International Journal of Digital Strategy, Governance, and Business Transformation
Volume 13 • Issue 1

# Port-to-Port Expedition Security Monitoring System Based on a Geographic Information System

Agung Mulyo Widodo, Universitas Esa Unggul, Indonesia
Riya Widayanti, Universitas Esa Unggul, Indonesia
Andika Wisnujati, Universitas Muhammadiyah Yogyakarta, Indonesia
https://orcid.org/0000-0001-6261-7936
Nizirwan Anwar, Universitas Esa Unggul, Indonesia
https://orcid.org/0000-0003-1189-9093
Shavi Bansal, Insights2Techinfo, India
Farhin Tabassum, Indian Institute of Technology, Kharagpur, India
Mosiur Rahaman, Asia University, Taiwan*

## ABSTRACT

Transportation companies operating both domestically and internationally are starting to worry about the safety of cargo freight. Utilizing a GIS-based port-to-port expedition safety monitoring system based on global information system is the appropriate way to handle the security and safety concerns in cargo assets because cargo crime is the largest difficulty facing supply chain companies. Reports will be sent in real time by the system to the central office via the data communication network. The application of tracking and traceability systems (tracking), dispatch (cargo loading and unloading), and access authority for cargo operations are the main topics of this study. Waterfall systems and system design using UML diagrams are the methods utilized in system development. This system employs GPS tracking technology with a digital lock for expedition operations where the position of the cargo dispatch, the location of the pick-up, and the open and closed status of each door container padlock during the field logistics' loading and unloading operations are all tracked in real time.

## KEYWORDS

Cargo, Digital Lock, Expedition Security Monitoring System

## INTRODUCTION

From the original warehouse to the port, goods transported in a pallet or container will travel via land, air, or sea. After the cargo arrives at the target port, it will be sent to the destination warehouse and eventually be delivered to the client. A cargo company is responsible for the delivery of goods from the initial warehouse to the port. Goods transported on pallets or containers will travel by land,

DOI: 10.4018/IJDSGBT.335897 *Corresponding Author

air, or sea. After the cargo arrives at the target port, it will be sent to the destination warehouse and finally delivered to the client (Stergiou et al., 2021; Wang et al., 2019). However, we need to realize that shipping cargo and assets requires a high level of security and safety because guaranteeing the assets in the shipping package is the responsibility of the logistics service provide(Akyuz, 2017; Progoulakis et al., 2021). Therefore, strategic decisions need to be taken to maintain the security and safety of assets during the journey from the origin location to the destination location by land, air, and sea (Ashraf et al., 2022). The issue of the security and safety of freight cargo has become a concern for transportation businesses both nationally and internationally. An international organization whose membership consists of three regions, namely America, Asia/Pacific, and Europe, has formed an association called TAPA (Transported Asset Protection Association) (Castro et al., 2020; Christensen et al., 2022). The aim is to combat cargo crime and create global standards that can be used in business and security agreements between buyers (shippers) and logistic service providers (LSPs). Cargo crime is the biggest challenge in the supply chain business. This challenge threatens valuable manufactured products, high-risk products, and logistics service providers (Casola et al., 2019). This motivates the author to conduct research that focuses on implementing monitoring and tracking systems, delivery (loading and unloading of cargo), and access authority into cargo operations.

Thus, this research has the following contributions:

- This research focuses on handling the security and safety issues of cargo assets by creating a system that uses a digital key system based on a geographic information system (GIS).
- The system will send reports via the data communication network to the head office in real time. This is conducted through the implementation of monitoring and tracking systems, dispatch (cargo loading and unloading), and access authority into cargo operations.
- The system uses a real-time GIS-based Digital Lock system by sending reports via a data communication network to the head office to address security and safety issues with cargo assets. An electronic padlock is installed on the container. This padlock will send location data that has been regulated by the system, where determining this location is a work order for picking up and dropping off cargo. Every logistics truck vehicle operator carrying the container must be equipped with an electronic padlock, and the operator must have an RFID card. This RFID is used to open and lock electronic padlocks by placing the RFID card on the surface of the padlock. Operators are only permitted to open containers in locations determined by the system as work orders. If RFID activity occurs to open electronic locks outside the work area, the system will send an alarm or warning that there has been a violation of loading and unloading activities in the field. Likewise, if, without RFID access, this electronic lock is opened either by force or automatically, the system will send an alarm as a sign that a violation with a high level of danger has occurred.

