RESEARCH IN MANAGEMENT OF TECHNOLOGY AND BUSINESS
e-ISSN: 2773-5044

RMTB

Vol. 6 No. 1 (2025) 102-114
https://publisher.uthm.edu.my/periodicals/index.php/rmtb

The Future of IoT Applications in Port Management System in Malaysia

Syahirah Shamsul Rizal[1], Fazian Hashim[1]*

[1] *Department of Management and Technology, Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, 86400, MALAYSIA*

*Corresponding Author: fazianh@uthm.edu.my
DOI: https://doi.org/10.30880/rmtb.2025.06.01.009

Article Info

Received: 31 March 2025
Accepted: 30 April 2025
Available online: 30 June 2025

Keywords

Internet of things, port management system, future, issues, drivers

Abstract

The Internet of Things (IoT) is the collective network of interconnected devices and the technology that enables communication between devices and the cloud. Nowadays, IoT has been adopted in port management system. The purpose of the study is to identify the issues, challenges, and trends of IoT applications in port management system, to study the key drivers of IoT applications in port management system, and to study the future image of IoT applications in port management system. The target respondents were selected among users of IoT applications in port management system in Westports Malaysia which is 359 respondents. The researcher utilized a quantitative method in this study. 359 questionnaires were distributed to the respondents via online survey and the survey return rate was 37.05%. This study employs foresight instruments such as STEEPV Analysis and SPSS analysis. STEEPV analysis is used to identify the issues, challenges, and trends of IoT applications in port management system. SPSS analysis has been used to show the result of the key drivers of IoT applications in port management system in the second phase of the research with impact-uncertainty analysis. 10 merged key drivers have been identified. The approach of impact-uncertainty analysis has been used to determine the future image of IoT applications in port management system. The top two drivers are technology reliability and IoT secure system in port management system. It indicates that these two drivers ensuring technology reliability and IoT security is crucial for future port management systems to maintain operational efficiency, safeguard data, and prevent disruptions in critical logistics networks. The scenario analysis has been formed based on the top two drivers and four scenarios will represent the possible outcome from 2024 to 2034. Hence, this research can help future researchers and developers increase their awareness of adopting IoT in the future.

1. Introduction

IoT is referred to as the Internet of Things. It represents a network of physical devices that are inserted with software, sensors, and other technologies that enable them to communicate with other devices and systems over the internet or other communication networks in order to connect and exchange data (Oracle, 2020) A port was considered intelligent when it is equipped with many 4.0 technologies like sensors, robots, Radio-frequency Identification (RFID), IoT, or Big Data accordingly for administration and analysis (Hoang Phuong Nguyen et al.,

2022). These technologies would improve the port's ability to solve problems efficiently. In brief, these technologies will optimise port operations and make port management simpler (Hoang Phuong Nguyen et al., 2022). The development of new digitization paradigms like robotics, cloud-edge computing, big data, machine learning, and the Internet of Things (IoT) has made the Industry 4.0 idea possible and opened up new opportunities for the port industry (Eduardo Garro et al., 2023). Due to the real-time factor and not relying on human data collection, IoT enables data driven inspection on demand which boosts uninterrupted port operations (Jorge Merino et al., 2022) Enabling a seamless and real-time connection of all equipment and systems is improving operational procedures and cargo handling. In these new circumstances, the industry can create more automated and interconnected systems with less risk, at a lower cost, with less need for human interaction, and with a faster lead time (Eduardo Garro et al., 2023). Due to the port industry's strict requirements and intense competition, port operations must be performed precisely in order to achieve high operating throughput and maintain profitability and safety (Eduardo Garro et al., 2023). Efficiency gains in this area can therefore have a significant positive impact. Cargo ports all over the world are currently undergoing various types of technological change in order to improve the visibility of their assets. They are moving towards digital, connected, and intelligent port automation (Eduardo Garro et al., 2023). Therefore, IoT application might make daily operations using human resources simpler and enable the port to meet client needs.

An essential component of port management is the use of IoT technologies. It offers a number of benefits to port management system. Firstly, optimization of operation where port managers are able to track and manage operational factors including container tracking, vessel traffic control, logistics management, and equipment maintenance through the data collecting and sharing capabilities of these devices (Prosertek, 2023). Greater efficiency, shorter waiting times, and lower operating expenses are all attained by optimising these procedures. Secondly, it improved security where sensors in networked devices at ports allow for continuous observation of port surroundings and early identification of possible threats or incidents (Prosertek, 2023). Quick and automatic emergency reaction greatly enhances security and safety while protecting workers and cargo. Thirdly, this technology makes port assets' location and status visible (Prosertek, 2023). Infrastructure and equipment with embedded sensors can gather information on wear and tear, energy usage, performance, and environmental factors. In order to prevent unanticipated failures, minimise downtime, and maximise resources, this information facilitates proactive asset management and predictive maintenance planning. However, besides these advantages, IoT still has many disadvantages, such as lack of security, unreliability, energy inefficiency, and centralized data storage (Fetahu et al., 2022; Talebkhah et al., 2021). For instance, when the Internet connection between IoT devices and cloud servers is interrupted, IoT services cannot be maintained properly. The port transportation sector is progressively relying more on digital tools and software. Numerous interconnected devices can directly retrieve sensitive information, such as port routes and safety plans, thereby elevating the risk of information breaches and unauthorized access (Zhou et al., 2021) In fact, the automation of the acquisition and processing of data enabled by IoT systems should lead to clear improvements at the levels of integration of the transport chain, sustainability and efficiency in the transport modes and change amongst modes, and intelligence in the decisions to be taken for the logistics sector (Papert & Pflaum, 2017; Tiwari, Wee, & Daryanto, 2018). Even if it can be difficult to overcome these obstacles, IoT has the power to revolutionise port management and enhance the effectiveness, security, and sustainability of ports all over the world.

