Data-Driven Requirements Verification in a Tool to Support the Cybersecurity Risk Management Process in Maritime Transportation Ecosystem

Mark McKenzie
Colorado Technical University,
Colorado Springs, CO, USA
mark.mckenzie23@student.ctuonline.edu

Yanzhen Qu
Colorado Technical University,
Colorado Springs, CO, USA
yqu@coloradotech.edu

Abstract— **Commercial maritime transportation is a critical infrastructure for countries and the global economy. Currently, the industry transports 80-90% of all international trade. However, the industry has traditionally focused on physical security and lacks a web-based distributed system for efficient cybersecurity risk management. This is challenging due to the diverse range of companies and organizations involved, each with different cybersecurity expertise and technologies and no common ownership. We have proposed a solution of developing a web-based distributed system called MTcyber RMPDS, to support the cybersecurity risk management processes in maritime transportation ecosystem. This paper explores the quantitative verification of the requirements represented by the use cases of various service requests sent to MTcyber RMPDS, aiming to improve its design efficiency.**

Keywords— **cybersecurity, cyber-risk, cybersecurity risk management process, design science research, transport**

I. Introduction

Critical infrastructure describes essential assets required for a nation's economic and social well-being, without which they find it challenging to achieve sustenance [1], [3]. Of the sixteen critical infrastructures identified in the United States, maritime transportation is known to have a significant impact on local and international trade. The United States shipping industry contributes to an industry in which 90% of global products and 75% of global trades are transported via shipping routes[4]. In addition, maritime trade global value is projected to double in value to USD 3 trillion by 2030 [5].

The United States maritime transportation employs nearly 700 000 people and contributes an annual economic output of USD 150 billion [6]. Within this ecosystem are multiple stakeholders comprising maritime terminals, port authorities, ports, port authorities, shipping lines, administrative staff, the Department of Homeland Security, United States Customs, and customs brokers.

Though late in innovation uptake compared to other industries, the maritime industry is experiencing digitalization [2], [7]. The maritime sector's increased reliance on technology, the Internet, and information sharing has led to more frequent and significant risks [8].

To address the increasing security threats in the maritime sector, the United States government and maritime stakeholders have implemented various mitigation tools such as cybersecurity risk management processes [9], investment in technologies [10], and training of stakeholders to increase awareness through Executive Orders [11]. The maritime sector, with different stakeholders, has various technologies, strategies, policies, and skill levels to address cybersecurity risk management. However, the result is the lack of a common tool within maritime transportation to support cybersecurity risk management processes.

The researchers have designed a web-based distributed system known as Maritime Transportation Cybersecurity Risk Management Process Distributed System (MTcyber RMPDS) to support risk assessment in the shipping sector. In designing MTcyber RMPDS, it was necessary to understand its effectiveness in processing maritime use case service requests to identify and prioritize risks. These unique use cases were then quantitatively verified to investigate the correlations between the system failure ratio and failure reasons, the correlation between failure reasons, and which components of MTcyber RMPDS is necessary to support most use cases. The answers to the research questions will inform the design of MTcyber RMPDS to ensure efficiency. This paper, therefore, examines the use of a data-driven approach to design a system using quantitative statistics.

This paper is structured as follows. Section II outlines the related work. Section III outlines the problem statement and hypotheses. Section IV discusses the methodological approach. Section V presents the results and analysis. Section VI is conclusion.

II. Related Work

A. The Maritime Cyber Risk Analysis Model - MaCRA

Researchers in the past have used various methods to address cybersecurity risk assessment in maritime shipping. Two ways include mathematical or formal models and manual analysis [12]. Other researchers have also proposed more

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00420

specific strategies, for example, the Maritime Cyber Risk Analysis Model MaCRA [13]. The MaCRA model maps effects, systems, and technologies to enable systems and risk rankings. This model, however, explicitly addresses risks associated with autonomous vessels, representing future trends in maritime shipping with minimal human interaction.

The MaCRA model depicts an attacker's objective, attack path, and engagement tools. Further, the model comprises three axes or criteria for assessing threats. Axis$_s$ addresses technology systems and corresponding impacts. Axis$_b$ investigates an attacker's ease of exploit, and Axis$_r$ examines the benefits of targeting autonomous vessels. Hence, the three axes represent an association of attacker and target characteristics [14]. However, the MaCRA model for maritime cybersecurity risk assessment can become complex and ineffective when ultimately operationalized [12].