This paper is organized as follows. Part 1 discusses the facts of many cases of cargo theft crimes during the journey from the location of origin to the destination location, motivation, and the contribution of this research. Section 2 describes the related work used in this research. Section 3 explains how to develop a system to monitor cargo from the origin location, throughout the journey to the delivery destination. Section 4 explains the flow of application development results and testing, followed by discussion. Finally, the research conclusions are presented in section 5.

## RELATED WORK

The introduction of new threats affecting all architectural layers has resulted from the heterogeneity of involved technologies, including the integration of various resource-constrained devices and networks. This has urged the design and enforcement of appropriate security countermeasures, including effective monitoring capabilities. According to Ashraf (Ashraf et al., 2022) the study aims

to analyse the significance of marine cyber security by examining the various threats and assessing their potential impact and magnitude of losses. An examination is conducted on the susceptibility of the digital revolution with respect to the utilization of internet of things (IoT) devices (Almomani et al., 2021; ARYA et al., 2022; Sharma & Singh, 2022), contemporary security frameworks for ships, and sensors and devices employed in modern ships. Concurrently with the advancement, it is imperative to prioritize the management of human interactions. Hence, the incorporation of novel technology should encompass the involvement of humans, the user elements, and should prioritize the harmonious integration of Man, Technology, and Organization (MTO) (Fjørtoft & Berge, 2019).

According to Chircop (2016), there are particular risks for ships operating in the Arctic region due to bad weather, a lack of navigational information, and communication systems. It is reasonable to conclude that these hazards would significantly affect any potential SAR operations or operations necessary in the event of environmental contamination. The available information on the threats to the environment and public safety in the Arctic Ocean is utilized to suggest vessel traffic paths for TSR vessels that can lower such risks (Chircop, 2016). After conducting extensive interviews with representatives from twenty HoReCa enterprises and seven wholesale suppliers, it was determined that the ICT tool was positively welcomed and has the potential to enhance the efficiency and sustainability of their collaboration. According to the hypothesis, these industries possess considerable potential to include innovative solutions in order to enhance communication channels and promote sustainability in their logistics operations (Ceynowa et al., 2023). Information on the type, size, and duration of the ship's stay in port, as well as details about the last port, were recorded in the official maritime traffic records with stops in Funchal. Furthermore, a thorough literature search was carried out on NIS found in Madeira Island up till 2004 (Ekwall & Lantz, 2015).

The academic comprehension of risk, including the analysis of numerical data, identification of causes, and categorization, is inadequate for facilitating the prevention or control of risks (Tam & Jones, 2019). Risks are contingent of their surroundings and circumstances. Therefore, in order to avert or control risks, risk managers must comprehend them inside a comprehensive framework. In order to evaluate the appropriate level of security, it is necessary to take into account the significant interaction effects between the type of product and the location of the transit chain. More specifically, the danger of cargo theft is higher for certain types of products(Ekwall & Lantz, 2016, 2019). Safety can be defined as a level of risk that is deemed acceptable by society. To evaluate the current safety of ships, it is essential to measure the risk associated with the global fleet. Hot work, electric arcs, static electricity, and the accumulation of combustible gas in the cargo tank are identified as the primary causes of fire and explosion mishaps. The primary contributing causes are the infringement of work permits and a deficiency in risk analysis. To enhance fire prevention on ships, it is necessary to improve training standards and safety awareness, while also lessening the commercial constraints on ship operations (Uğurlu, 2016; Wu et al., 2020). This involves estimating and evaluating the main factors that contribute to risk, which are the frequency of maritime accidents and the severity of their repercussions. The current study was prompted by previous research conducted by Det Norske Veritas (DNV, 2006), which identified concerning indications of a deterioration in maritime safety standards (Eliopoulou et al., 2023).

Over the past decade, there has been a rise in the number of cruise ships and passengers in the Arctic, mirroring the overall growth of the worldwide cruise sector. Conversely, with the rise in activity in the region, the likelihood of environmental pollution in the area also increased. The presence of a delicate and unexplored ecology in the region amplifies the significance of this environmental pollution potential (KOLÇAK et al., 2022; Stevenson et al., 2019).

