkor, T. N. 2021. Advancing sustainability accounting: A unified model for ESG integration and auditing. Int J Sci Res Arch, 2(1), 169-85.

[42] Oyedokun, O. O. 2019. Green human resource management practices and its effect on the sustainable competitive edge in the Nigerian manufacturing industry (Dangote) (Doctoral dissertation, Dublin Business School).

[43] Boschmans, K., & Pissareva, L. (2018). Fostering markets for SME finance: Matching business and investor needs.

[44] Neumeyer, X., Santos, S. C., & Morris, M. H. (2020). Overcoming barriers to technology adoption when fostering entrepreneurship among the poor: The role of technology and digital literacy. IEEE Transactions on Engineering Management, 68(6), 1605-1618.

[45] Radicic, D., Pugh, G., & Douglas, D. (2020). Promoting cooperation in innovation ecosystems: evidence from European traditional

manufacturing SMEs. Small Business Economics, 54(1), 257-283.

[46] Oduro, B., Akpabot, S., Akakpo, A., & Gyasi, E. A. (2018). Pledge towards workforce diversity and organisational wellbeing: A case study of Aviva Plc. In Futures Thinking and Organizational Policy: Case Studies for Managing Rapid Change in Technology, Globalization and Workforce Diversity (pp. 287-303). Cham: Springer International Publishing.

[47] Fatoki, O. (2018). The impact of entrepreneurial resilience on the success of small and medium enterprises in South Africa. Sustainability, 10(7), 2527

[48] Chan, Calvin ML, et al. "Agility in responding to disruptive digital innovation: Case study of an SME." Information Systems Journal 29.2 (2019): 436-455

[49] Okolie, C.I., Hamza, O., Eweje, A., Collins, A., Babatunde, G.O., & Ubamadu, B.C., 2021. Leveraging Digital Transformation and Business Analysis to Improve Healthcare Provider Portal. ICONIC RESEARCH AND ENGINEERING JOURNALS, 4(10), pp.253-257.

[50] Okolie, C.I., Hamza, O., Eweje, A., Collins, A. and Babatunde, G.O., 2021. Leveraging Digital Transformation and Business Analysis to Improve Healthcare Provider Portal. IRE Journals, 4 (10), 253-254