The foresight study was conducted ten years into the future or between 2024 to 2034. The resources and data related to the IoT application trend in port management systems are highlighted in this study. Every important piece of information and data about IoT in port management systems has been gathered from a variety of sources, including books, journals, conference proceedings, and other research materials. This study's focus was on port management systems. Users of IoT in port management systems in Westports Malaysia were the research responders. The target respondents were mostly IoT users in the port management system within organisations in Westports Malaysia. The goal of the questionnaire is to gather data from respondents, which then be analysed and utilised for data analysis. The questionnaire has been distributed to the advocates' respondents.

2. Literature Review

Table 1 presents a consolidated view of the drivers associated with the merged issues, challenges and trends.

Table 1 *Table of drivers related to merged issues, challenges and trends*

No.	Issues, Challenges and Trends	Drivers
1	Security measures Edge oriented secure system Cyber security threats Expose sensitive information Detecting cyber attacks	IoT secure system

2	Smart objects and sensors Information and Communication Technology (ICT) Edge, fog and cloud computing IoT sensors via 5G technology	Digitalization
3	Competitiveness and demanding needs Increased customer demand Local and global logistics Global supply chain	Market demand
4	Worldwide economic Return in investment Economic survival and growth Flexible and reliable service	Economic growth
5	6G networks 6G wireless technologies Internet of Drones (IoT) Modern IoT platform	Technology innovativeness
6	Controlled environment Monitoring environmental compliance Sustainability improvement	Environment sustainability
7	Cost savings Lower cost Loss of revenue Return in investment	Production cost
8	Minimized human intervention Simplify human resources Operational efficiency Smarter decision making	Human resource reliability
9	Congestion pressures Operational process Efficient processing power Quality of goods	Technology reliability
10	Achieving dynamic and adaptable coverage Achieving global maritime communication coverage Achieving operational efficiency Achieving automated and interoperable solutions Achieve high operational throughput	Technology effectiveness

3. Research Methodology

3.1 Research Design

In order to gain a comprehensive understanding, quantitative data has been examined. Using a mixed-method foresight technique, the research attempts to analyse the issues, challenges, and trends of IoT applications in port management systems. In order to analyse the future of IoT applications in port management systems, this foresight technique uses a quantitative method in this study. Figure 1 is a flowchart that shows the visual display of the activities in a process. The researcher will better understand the processes and the work at all levels with the aid of this visual review process, which serves as a framework. This research flow chart helps the researcher ensure that the research was carried out properly, as shown in Fig. 1.