B. The MITIGATE Model

Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs (MITIGATE) represents a model targeting supply chain risk assessment [15]. Specifically, MITIGATE's objective is to leverage the intelligence of port authorities and risk officers within maritime transportation. The model analyzes the impact of the risk spectrum on all areas of the supply chain within the maritime ecosystem. In addition, the MITIGATE model enables real-time updates of cyber risk status with an enterprise and among business interests. The model uses a qualitative methodology for risk assessment.

MITIGATE consists of reproduction models that efficiently generate high-quality artifacts, data, and indicators [16]. Risk assessment using the MITIGATE model comprises components that include Boundary Setting, where the capacity and objective of the supply chain risk assessment are assessed. The Vulnerability Analysis component investigates single and combined weaknesses within the supply chain. Risk Estimation within the MITIGATE framework explores the potential attacks that impact the function of stand-alone assets or their effect on devices. Finally, the Mitigation Strategy produces a mitigation strategy to prevent asset downtime or inefficiencies.

III. Problem Statement, Hypothesis, and Research Question

A. Problem Statement

The maritime industry has no common system to support the cybersecurity risk management process to identify and prioritize threats. A common system is absent due to multiple stakeholders with various technologies, procedures, policies, and cybersecurity competencies.

B. Research Question

RQ1: How is the failure ratio related to the different failure reasons of MTcyber RMPDS service requests to process use cases?

RQ2: How is the component that supports the most significant number of use cases related to MTcyber RMPDS efficiency?

C. Hypotheses

H1: There is a correlation between the failure ratio and the failure reasons of MTcyber RMPDS service request to process use cases.

H2: There is a relation between the component that supports the most significant number of use cases and MTcyber RMPDS efficiency.

IV. Methodology

This section presents an overview of MTcyber RMPDS functionality across various stakeholders' applications and the options for handling use case service requests. The study identifies unique use cases to generate the research sample size. It then identifies possible failure reasons and calculates the failure ratio of MTcyber RMPDS to conduct a quantitative analysis that verifies the use case and answers the research questions.

A. MTcyber RMPDS Functionality

MTcyber RMPDS is a web-based distributed feature that enables its functionality across multiple stakeholders' applications, Figure 1. As a middleware, the system is scalable and enables more users to execute cybersecurity risk management processes without bottlenecks. MTcyber RMPDS effectiveness is determined by factors that represent the risk scenarios in maritime shipping, use case verification, service request acceptance and rejection, and data analytics.

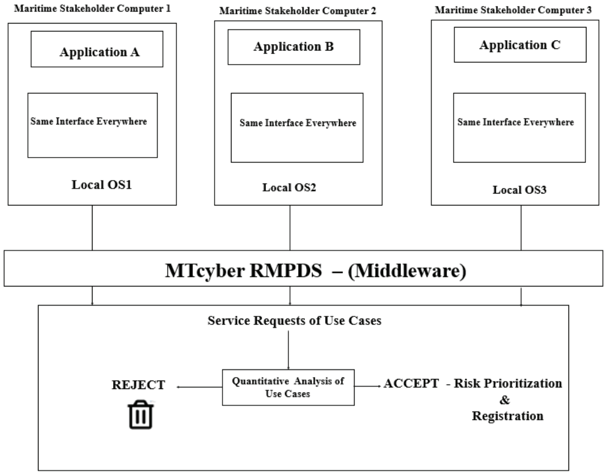

Maritime Stakeholder Computer 1
Maritime Stakeholder Computer 2
Maritime Stakeholder Computer 3
Application A
Application B
Application C
Same Interface Everywhere
Same Interface Everywhere
Same Interface Everywhere
Local OS1
Local OS2
Local OS3
MTcyber RMPDS – (Middleware)
Service Requests of Use Cases
REJECT
Quantitative Analysis of Use Cases
ACCEPT - Risk Prioritization & Registration

FIGURE 1. OVERVIEW OF THE CONCEPTUAL FRAMEWORK OF MTCYBER RMPDS

B. Use Case Identification

The result of cyber-attacks on various United States maritime critical infrastructure suggests that targeted mitigation strategies are best suited to reduce the impact on human, infrastructure, and procedural dislocations [17]. This study identified three risk types within the maritime transportation sector from which the researchers have proposed that unique use cases can be generated: ship grounding [18], maritime piracy [19], and maritime supply chain [20].