Based on mobile GIS, the TIKI Online program offers a number of main functions, including displaying package delivery status and cost information, agent information spread throughout Semarang City, and a list of agents closest to the user's location(Gupta et al., 2023; Khan, 2021). The research's final product is a mobile GIS-based TIKI Online application with a number of key features, including showing package delivery status and cost information, agent information dispersed

throughout Semarang, and a list of agents nearest to the user's position. However, the weakness of this system is that the GPS is installed on the vehicle carrying the container, so it cannot protect against theft of assets in the container. So, the right solution to overcome security and safety issues for cargo assets is to use a digital lock system(Gupta & Panigrahi, 2023; SINGH, 2021). The system will send reports in real-time via the data communication network to the head office. An electronic padlock is installed on the container. This padlock will send location data that has been set by the system, where determining this location is a work order for picking up and dropping off cargo. Every logistics truck vehicle operator carrying these containers must be equipped with an electronic padlock, and the operator must have an RFID card. This RFID card is used to open and lock electronic locks by placing the RFID card on the surface of the electronic lock. Operators are only permitted to open containers at locations determined by the system as work orders. If RFID activity occurs when opening an electronic lock outside the work area, the system will send an alarm or warning that there has been a violation of loading and unloading activities in the field. Likewise, if, without RFID access, this electronic lock is opened either by force or automatically, the system will send an alarm as a sign that a high-level violation has occurred.

## PROPOSED METHOD

The first stage of research implementation was observation of goods sending companies. From the observations made, the mapping of the facts that occurred using a fishbone diagram was carried out to reveal the problems that occurred. Apart from that, information was also obtained regarding ongoing business processes at companies providing goods delivery services, which currently refers to the export and import business processes at Tanjung Priok Port, where forwarder agents start their transportation activities from there. The two things mentioned above can be explained below.

From the fishbone diagram, there are six main problems, namely:

a. **Regulations**: By completing the export/import documents, it is not certain that the cargo will be able to leave the port directly. This is due to the following checks:
   - **Customs and Excise**: Customs and Excise must check the type and contents of the cargo.
   - **Red Line Cargo Category**: If the contents of the cargo include prohibited items, customs will inspect the contents and carry out quarantine.
   - **Green Line Cargo Category**: if the contents of the cargo and documents are included in the non-dangerous or prohibited goods category, then customs can grant permission to exit the port smoothly.

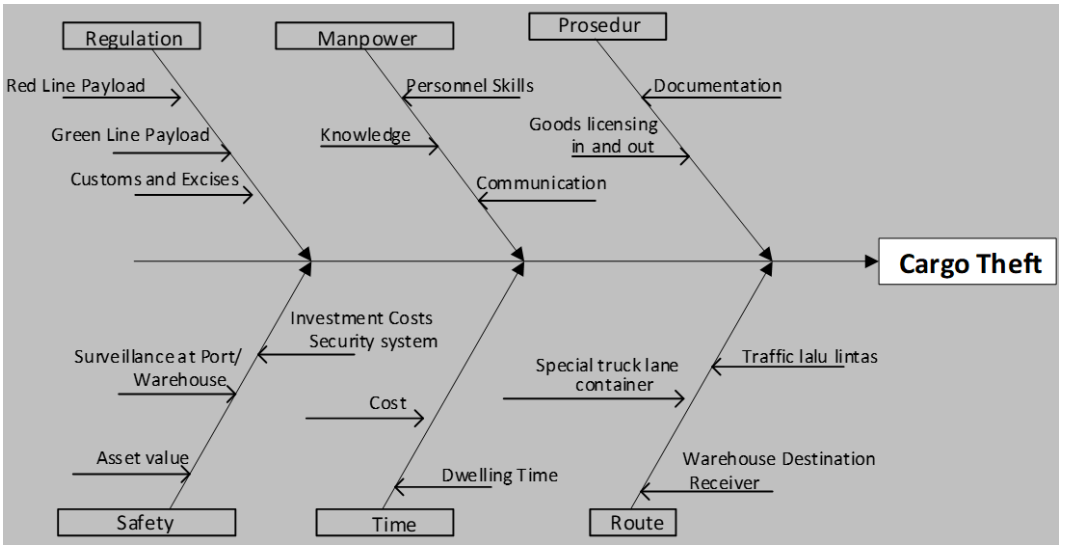
b. **Manpower**: There are three factors that cause the problem of cargo theft:
   - **Personnel Skills**: Container transport operators are very reliable when the cargo is already on its way to its destination because technical problems on the way can only be resolved with the technical skills of the container truck operator. If you lack expertise, the cargo you carry is at risk of theft or asset damage.
   - **Knowledge**: Apart from expertise, good knowledge of documents and assets is also required.
   - **Communication**: With the current communication technology, this does not mean that cargo is transported safely because there could be fraud committed by container truck operators and freight forwarders(Jain & Gupta, 2019; Mahmood et al., 2022).

c. **Procedure**: The cause of cargo theft could also be procedural irregularities.

d. **Security**: The high cost of security investments and the absence of insurance can create opportunities for criminal activity.

e. **Time**: The waiting period for export-import permits and documents is known as dwelling time. This results in a build-up of cargo at the container yard because licensing problems have to be resolved. In this condition, cargo security has the potential to become a target for theft operations.