Research in Management of Technology and Business Vol. 6 No. 1 (2025) p. 102-114

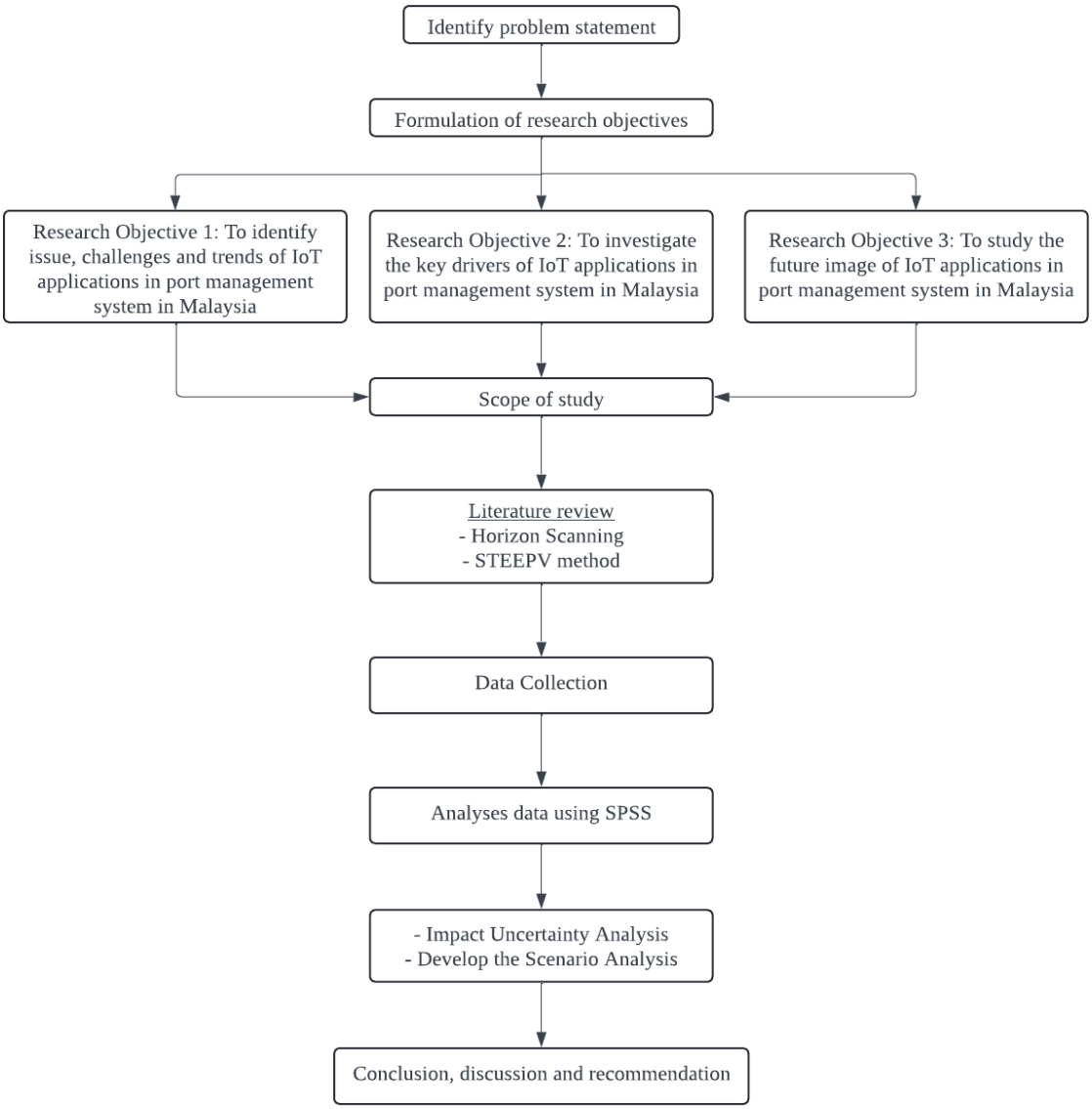

Fig. 1 *Research flow chart*

3.2 Foresight Process

The foresight process gathers and analyses data in order to enable individuals to think about the future in novel and varied ways. Foresight has involved a number of stages. For example, the data has been analysed using STEEPV analysis, the change drivers for IoT applications in port management systems were identified, and the foresight process started with horizon scanning.

3.2.1 Horizon Scanning

Focusing on the new technology and its implications, horizon scanning is a technique for seeing possible dangers, risks, emerging challenges, opportunities, and future advancements. According to the Government Office of Science & Cabinet Office (2013), horizon scanning is a tool for future analysis and the identification of emerging trends and changes that will impact policies and practices in the future. Based on desk research, the purpose of horizon scanning was to help the researcher find patterns, changes, unforeseen issues, and constants. Journal articles, books, the internet, and other sources are a few examples of desk research.

3.2.2 STEEPV Method

The STEEPV method has 10 steps, which are data designing, data listing, data classification, data identification, theme comparison, repeat, data inspection, revision, data merging, and final confirmation.

3.2.3 Drivers

The elements that will shape, change, or influence future growth are known as drivers. Every driver that has been gathered will be identified or determined using STEEPV. A wide range of instruments are available for evaluating or classifying drivers. Examples include the future wheel, the S-curve, and impact-uncertainty analysis. Impact-uncertainty analysis is used in this study to examine the future variables or drivers that will affect and influence the issues, challenges, and trends associated with IoT applications in the port management system. Based on desk research, the purpose of horizon scanning was to help the researcher find trends, changes, unforeseen issues, and constants. Journal papers, books, and the internet are a few examples of desk research.

3.3 Population and Sampling Techniques

A study population is a significant population of persons or individuals who are the main subject of a scientific investigation. The population is defined as a large group of individuals, institutions, items, and other things that share common characteristics, and the researcher was interested in this characteristic (Rafeedalie, n.d.). The Internet of Things (IoT) applications in port management systems are the focus of this study. Therefore, the target audience consisted of users of the IoT application in the port management system in Westports Malaysia. Thus, this study aims to gather information from the 5725 IoT users in the port management system in Westports Malaysia.

The sampling technique utilised in this investigation is purposive sampling. Purposive sampling is the process of choosing samples based on the goals of the study and the characteristics of the population. Based on a population of 5725 people, the Krejcie and Morgan Table indicates that the study's sample size will be 359 respondents (KENPRO, 2012). 359 respondents who use the IoT in the port management system have contributed to the study's sample size.

3.4 Research Instrument

This study chose to use a questionnaire as its primary research tool. This study used a questionnaire because the data obtained from the questionnaire was effective and easy to understand. The questionnaire was employed in this study because it can be utilised to determine future trends, challenges, and issues of IoT applications in port management systems. The advocates of IoT applications in the Malaysian port management system were given the questionnaire. There were four parts to this research questionnaire: parts A, B, C, and D. The respondents' demographic data is shown in Part A, while Part B reveals how they ranked or chose the important drivers. Part C measured the degree of impact of the drivers of IoT applications in port management systems, whereas Part D measured the degree of uncertainty of the key drivers of IoT applications in ports.

3.5 Data Collection

Data collection is the process of collecting, analysing, and ensuring that data from multiple sources may be utilised to meet the goals of the research. The two components of the data collection method are primary data and secondary data. The researcher gathers primary data through surveys, questionnaires, and sampling from primary sources. Stated in different ways, primary data includes various types of information that has been gathered for the first time. For instance, the majority of the main data was collected using a questionnaire. Information gathered from a previous study is known as secondary data. The gathering of secondary data from articles, books, journals, newspapers, websites, and other sources. Both primary and secondary data gathering were performed in this study to gather information. To determine the issues, challenges, and trends in IoT applications in the port management system, a collection and analysis of IoT sources was conducted. The application of secondary data collection was common in many research studies due to its potential as an additional resource for primary source data. Table 2 shows the reliability of the pilot study. Meanwhile, Table 3 shows the reliability test for the actual study.

Table 2 *Reliability of pilot test*

Factors	Cronbach's Alpha Value
Level of Importance	0.727
Level of Impact	0.708
Level of Uncertainty	0.811

Table 3 *Reliability for the Actual Study*

Factors	Cronbach's Alpha Value
Level of Importance	0.842
Level of Impact	0.836
Level of Uncertainty	0.908

3.6 Analysis of Data

3.6.1 Descriptive Analysis

Descriptive Analysis is the type of analysis of data that helps describe, show or summarise data points in a constructive way such that patterns might emerge that fulfil every condition of the data (Ayush Singh Rawat, 2021). The 'Statistical Package for Social Science' (SPSS) was utilised to analyse the data that was collected through the questionnaire. The SPSS software will assist in producing statistical data in numerical form. Additionally, SPSS displayed the collected data as a percentage, mean, and standard deviation.