TABLE I.
USE CASES IN MARITIME TRANSPORTATION

UC	Use Case Type
1.01	Cybersecurity Fatigue
1.02	Physical Access Breach
1.03	File and System Breach
1.04	Weak Password
1.05	Unsecured Wi-Fi
1.06	Social Engineering
1.07	Data mishandling
1.08	Insider Threats
1.09	Automatic Identification System (AIS) Breach
1.10	Video Surveillance System (VSS) Breach
1.11	Electronic Chart Display Information System (ECDIS) Breach
1.12	Global Position System (GPS) and Global Navigation Satellite System (GNSS) Breach
1.13	Radar Breach
1.14	Global Industrial Control System (GICS) Breach
1.15	Global Maritime Distress System (GMDSS) Breach
1.16	Propulsion and Machinery and Power Control Systems **(**PMPCS) Breach
1.17	Track Control System (TCS) Breach
1.18	Procedural/ Document Breaches
2.01	Pirate Physical Attack Breach
2.02	Illegal Boarding Breach
2.03	Hijack - Full Control of Vessel
2.04	Main Engine Control System (MECS) Breach
2.05	Cargo Handling and Control Systems (CHCS) Breach
2.06	Automated Manifest System (AMS) Breach
2.07	Ship Security Reporting System (SSRS) Breach
2.08	Long Range Identification and Tracking (LRIT) System Breach
2.09	Vessel Public Internet Networks Breach
2.1	Alteration of Suspicious Activity Checklists Breach
3.01	Container Yard Management Software (CYMS) Breach
3.02	Cargo Billing and Demurrage System (CBDS) Breach
3.03	Gate Management System (GMS) Breach
3.04	Closed Circuit Television (CCTV) Breach

Examples of in the human, infrastructure, and procedure risk domains of maritime transportation include cybersecurity fatigue breaches [21], physical access breaches [22], file and system breaches [23], weak password breaches [24], u1nsecured Wi-Fi breach [25], social engineering breach [26], data mishandling breach [27], and insider breach [28].

The infrastructure use cases include breaches in automatic identification systems [29], video surveillance systems [30], electronic chart display information systems [31], radar [32], and global maritime distress systems [33]. Procedural and document breaches due to alteration, theft, deletion, or steganography have also been identified by researchers [34]. Table I outlines the 32 use cases used in sample generation2.

To develop MTcyber RMPDS, researchers identified countermeasures to mitigate various cyberattacks. These countermeasures were considered components supporting the service requests of use cases. Eight components were agreed upon: access control, access log, graphic storage, habituation reduction for document storage and human resource activities, malware detection, multifactor authentication, password complexity check, and staff scheduling.

Based on mitigation considerations, access control supported 26 of the 32 use cases, access log 3, graphic storage 9, habituation reductions 1, malware detection 1, multifactor authentication 14, password complexity check 1, and staff scheduling 1. Researchers assumed that components supporting multiple use cases would be busier than those supporting a single use case. Single-use cases were more likely to have a higher success rate of being processed by MTcyber RMPDS compared to multiple use cases accessing a component, Table II.

TABLE II.
SYSTEM FUNCTIONS TO SUPPORT USE CASES

System Functions (cid)	Use case Ids	Total Use case
Access Control (C1)	1.03, 1.04, 1.05, 1.07, 1.08, 1.09, .110, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 2.03, 2.04, 2.05, 2.06, 2.07, 2.08, 2.10, 3.01, 3.02, 3.03, 3.04	26
Access Log (C2)	1.02, 1.05, 2.01	3
Graphic Storage (C3)	1.02, 1.12, 1.16, 2.01, 2.02 2.03, 2.04, 2.05, 3.04	9
Habituation Reduction (C4)	1.01	1
Malware Detection (C5)	1.06	1
Multi-Factor Authentication (c6)	1.03, 1.04, 1.07, 1.11, 1.14, 1.16, 1.17, 1.18, 2.04, 2.05, 2.06, 2.07, 2.09, 3.01	14
Password Complexity check (c7)	1.04	1
Staff scheduling (C8)	1.01	1

C. Population and Sample Size Determination

There are over 3,500 maritime terminals in the United States [35]. The researchers assumed that the population is an unlimited number of cybersecurity risks over many years. The sample size was obtained by determining the availability or success rate of the eight components within MTcyber RMPDS to support use cases identified from 32 unique maritime shipping security breach scenarios, Table III. A Confidence Level of 95% [36] and an Error Rate of 3-5% [37] were used to generate the sample size among the 32 use cases. A sample size calculator and (1)a were used to generate the sample size of use cases:

S= Z2 x P x (1-P)/M2 (1)

where:
M is the margin of error.
p is the estimated value of the proportion or success rate.
z is the standard score or number of standard deviations where a data point falls above or below the mean. This research used a Confidence Interval of 99% that corresponded to a Z score of 2.576.

V. Experiments Results Analysis

In this section, we will calculate the failure ratio among the use cases processed by MTcyer RMPDS due to the failure reasons identified. This calculation will enable the derivation of the number and percentage of failure and success instances among these used cases helpful in the quantitative statistics.

TABLE III
Sample Size and Availability Rate

Use Case ID	Total Number of Use Case Instances Using Sample Calculator	Availability Rate (Success Rate) (S_use-case-id)
1.01	428	93.84%
1.02	1680	65.13%
1.03	698	10.55%
1.04	679	10.22%
1.05	1044	16.99%
1.06	225	96.87%
1.07	698	10.55%
1.08	1127	18.75%
1.09	1127	18.75%
1.10	1127	18.75%
1.11	698	10.55%
1.12	863	13.48%
1.13	1127	18.75%
1.14	698	10.55%
1.15	1127	18.75%
1.16	519	7.58%
1.17	698	10.55%
1.18	698	10.55%
2.01	1680	65.13%
2.02	1496	71.87%
2.03	863	13.48%
2.04	519	7.58%
2.05	519	7.58%
2.06	698	10.55%
2.07	698	10.55%
2.08	1127	18.75%
2.09	1821	56.25%
2.10	1127	18.75%
3.01	698	10.55%
3.02	1127	18.75%
3.03	1127	18.75%
3.04	863	13.48%

Confirming or rejecting the hypotheses was essential for designing an effective MTcyber RMPDS to handle service requests in maritime shipping. This was achieved by investigating the failure ratio of use cases against various failure reasons likely to impact MTcyber RMPDS functionality.

The researchers identified failure reasons such as virus attacks, network failures, lack of system updates, pirate physical control, weather conditions, and physical sabotage. They assumed that when a use case had multiple failure reasons, the total failure was equally distributed for ease of calculation.

A. Calculation of Failure Ratio Among Use Cases

Researchers assumed that system functions accessed by multiple use cases had lower availability than a single use case accessing a system component. Table IV shows data for MTcyber RMPDS Systems Components (cid), Use Case IDs, Total Use Cases, and the percentage of busy System Component (R_cid).

TABLE IV
Percentage of system Components Busy

System Components	Use Cases IDs	Total Use Case	% of the System Component Busy (R_cid)
Access Control (C1)	1.03,1.04, 1.05, 1.07, 1.08, 1.09, 1.10, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 2.03, 2.04, 2.05, 2.06, 2.07, 2.08, 2.10, 3.01, 3.02, 3.03, 3.04	26	81.25%
Access Log (C2)	1.02, 1.05, 2.01	3	9.38%
Graphic Storage (C3)	1.02, 1.12, 1.16, 2.01, 2.02, 2.03, 2.04, 2.05, 3.04	9	28.13%
Habituation Reduction (C4)	1.01	1	3.13%
Malware Detection (C5)	1.06	1	3.13%
Multi-Factor Authentication (C6)	1.03, 1.04, 1.07, 1.11, 1.14, 1.16, 1.17, 1.18, 2.04, 2.05, 2.06, 2.07, 2.09, 3.01	14	43.75%
Password Complexity Check (C7)	1.04	1	3.13%
Staff Scheduling (C8)	1.01	1	3.13%

The Percentage of System Component Busy (R_cid) was derived from (2):

Percentage of System Component Busy (R_cid) = Number of Use Cases/Total independent Use Case x 100. (2)

For the access control (C1) component, 26 use cases were identified from 32 independent use cases, resulting in a System Component Busy (R_cid) of 81.25%, Table IV.

To derive the Success or Availability Rate of each use case instance shown in Table 3, the researchers assumed Availability rate = Success rate. We also assumed that the Success Rate of each instance was equal to the rate when all active system components were available. R_cid was denoted as the Usage Rate of the system component with cid, where cid was equal to C1, C2, C3, C4, C5, C6, C7, and C8.

While eight system components were used for this research, it was understood that a typical system would have many functionalities. The rate of the ith system component available was equal to (1-R_cid). If a use case instance involved n system components, then the rate of all involved system components being available was equal to (3).

(1-R_c1)x(1-R_c2) x … x (1 – R_cn) (3)

where n is an integer <= 8.