3.6.2 Impact-Uncertainty Analysis

An impact uncertainty analysis was developed using the driver list. The drivers were ranked in terms of importance, impact, and uncertainty. To create a scenario analysis, the top two variables with the highest degree of impact and uncertainty have been selected based on the list. The creation of the scenario analysis followed an impact uncertainty analysis based on the computed mean value from the data analysis.

3.6.3 Development of Scenario Analysis

The impact-uncertainty analysis's top two drivers were used to create the scenario analysis. Regardless of positive or negative outcomes, the future effects of events and trends of IoT applications in the port management system were divided into four unique possible scenarios. The study's recommendations and implications were examined at the end of the study. The four potential outcomes that could occur between 2024 and 2034 are represented by these alternate scenarios.

4. Results and Discussion

4.1 Demographic Analysis

In this research, there are 59 males (44.4%) and 74 females (44.4%). For age, 68 respondents (51.1%) are between 20-29 years old. 35 respondents (26.3%) are between 30-39 years old, and 30 respondents (22.6%) are above 40 years old. For Job Level, 53 respondents (39.8%) are middle management, 39 respondents (29.3%) are executive or senior management, and 31 respondents (23.3%) are intermediate or experienced staff. Entry-level had the lowest number of respondents, with only 10 workers (7.5%). For work sector, Marketing had the highest number of respondents at 36 workers (27.1%), followed by Supply Chain Management had 21 respondents (15.8%), Port Management & Administration had 20 respondents (15%), Maintenance and Engineering had 19 respondents (14.3%), Security and Safety had 18 respondents (13.5%) and Finance had 7 respondents (5.3%). As for the years of experience in port industry, 68 respondents (51.1%) had 5-10 years' experience, 23 respondents (17.3%) had 2-5 years' experience, 19 respondents had 10-20 years' experience, 15 respondents (11.3%) had less than 2 years' experience and only 8 respondents (6%) had more than 20 years' experience in port industry. Lastly, 122 respondents (91.7%) stated that they are high chance that IoT will play an integral role in the port industry in the next 10-15 years, while only 11 respondents (8.3%) stated that the chances are medium.

4.2 Mean of Drivers in Corresponding with Importance

Table 4 below shows the mean of the first six leading Drivers based on level of importance.

Table 4 *Mean of the first six leading drivers on importance*

No	Drivers	Mean
1	IoT secure system	4.4060
2	Production cost	4.3609
3	Human resource reliability	4.3459

4	Technology innovativeness	4.3383
5	Digitalization	4.3308
6	Technology reliability	4.3158

4.3 Mean of Drivers in Corresponding with the Level of Impact

Table 5 below shows the mean of the six leading drivers on the level of impact.

Table 5 *Mean of the six leading drivers on the level of impact*

No	Drivers	Mean
1	IoT secure system	4.3383
2	Production cost	4.3008
3	Human resource reliability	4.2707
4	Technology innovativeness	4.3609
5	Digitalization	4.2632
6	Technology reliability	4.4060

4.4 Highest to The Lowest Mean Based on Its Uncertainty

Table 6 below shows the mean of the six leading drivers on the level of uncertainty.

Table 6 *Mean of the six leading drivers on the level of Impact*

No	Drivers	Mean
1	IoT secure system	4.2932
2	Production cost	4.2707
3	Human resource reliability	4.2632
4	Technology innovativeness	4.2782
5	Digitalization	4.2556
6	Technology reliability	4.3308

4.3 Impact-Uncertainty Analysis

According to the graph in Fig. 2, D3 and D5 had the highest impact and uncertainty. D3 represented the economic dynamics, and D5 represented the governance in the Metaverse.

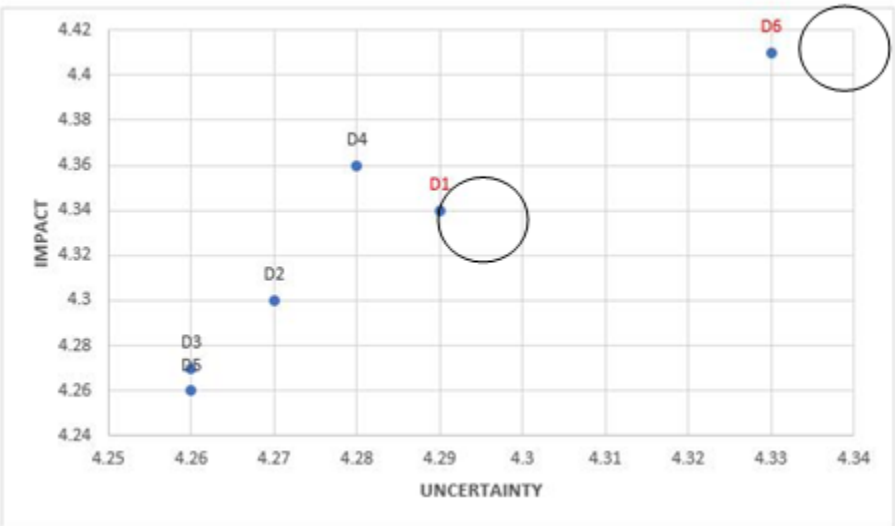

Fig. 2 *Impact Uncertainty Analysis*

The mean values for impact-uncertainty are illustrated in Table 7. The researcher must arrange and evaluate the data gathered during the data collection phase in order to comprehend it. Data analysis is used to identify study findings and whether the research will fulfil its goals. Data will be gathered from primary sources through the distribution of questionnaires.

Table 7 *Mean of the six leading drivers on Level of Impact and Uncertainty*

No	Drivers	Mean	
		Uncertainty	Impact
D1	IoT secure system	4.2932	4.3383
D2	Production cost	4.2707	4.3008
D3	Human resource reliability	4.2632	4.2707
D4	Technology innovativeness	4.2782	4.3609
D5	Digitalization	4.2556	4.2632
D6	Technology reliability	4.3308	4.4060

4.5 Scenario 1: Booming of Internet of Things (IoT)

Based on Fig. 3 below, the first scenario occurs when there is a high technology reliability and high IoT secure system. The "booming of Internet of Things (IoT)" in the context of port management systems refers to a transformative period where IoT technologies are rapidly adopted and integrated into port operations, leading to significant improvements in efficiency, safety, and sustainability. In this scenario, the Internet of Things (IoT) experiences unprecedented growth and integration across various sectors, driven by high technology reliability and strong security systems. The convergence of these two critical factors creates an environment where IoT devices and applications flourish, transforming industries and enhancing everyday life. As IoT systems become increasingly integrated into port operations, ensuring cybersecurity is paramount (Barak et al., 2020). Governments must implement strong cybersecurity measures to protect IoT devices and networks from cyber threats. This includes establishing cybersecurity standards, conducting regular security assessments, and providing training and resources to port operators. Besides, governments can invest in the necessary infrastructure to support IoT deployment in ports. This includes upgrading existing port facilities with modern IoT-compatible equipment and building new infrastructure that integrates IoT technologies from the ground up. Investments in high-speed internet connectivity, advanced sensor networks, and data processing centres are essential to ensure that ports can effectively utilise IoT solutions.

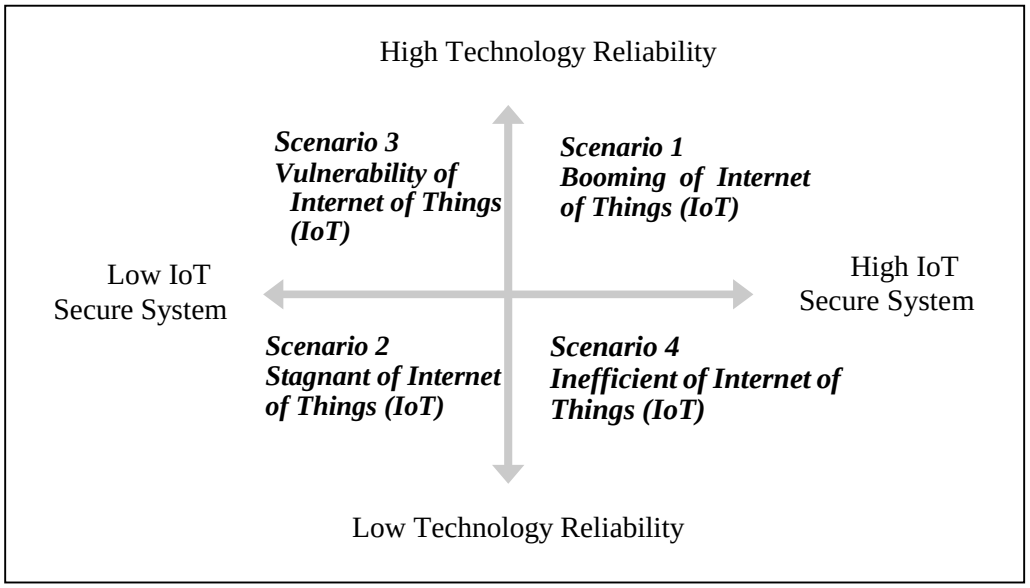

Fig. 3 *Development of Four Scenario Analysis*

4.6 Scenario 2: Stagnation of Internet of Things (IoT)

Based on Fig. 3 above, the second scenario occurs when there is a low IoT secure system and low technology reliability. The phrase "stagnant of Internet of Things (IoT)" describes a situation in which the adoption and advancement of IoT technology in ports is sluggish or slow. Numerous causes, such as low technology reliability, insufficient security measures and lack of investment, might cause this stagnation. The potential advantages of IoT in port management are not fully utilized in such a situation, which results in inefficiencies and lost chances for improvement. The lack of reliable technology infrastructure is a significant barrier to IoT adoption in port management. To overcome this, governments can prioritise the modernisation of existing digital infrastructures, such as communication networks and data processing systems. Besides, government should also strengthen IoT security system by establishing laws requiring strict security measures for all IoT implementations. This includes secure authentication procedures, end-to-end encryption, and frequent software updates to reduce vulnerabilities.

4.7 Scenario 3: Vulnerability of Internet of Things (IoT)

Based on Fig. 3 above, the third scenario occurs when there is a high technology reliability but low IoT secure system. In the context of high-technology reliability and low IoT secure systems, the phrase "vulnerability of Internet of Things (IoT)" describes a situation in which IoT systems and devices in port management are very reliable in terms of performance and functionality but have a severe lack of security measures. As a result, the technology functions well and efficiently, but the systems are vulnerable to different cyberthreats and attacks due to the absence of strong security frameworks. The safety, effectiveness, and integrity of port operations may be significantly impacted by this vulnerability in port management systems. The low security of IoT systems leaves ports vulnerable to cyberattacks, data breaches, and unauthorized access. To overcome this, governments should make sure port authorities have strong incident response strategies in place to reduce interruption and lessen the harm that security breaches can bring.

4.8 Scenario 4: Inefficient of Internet of Things (IoT)

Based on Fig. 3 above, the last scenario will occur when there is a high IoT secure system and low technology reliability. In the context of low technology reliability and high IoT secure systems, the phrase "inefficient of Internet of Things (IoT)" describes a situation in which IoT systems and devices in port management are extremely secure but have low reliability. This results in a scenario where the technology performs inconsistently and ineffectively in spite of strong security measures, causing operational difficulties and inefficiencies. The total effectiveness and productivity of port operations may be significantly impacted by this inefficiency in port management systems. To overcome these inefficiencies, governments must implement strategies that strike a balance between enhancing technology reliability and optimizing security systems. System reliability can be increased, and downtime can be decreased by putting predictive maintenance technologies into place to help detect any device problems before they happen. Government can use grants or subsidies to encourage ports to implement these technologies. Government should also aim to optimize security measures to maintain both safety and performance. Additionally, rather than enforcing consistent security protocols for all IoT systems, governments might promote a risk-based strategy. High-security protocols should focus on critical systems, while less-sensitive systems can use lighter security measures to optimize efficiency.