TABLE V
PERCENTAGE AND NUMBER OF INVOKED INSTANCES

UC ID	Percentage of Instances Invoked	Number of Instances Invoked
1.01	6.25%	1852
1.02	6.25%	1852
1.03	6.25%	1852
1.04	9.38%	2779
1.05	6.25%	1852
1.06	3.13%	927
1.07	6.25%	1852
1.08	3.13%	927
1.09	3.13%	927
1.10	3.13%	927
1.11	6.25%	1852
1.12	6.25%	1852
1.13	3.13%	927
1.14	6.25%	1852
1.15	3.13%	927
1.16	9.38%	2779
1.17	6.25%	1852
1.18	6.25%	1852
2.01	6.25%	1852
2.02	3.13%	927
2.03	6.25%	1852
2.04	9.38%	2779
2.05	9.38%	2779
2.06	6.25%	1852
2.07	6.25%	1852
2.08	3.13%	927
2.09	3.13%	927
2.10	3.13%	927
3.01	6.25%	1852
3.02	3.13%	927
3.03	3.13%	927
3.04	6.25%	1852

If S_use-case-id represents the Success Rate for a specific Use Case ID, the formula to calculate the Success Rate for each use case type is (3):

S_use-case-id = (1-R_c1) x (1-R_c2) x … x (1-R_cn) (3)

where n is an integer <= 8.

As illustrated by Use Case 1.01, which involves the C4 and C8 components where R_c4 =3.13% and R_c8 = 3.13%., this results in a Success or Availability Rate of 93.84 %, represented by (3):

S_1.01 = (1- R_c4)x(1-R_c8) = (1-0.0313) x (1-0.0313) = 0.9687 x 0.9687 =0.9384 = 93.84%

B. *Percentage of Invoked Instances and Number of Instances Invoked*

The researchers applied the following equation to determine the percentage of invoked instances (4):

Percentage of Invoked Instance = Number of Instances of Use Case/Total Use Cases *100 (4)

This percentage was crucial for generating data for the number of instances invoked for each use case based on a sample size total of 29,624. Table 5 shows data for the percentages of instances invoked and the number of instances invoked for each use case.

TABLE VI
COMPONENT ID AGAINST FAILURE REASON

Component Description	FR1	FR2	FR3	FR4	FR5	FR6	FR %
Access Control (C1)	5777	5762	5760	1288	661	1290	50.22
Access Log (C2)	348	348	348	118	348	118	3.98
Graphic Storage (C3)	1301	1322	1300	732	506	833	14.66
Habituation Reduction (C4)	0	0	0	0	57	0	0.14
Malware Detection (5)	251	251	251	0	0	0	1.84
Multi-Factor Authentication (C6)	3430	3428	3428	307	142	307	27.00
Password Complexity Check (C7)	277	277	277	0	0	0	2.03
Staff Scheduling (C8)	0	0	0	0	57	0	0.14

C. *Number of Failure and Success Instanes*

The researchers generated data for the number of success and failure instances, as illustrated in Table 6, by applying the following formulae (5, 6):

Number of Success Instances
= Number of Instances Invoked * Availability (5)

Number of Failure Instances
= Number of Instances Invokes - Number of Success Instances (6)

D. *Experiment 1*

The authors' goal in experiment 1 was to answer the first research question and the first hypothesis, which both are about the correlation between the failure ratio and failure reasons of MTcyber RMPDS service requests to process use cases. The research also investigated the relationship between failure reasons and their impact on MTcyber RMPDS. s

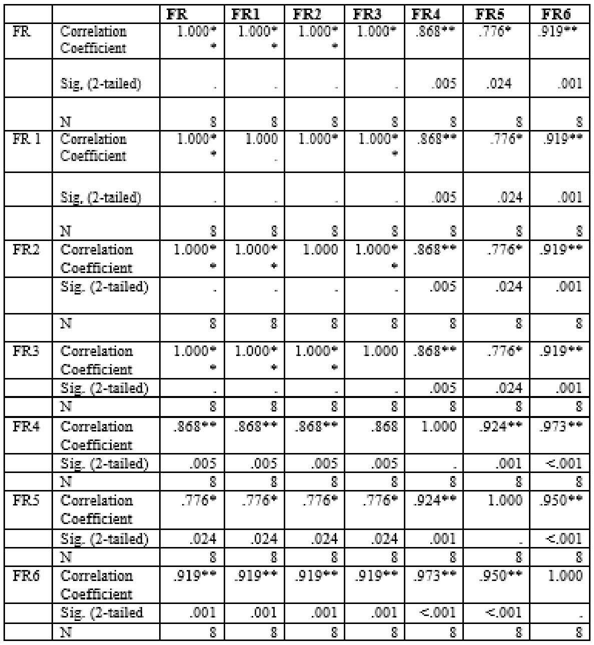
Table VI was used to determine the failure reason and failure ratios for each system component. To investigate the correlation between the failure ratio and failure reasons of MTcyber RMPDS service requests to process use cases, data for Failure Reasons 1-6 and corresponding Failure Ratios were uploaded into IBM SPSS to perform a linear correlation study. The results are shown in Table VII.

Based on Table VII:

(a) The p1=0.005, which is less than 0.01; r = 0.868. This suggests that the Failure Ratio is significantly correlated with Failure Reason 4.

(b) The p2 = 0.024, which is less than 0.01; r = 0.776. This suggests that Failure Ratio is significantly correlated with Failure Reason 5.

TABLE VII
FAILURE RATIO VERSUS FAILURE REASONS



		FR	FR1	FR2	FR3	FR4	FR5	FR6
FR	Correlation Coefficient	1.000**	1.000**	1.000**	1.000*	.868**	.776*	.919**
	Sig, (2-tailed)	.	.	.	.	.005	.024	.001
	N	8	8	8	8	8	8	8
FR 1	Correlation Coefficient	1.000**	1.000.	1.000*	1.000**	.868**	.776*	.919**
	Sig, (2-tailed)	.	.	.	.	.005	.024	.001
	N	8	8	8	8	8	8	8
FR2	Correlation Coefficient	1.000**	1.000**	1.000	1.000**	.868**	.776*	.919**
	Sig. (2-tailed)	.	.	.	.	.005	.024	.001
	N	8	8	8	8	8	8	8
FR3	Correlation Coefficient	1.000**	1.000**	1.000**	1.000	.868**	.776*	.919**
	Sig. (2-tailed)	.	.	.	.	.005	.024	.001
	N	8	8	8	8	8	8	8
FR4	Correlation Coefficient	.868**	.868**	.868**	.868	1.000	.924**	.973**
	Sig. (2-tailed)	.005	.005	.005	.005	.	.001	<.001
	N	8	8	8	8	8	8	8
FR5	Correlation Coefficient	.776*	.776*	.776*	.776*	.924**	1.000	.950**
	Sig. (2-tailed)	.024	.024	.024	.024	.001	.	<.001
	N	8	8	8	8	8	8	8
FR6	Correlation Coefficient	.919**	.919**	.919**	.919**	.973**	.950**	1.000
	Sig. (2-tailed	.001	.001	.001	.001	<.001	<.001	.
	N	8	8	8	8	8	8	8

** Correlation is significant at the .01 level (2-tailed)

(c) The p3 = 0.001, which is less than 0.01; r = 0.919. This suggests that Failure Ratio is significantly correlated with Failure Reason 6.

(d) The p4 = 0.005, which is less than 0.01; r = 0.868. This implies that Failure Reason 1 is significantly correlated with Failure Reason 4.

(e) The p5 = 0.024, which is less than 0.01; r = 0.776. This implies that Reason 1 is significantly correlated with Failure Reason 5.

(f) The p6 = .001, which is less than 0.01; r = 0.919. This implies that Reason Failure 1 is significantly correlated with Failure Reason 6.

(g) For p7 = .005, which is less than 0.01; r = 0.868, This implies that Failure Reason 4 is significantly correlated with the Failure Ratio. The same significant correlation occurs with Failure Reasons 1, 2, and 3.

(h) For p8 = 0.024, which is less than 0.01; r = 0.776. This implies that Failure Reason 5 is significantly correlated with the Failure Ratio. The same significant correlation occurs with Failure Reason 1, 2 , 3, and 4.

(i) For p9 = 0.001, which is less than 0.01; r = 0.919.

This implies that Failure Reason 6 is significantly correlated with the Failure Ration. The same significant correlation occurs with Failure Reasons 1, 2, 3, 4, and 5.

Based on (a), (b), (c), (d), (e), (g), (h), and (i) the first hypothesis has be confirmed.

E. *Experiment 2*

Experiment 2 objective was to answer the 2nd research question and the 2nd hypothesis which both are about how is the component that supports the most significant number of use cases related to MTcyber RMPDS efficiency.

Table IV shows that the access control functionality is crucial for MTcyber RMPDS functionality because it supports 26 of 32 (81.25%) use cases. Additionally, the access control component has the highest number of total failures and failure ratio across the six failure reasons, as seen in Table 8. This result indicates that the access control component is critical for MTcyber RMPDS efficiency. That is the 2nd hypothesis has been confirmed.

F. *Summary of Experiments*

Based on the correlation statistics, it was observed that there was a significant relationship between the failure ratio and failure reason. Also, failure reasons 4, 5, and 6 were correlated to failure reasons 1, 2, and 3. This suggests that failure reason could likely impact each other and determine the efficiency of use case service request. For experiment 2, it was observed that the access control component supported most use cases. This was followed by multifactor authentication which supported 14 use cases.