5. Conclusion

The first objective of this research is to identify issues, challenges, and trends of IoT applications in the port management system. This objective had been generated through the STEEPV analysis. The issues, challenges, and trends have been analysed based on previous research. Based on STEEPV analysis, social is the most critical driver in IoT applications, followed by technological, economic, values, environmental, and political factors.

The second objective is to study the key drivers of IoT applications in the port management system. After the STEEPV analysis, the 10 drivers have been developed based on merged issues, challenges, and trends of IoT applications in the port management system. The ten drivers are IoT secure system, digitalisation, market demand, economic growth, technology innovativeness, environment sustainability, production cost, human resource reliability, and technology reliability. The top 60 per cent of drivers were selected based on three aspects, which are importance, level of impact, and level of uncertainty. The two top drivers have been chosen based on the impact-uncertainty analysis. Based on the use of IoT in the port management system, the top two drivers have the most impact and uncertainty.

The capacity of IoT devices and systems to function reliably and efficiently without malfunctions or disruptions is referred to as technology reliability in IoT applications for port management systems. Accurate data gathering, seamless device connection, and effective operations in vital port services, including cargo handling, vessel tracking, and equipment monitoring, are all made possible by dependable technology (Othman et al.,2023). Reliable IoT systems allow for improved safety, predictive maintenance, and real-time decision-making (Wang et

el.,2024). However, low technological reliability can have a negative effect on port efficiency and safety by causing frequent malfunctions, inaccurate data, and operational disruptions. Sustaining high reliability is essential for cost reduction, resource optimisation, and smooth port operations.

IoT secure system is the deployment of strong security mechanisms that shield IoT networks, devices, and data from intrusions, illegal access, and data breaches. IoT security is crucial for maintaining seamless operation and stakeholder trust because ports are vital infrastructure that handle enormous volumes of sensitive data and automated processes (Cui et al., 2023). An IoT system with a high level of security guarantees strong defence against online attacks, illegal access, and data breaches (Li et al., 2024). However, IoT devices and networks are exposed when a low IoT security system is not sufficiently protected against cyberattacks. Significant dangers, such as financial losses, data breaches, and operational interruptions, may result from this.

The third objective was to describe the future image of IoT applications in port management system. This objective also needs to identify the forces that can change the future of IoT applications in port management system. Four different scenarios have been formed based on the top two drivers chosen from the impact-uncertainty analysis. These four alternative scenarios represent the four possibilities that might happen from 2024 to 2034. The top two drivers that has the highest impact and uncertainty were technology reliability and IoT secure system.

In conclusion, this research aims to identify the issues, challenges, and trends, study the key drivers of IoT applications in the port management system, and describe the future image of IoT applications in the port management system in Malaysia. IoT's growth and demand in port management systems have both expanded in the current era of digitalisation. The industry's adoption of IoT for applications has also been inspired by the widespread use of IoT applications in the port management system. The four scenarios indicated the technology reliability and secure system in IoT applications in the port management system. The technology reliability in IoT and the secure system have a strong relationship. Both factors can create the best scenario, such as "Booming of Internet of Things (IoT)", where port management systems are more effective in using IoT. But those two factors also will cause some adverse scenarios in the future, like "Stagnation of Internet of Things (IoT)", "Vulnerability of Internet of Things" and "Inefficiency of Internet of Things (IoT)". Hence, these future scenarios can benefit future researchers and industries in sustaining the future development of IoT applications in the port management system.

Acknowledgement

The authors would like to thank the Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia for its support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Syahirah Shamsul Rizal and Fazian Hashim;* ***data collection:*** *Syahirah Shamsul Rizal and Fazian Hashim;* ***analysis and interpretation of results:*** *Syahirah Shamsul Rizal and Fazian Hashim;* ***draft manuscript preparation:*** *Syahirah Shamsul Rizal and Fazian Hashim. All authors reviewed the results and approved the final version of the manuscript.*

References

Ahmed, E., Yaqoob, I., Hashem, I. a. T., Khan, I., Ahmed, A. I. A., Imran, M., & Vasilakos, A. V. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, 129, 459–471. https://doi.org/10.1016/j.comnet.2017.06.013

Alamer, A. M. A., Basudan, S. a. M., & Hung, P. C. (2023). A privacy-preserving scheme to support the detection of multiple similar request-real-time services in IoT application systems. *Expert Systems With Applications*, 214, 119005. https://doi.org/10.1016/j.eswa.2022.119005

Barak, D. D., Singh, K., Ahlawat, P., & Sharma, H. K. (2020). Real Time Tracking System: an IoT based application. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3545226Barasti, D., Troscia, M., Lattuca, D., Tardo, A.,

Barsanti, I., & Pagano, P. (2021). An ICT Prototyping Framework for the "Port of the Future." *Sensors*, 22(1), 246. https://doi.org/10.3390/s22010246

Bhaskaran, P. E., Maheswari, C., Thangavel, S., Ponnibala, M., Kalavathidevi, T., & Sivakumar, N. (2021). IoT Based monitoring and control of fluid transportation using machine learning. *Computers & Electrical Engineering*, 89, 106899. https://doi.org/10.1016/j.compeleceng.2020.106899

Cedillo-Campos, M. G., Flores-Franco, J. E., & Covarrubias, D. (2024). A physical internet-based analytic model for reducing the risk of cargo theft in road transportation. *Computers & Industrial Engineering*, 190, 110016. https://doi.org/10.1016/j.cie.2024.110016