VI. CONCLUSION

In this paper, we have presented a data-driven approach to quantitively verify the requirements represented by the use cases of various service requests sent to the MTcyber RMPDS, which is a web-based distributed system to support the cybersecurity risk management processes in maritime transportation ecosystem, aiming to improve its design efficiency. Understanding failure reasons helps avoid design strategies that could impact system functionalities. This study is limited because it quantitatively verifies 32 use cases. In addition, typical systems consider a more significant number of components than the eight examined in this research. Future work should examine additional use case types, components, and other software development life cycle phases. In addition, user input should include all levels of the maritime ecosystem to test and provide feed on the effectiveness of MTcyber RMPDS.

REFERENCES

[1] Brew, L.. Drazovich, L. & S. Wetzel, S. "The Impact of COVID-19 on the Security and Resilience of the Maritime Transportation System," *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 510-517, https://doi: 10.1109/CSR51186.2021.

[2] Tam, K. & Jones, K. (2018). Maritime cybersecurity policy: the scope and impact of evolving tehnoogy on international shipping. Journal of Cyber Policy, 3(2), 1-18.https://www.tandofonline.com/doi/abs/10.10802378871.2018.1513050?journalCode=Code=rcyb20

[3] United States Department of Homeland Security, (2019). A guide to critical infrastructure security and resilience. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

[4] Lane, J. M. & Pretes, M. (2020). Maritime dependency and economic prosperity: Why access to oceanic trade matters. *Marine Policy, 121*, 104180. https://doi.org/10.1016/j.marpol.2020.104180.

[5] Organisation for Economic Co-operation and Development, (2022). How much could the ocean economy grow by 2030? https://www.oecd.org/ocean/topics/ocean-economy American Maritime Partnership, (2020). Maritime in your community. https://www.americanmaritimepartnership.com.

[6] Amerian Maritime Partnership, (2020). Maritime in you community. https://www.americanmaritimepartnership.com

[7] Terpsidi, F, Nikitakos, N. & Papachristos, (2019). Maritime industry revival through system digitalization. Journal of Multidisciplinary Engineering Science and Technology, 6(12), 111178 – 11185. http://www.jmest.org/wp-content/uploads/JMESTN42353215.pdf.

[8] Caprolu, M., Pietro, R. D., Raponi, S., Sciancalepore, S. & Tedeschi, P. (2020). Vessel cybersecurity: issues, challenges, and the road ahead. *IEEE Communications Magazine 58*(6)*, 90-96*. https://ieeexplore.ieee.org/document/9141222

[9] Tam, K. & Jones, K. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 1-18. https://doi/abs/10.1080/23738871.2018.1513053?journalCode=rcyb20

[10] National Institute of Standards and Technology, (2002). Risk management guide for informatino tehnology systems. http://www.icsdefender.ir/files/scadadefender-ir

[11] The White Hous, (2013). Executive order – Improving critical infrastructure cybersecurity. https://obamawhitehouse.archives.gov

[12] Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V.. & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection, 39*, 1-18. https://doi.org/10.1016/j.ijcip.202.100571

[13] Tam, K. & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18, 129-163. https://doi.org/10.1007/s13437-019-00162-2

[14] Tam, K. & Jones, K. (2018, June). "Cyber-risk assessment for autonomous ships. In 2018 international conference on cybersecurity and protection of digitial services(cyber security((pp. 1-8). IEEE. https://doi:10.1109/CyberSecPODS.2018.8560690.

[15] Shauer, S. Polemi, N. & Mouratidis, H. (2019). MITIGATE: A dynamic supply chain cyber risk assessment methodology. Journal of Transportation Security, 12, 1-35. https://10.1007/s12198-018-0195-z.

[16] Circle S.p.A. (2023). The MITIGATE methodology for risk assessment. https://www.onthemosway.eu

[17] Senarak, C. (2020). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics*, 371(1), 20-36. https://doi.org/10.1016/j.ajsl.2020.05..001.