Conways. (n.d.). An Overview of Foresight Methodologies. Thinking futures. pp. 1-10.Cui, D., Sun, G., & Zhan, X. (2023). Security Risk Management System for the construction and operation of smart port area based on BP Neural Network Algorithm. *Procedia Computer Science,* 228, 838–846. https://doi.org/10.1016/j.procs.2023.11.111

Europea, E. (2020, March 17). IoT impact on Port Operations. Escola Europea - *Intermodal Transport*. https://escolaeuropea.eu/blue-innovation/iot-impact-on-port-operations/

Fazel, E., Nezhad, M. Z., Rezazadeh, J., Moradi, M., & Ayoade, J. (2024). IoT convergence with machine learning & blockchain: A review. Internet of Things, 101187. https://doi.org/10.1016/j.iot.2024.101187

Fetahu, L., Maraj, A., & Havolli, A. (2022). Internet of Things (IoT) benefits, future perspective, and implementation challenges. *45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*. https://doi.org/10.23919/mipro55190.2022.9803487

Garro, E., Lacalle, I., Blanquer, F., Ramos, A., Martinez, A., Sowiński, P., Llorente, M. A., & Palau, C. (2023). Maritime terminals' cargo handling equipment cooperation leveraging IoT and edge computing: The ASSIST-IoT approach. *Transportation Research Procedia*, 72, 2864–2871. https://doi.org/10.1016/j.trpro.2023.11.831

Huaranga-Junco, E., González-Gerpe, S., Castillo-Cara, M., Cimmino, A., & García-Castro, R. (2024). From cloud and fog computing to federated-fog computing: A comparative analysis of computational resources in real-time IoT applications based on semantic interoperability. *Future Generation Computer Systems*, 159, 134–150. https://doi.org/10.1016/j.future.2024.05.001

IoT M2M Council. (2024, August 26). US Executive Order on port cybersecurity - IoT M2M Council. https://www.iotm2mcouncil.org/iot-library/news/iot-in-public-policy/us-executive-order-on-port-cybersecurity/

K.-L.A. Yau, S. Peng, J. Qadir, Y.-C. Low, M.H. Ling, Towards smart port Kaderi, F. A., Koulali, R., & Rida, M. (2019). Automated management of maritime container terminals using internet of things and big data technologies. *Proceedings of the 4th International Conference on Smart City Applications.* https://doi.org/10.1145/3368756.3369046

Kenpro. (2012). Sample Size Determination Using Krejcie and Morgan Table. *Retrieved from http://www.kenpro.org/sample-size-determination-using-krejcie-and-morgan-table/*

Khajenasiri, I., Estebsari, A., Verhelst, M., & Gielen, G. (2017). A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications. *Energy Procedia*, 111, 770–779. https://doi.org/10.1016/j.egypro.2017.03.239

Kizilay, D., & Eliiyi, D. T. (2020). A comprehensive review of quay crane scheduling, yard operations and integrations thereof in container terminals. *Flexible Services and Manufacturing Journal,* 33(1), 1–42. https://doi.org/10.1007/s10696-020-09385-5

Kou, G., Yi, K., Xiao, H., & Peng, R. (2022). Reliability of a distributed data storage system considering the external impacts. *IEEE Transactions on Reliability*, 72(1), 3–14. https://doi.org/10.1109/tr.2022.3161638

Kumar, C., & Ansari, M. S. A. (2024). An explainable nature-inspired cyber attack detection system in software-defined IoT applications. *Expert Systems With Applications,* 250, 123853. https://doi.org/10.1016/j.eswa.2024.123853

Kumar, N., & Ali, R. (2024). Blockchain-enabled authentication framework for maritime transportation system empowered by 6G-IoT. *Computer Networks*, 244, 110353. https://doi.org/10.1016/j.comnet.2024.110353

Li, J., Han, D., Weng, T., Wu, H., Li, K., & Castiglione, A. (2024). A secure data storage and sharing scheme for port supply chain based on blockchain and dynamic searchable encryption. *Computer Standards & Interfaces*, 91, 103887. https://doi.org/10.1016/j.csi.2024.103887

Li, X., Xiao, P., Tang, D., Li, X., Wang, Q., & Chen, D. (2024). UAVs-assisted QoS guarantee scheme of IoT applications for reliable mobile edge computing. *Computer Communications.* https://doi.org/10.1016/j.comcom.2024.05.010

Lira, C., Batista, E., Delicato, F. C., & Prazeres, C. (2023). Architecture for IoT applications based on reactive microservices: A performance evaluation. *Future Generation Computer Systems,* 145, 223–238. https://doi.org/10.1016/j.future.2023.03.026

Lyu, Y., & Yin, P. (2019). Internet of Things transmission and network reliability in complex environment. *Computer Communications,* 150, 757–763. https://doi.org/10.1016/j.comcom.2019.11.054

Macheso, P. S., & Zekriti, M. (2024). Modelling and Analysis of Fiber Bragg Grating Temperature Sensor for Internet of Things Applications (FBG-4-IoT). *International Journal of Intelligent Networks*. https://doi.org/10.1016/j.ijin.2024.05.006

McCombes, S. (2023, January 2). How to write a literature review. Scribbr. https://www.scribbr.com/methodology/literature-review/

Merino, J., Sasidharan, M., Herrera, M., Zhou, H., Del Castillo, A. C., Parlikad, A. K., Brooks, R., & Poulter, K. (2022). Lessons learned from an IoT deployment for condition monitoring at the Port of Felixstowe. *IFAC-PapersOnLine*, 55(19), 217–222. https://doi.org/10.1016/j.ifacol.2022.09.210

Min, H. (2022). Developing a smart port architecture and essential elements in the era of Industry 4.0. *Maritime Economics & Logistics*, 24(2), 189–207. https://doi.org/10.1057/s41278-022-00211-3