[18] Galic, S., Lusic, Z., Mladenovic, S. & Gudelj, A. (2022). A chronological overview of scientific research on ship grounding frequency estimation models. Journal of Marine Science and Engineering, 10, 207. https://doi.org/10.3390/jmse10020207

[19] Melnyk, O., Onyshcenko, S., Pavlova, N., Kravchenko, O. & Borovyk, S. (2022). Integrated ship cybersecurity management as part f = of maritme safety and security systems. *International Journal of Computer Science and Network Security, 22*(3), 1-6. https://doi.org/10.22937/IJCSNS.2022.22.3.18

[20] Reeves, A., Delfabbro, P., & Calic, D. (2021). Encourading employee engagement with cybersecurity. How to tackle cyber fatigue. SAGE open, 11(1). https://doi.org/10.1177/21582440211000049

[21] Ramadan, R. A., Aboshosha, B.W., Alshudukhi, J. S., Alzahrani, A. J, Alzaharani, A. J. (2021) Cybersecurity and countermeasures at the time of pandemic. Journal of Advances Transportation, 2021, 1-19. https://doi.org/10.1155/2021/6627264

[22] Brooks, S. K. & Greenberg, N. (2022). Mental health and psychological wellbeing of maritime personnel: A systematic review. BMC Psychology, 10(139), 1-26. https://doi.org/10.1186/s40359-022-00850-4*Society, 68*(7), 780-791. doi:http://dx.doi.org/10.1057/jors.2016.37.

[23] Park, C., Kontovas, C., Yang, Z. & Chang, C. (2023).A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean and Coastal Managments, 235, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

[24] Malviya, S. & Lohiya, H. (2022). An analysis of authentication attacks with countermeasures and various authentication methods n a distributed environment. *International Research Jornal of Modernization in Engineering Technology and Science, 4*(12), 1-8. https://doi.org/10.56726IRJMETS319601.

[25] Sivasankari, N. & Kamalakkannan, S. (2022). Detectiona in prevention of man-in-the-middle attack in iot networking using regression modeling. *Advances in Engineering Software, 169*, 1-7. https://doi.org/10.1016/jadventgsoft.2022.103126

[26] Hopcraft, R., Tam, K. Misas, K.D. P., Moara-Nkwe, K. & Jones, K. (2023). Developing a maritime cyber safety culture: Improving safety of operations. *Maritime Technology and Research, 5*(1), 1-18. https://doi.org/10.33175/mtr.2023.258750.

[27] Liu, W., Xu, X., Wu, L., Qi, L., Jolfaei, A.....Ding, W. (2022). Intrusiong detectioin for maritime transportation systesm with batch federated aggregation. *Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3181436

[28] Zeng, M., Dian, C. & Wei, Y. (2023) Risk assessment of insider threats based on IHFACS-BN. Sustainability, (15(1),1-18. https://doi.org/10.3390/su15010491

[29] Shyshkin, O. (2022). Cyberseucrity providing for maritime automatic automatic identification system. 2022 IEEE 41st International Conference on Electronics and Nanotechnolo (ElNANO), Kyiv, Ukraine, pp. 736-740. https:10.1109ELNANO54557.2022.9926987

[30] Nalamati, M., Sharma, N., Saqib, M. & Blumenstein, M. (2020). Automated monitoring in maritime video surveillance system. *2020 35th International Conference on Image and Vision Computing New Zealand (IVCNZ)*, Wellington, New Zealand, 2020, pp. 1-6. https://doi.1109/IVCNZ51579.2020.9290533.

[31] Zaib, A., Yin, J., Khan, R. U. (2022). Determining role of human factors in transportation accidents by Fuzzy Fault Tree Analysis (FFTA). *Journal of Maritiem Science and Engineering, 10*(3), 1-14. https://doi.org/10.3390jmse10030381

[32] Ghahramani, H., Parhizgar, N., Bijan, A. A. & Barari, M. (2021). Convolutive complex valued independent component analysis for nonlinear radar signal processing and maritime weak target detection. *Mathematical Problems in Engineering*, 202. https://doi.org/10.115/2021/6191303

[33] Ilcev, M. (2020). New aspects for modernization Global Maritime Distress and Safety System (GMDSS). *The International Journal on Marine Navigation and Safety of Sea Transportation, 14*(4), 991-998. https://doi.org/10.12716/1011.14.04.26

[34] Kushch, S., Baryshev, Y. & Ranise, S. (2020). Blockchain tree as solution for distributed storage of personal id data and document access control. *Sensor, 20*(13), 3621. https://doi.org/10.3390/s20133621

[35] U.S. Department of Transportation Maritime Administration, (2021). Maritime transportation system (MTS) improving the U.S. marine transportation system. https://www.maritime.dot.gov/outreach.maritime-transportation-system-mts/maritime-transportation-system-mts

[36] Vogt, W. P. (Ed) (2005). Dictionary of statistics & methodology, (Vols. 1 -0). SAGE Publication, Inc., https://doi.org/10.4135/9781412983907.

[37] Cavanauge, J. & Foster, E. (Eds.) (2010)..(Vols. 1-0) SAGE Publications, Inc., https.doi.org/10.1435/9781412961288