Molavi, A., Lim, G. J., & Race, B. (2019). A framework for building a smart port and smart port index. International *Journal of Sustainable Transportation*, 14(9), 686–700. https://doi.org/10.1080/15568318.2019.1610919

Moore, S. J., Nugent, C. D., Zhang, S., & Cleland, I. (2020). IoT reliability: a review leading to 5 key research directions. *CCF Transactions on Pervasive Computing and Interaction*, 2(3), 147–163. https://doi.org/10.1007/s42486-020-00037-z

Muñuzuri, J., Onieva, L., Cortés, P., & Guadix, J. (2020). Using IoT data and applications to improve port-based intermodal supply chains. *Computers & Industrial Engineering*, 139, 105668. https://doi.org/10.1016/j.cie.2019.01.042

Negueroles, S. C., Simón, R. R., Julián, M., Belsa, A., Lacalle, I., S-Julián, R., & Palau, C. E. (2024). A Blockchain-based Digital Twin for IoT deployments in logistics and transportation. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2024.04.011

Nguyen, H. P., Nguyen, P. Q. P., Nguyen, D. K. P., Bui, V. D., & Nguyen, D. T. (2023). Application of IoT Technologies in Seaport Management. JOIV : *International Journal on Informatics Visualization*, 7(1), 228. https://doi.org/10.30630/joiv.7.1.1697

Nguyen, T., Nguyen, H., & Gia, T. N. (2024). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. *Journal of Network and Computer Applications*, 103884. https://doi.org/10.1016/j.jnca.2024.103884

Oracle. (2020). What is the Internet of Things (IoT)? Oracle.com. https://www.oracle.com/my/internet-of-things/what-is-iot/

Othman, M. K., Rahman, N. S. F. A., Ismail, A., Osnin, N. A., & Hanafiah, R. M. (2023). Revisiting Malaysia's port classification system in a complex operational environment to streamline the coordination and management of maritime ports. *Case Studies on Transport Policy,* 13, 101062. https://doi.org/10.1016/j.cstp.2023.101062

Papert, M., & Pflaum, A. (2017). Development of an Ecosystem Model for the Realization of Internet of Things (IoT) Services in Supply Chain Management. EM, 27(2), 175–189. https://doi.org/10.1007/s12525-017-0251-8

Prosertek. (2023, June 19). The implementation of IoT technology in port management. Prosertek. https://prosertek.com/blog/iot-technology-in-port-management/

Rawat, A. S. (2021, March 31). What is Descriptive Analysis?- Types and Advantages | Analytics Steps. Analytic Steps. https://www.analyticssteps.com/blogs/overview-descriptive-analysisReliability Analysis. (2017, September 8). Www.ibm.com. https://www.ibm.com/docs/kk/spss-statistics/25.0.0?topic=features-reliability-analysis

Rajawat, A. S., Bedi, P., Goyal, S. B., Shaw, R. N., & Ghosh, A. (2022). Reliability Analysis in Cyber-Physical System using deep learning for smart cities industrial IoT network node. *In Studies in Computational Intelligenc*e (pp. 157–169). https://doi.org/10.1007/978-981-16-7498-3_10

Singh, K., Yadav, M., Singh, Y., Barak, D., Saini, A., & Moreira, F. (2024). Reliability on the Internet of Things with designing approach for exploratory analysis. *Frontiers in Computer Science*, 6. https://doi.org/10.3389/fcomp.2024.1382347

Siraparapu, S. R., & Azad, S. (2024). Securing the IoT Landscape: A Comprehensive review of secure systems in the digital era. e-Prime - *Advances in Electrical Engineering Electronics and Energy*, 100798. https://doi.org/10.1016/j.prime.2024.100798

Spektor, H. (2024, September 10). Understanding IoT Security: Threats, standards & best practices. Sternum IoT. https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/

Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., & Rokhani, F. Z. (2021). IoT and Big Data Applications in Smart Cities: Recent Advances, Challenges, and Critical Issues. *IEEE Access,* 9, 55465–55484. https://doi.org/10.1109/access.2021.3070905technology, Ieee Access 8 (2020) 83387–83404.

Tiwari, S., Wee, H., & Daryanto, Y. (2018). Big data analytics in supply chain management between 2010 and 2016: Insights to industries. *Computers & Industrial Engineering*, 115, 319–330. https://doi.org/10.1016/j.cie.2017.11.017

Wang, S., Wang, H., Xue, G., Han, Y., Qin, Q., Zhang, L., & Ma, X. (2024). Correlation analysis of failure risk factors in automated container port logistics systems from a resilience perspective. *Journal of Sea Research*, 102552. https://doi.org/10.1016/j.seares.2024.102552

Wang, Y., & Wright, L. A. (2021). A Comparative Review of Alternative Fuels for the Maritime Sector: Economic, Technology, and Policy Challenges for Clean Energy Implementation. *World*, 2(4), 456–481. https://doi.org/10.3390/world2040029

Wang, Z., Zeng, Q., & Haralambides, H. (2024). Shift of emphasis toward intelligent equipment maintenance in port operations: A critical review of emerging trends and challenges. *Ocean & Coastal Managemen*t, 259, 107408. https://doi.org/10.1016/j.ocecoaman.2024.107408

Xing, L. (2020). Reliability in Internet of Things: Current status and future Perspectives. *IEEE Internet of Things Journal*, 7(8), 6704–6721. https://doi.org/10.1109/jiot.2020.2993216

Zhou, T., Shen, J., Ren, Y., & Ji, S. (2021). Threshold Key Management Scheme for Blockchain-Based Intelligent Transportation Systems. *Security and Communication Networks*, 2021, 1–8. https://doi.org/10.1155/2021/1864514