**Figure 1. Fishbone analysis of the causes of cargo theft**




f. **Route**: In the case of heavy equipment loads passing between cities and provinces, it results in road damage, so the transportation service directs heavy equipment routes at certain times and certain routes. This is a potential easy target for asset theft when passing through areas with minimal telecommunications infrastructure.

Next, the export/import freight forwarding business process on going can be explained in Fig 2 below. The shipper is the party sending the goods. While the consignee is the party receiving the goods. LCL (less than container loaded) is a type of partial delivery of goods where goods sent by the shipper are first collected in the shipping agent's stacking warehouse(Zou et al., 2019). Then, the agent will collect the goods until they meet the quota for loading them into the container. FCL (full container loaded) is a type of delivery of goods using containers. In this way, the container must be brought to the warehouse for the stuffing process. After being loaded, the container is sealed and sent to the container storage area at the port(Gupta et al., 2023; Gupta & Panigrahi, 2023).

Based on observations of freight forwarder agents, they basically have the following duties and responsibilities:

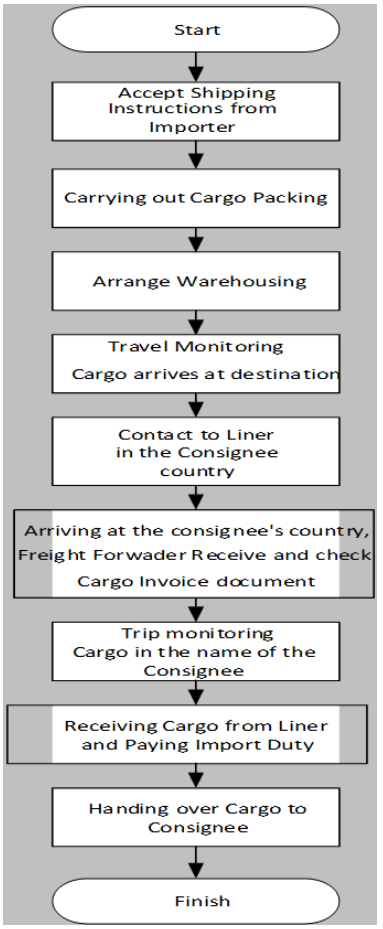
Acting on behalf of the shipper

i. Freight Forwarder The agent monitors cargo travel on behalf of the shipper by selecting the right route and mode of transportation.
ii. Pack the cargo according to the cargo's destination route.
iii. Arrange warehousing for cargo before loading and unloading.
iv. Monitor the cargo until it arrives at its destination by contacting the consignee agent (recipient).

Acting on behalf of the cosigner.

i. Monitor cargo travel on behalf of the consignee.
ii. Hand over the cargo to the consignee.

**Figure 2. Export/import freight forwarding business process ongoing**
*Source: Tanjung Priok Harbor (2018)*




In this study, the waterfall method—a work approach that emphasizes sequential and systematic phases—is applied to software development. In the following, it is explained the steps of the water which is used.

## Requirement Analysis

Based on the results of the observations, the requirements needed for system development were obtained, which consist of the following items:

### *Functional Requirements*

1. **Dispatcher**
   i. Login and Logout: Login as a Monitoring Officer and Logout when exiting the application.
   ii. Scheduling data entry and performing job assignments: Assigning work to operators for available transportation units, assigning fleets to loading pools and warehouse destinations.
   iii. Distribution monitoring: Real time monitoring of asset journeys on the dashboard
   iv. Reporting: produces operational monitoring reports

2. **Operator**
    i. Login and Logout: Login as a Truck Operator on the tracking device before starting the unit and Logout when finished working.
    ii. Update Status: Operators can report activity status at the start of the shift, during operations and at the end of the shift.
    iii. RFID Scan: Reads RFID to open the Digital Lock on the Container
3. **Management Team**
    i. Open the monitoring dashboard via the web application.
    ii. Retrieves reports based on required filters from the web application.

### *Non-Functional Requirements*

1. **Information Technology**
    i. This information system uses GIS technology for tracking and GSM for data communication and RFID for asset data collection.
2. **Performance**
    i. The system works in real time during operational work periods, for example 12 hours or 24 hours.
3. **Information**
    i. The information received by the system is accurate, timely and relevant.
4. **Usability**
    i. The system user interface on the dispatcher side is a dashboard monitor on the operator side is simple and has little interaction to avoid being out of focus while driving.

## Software Design

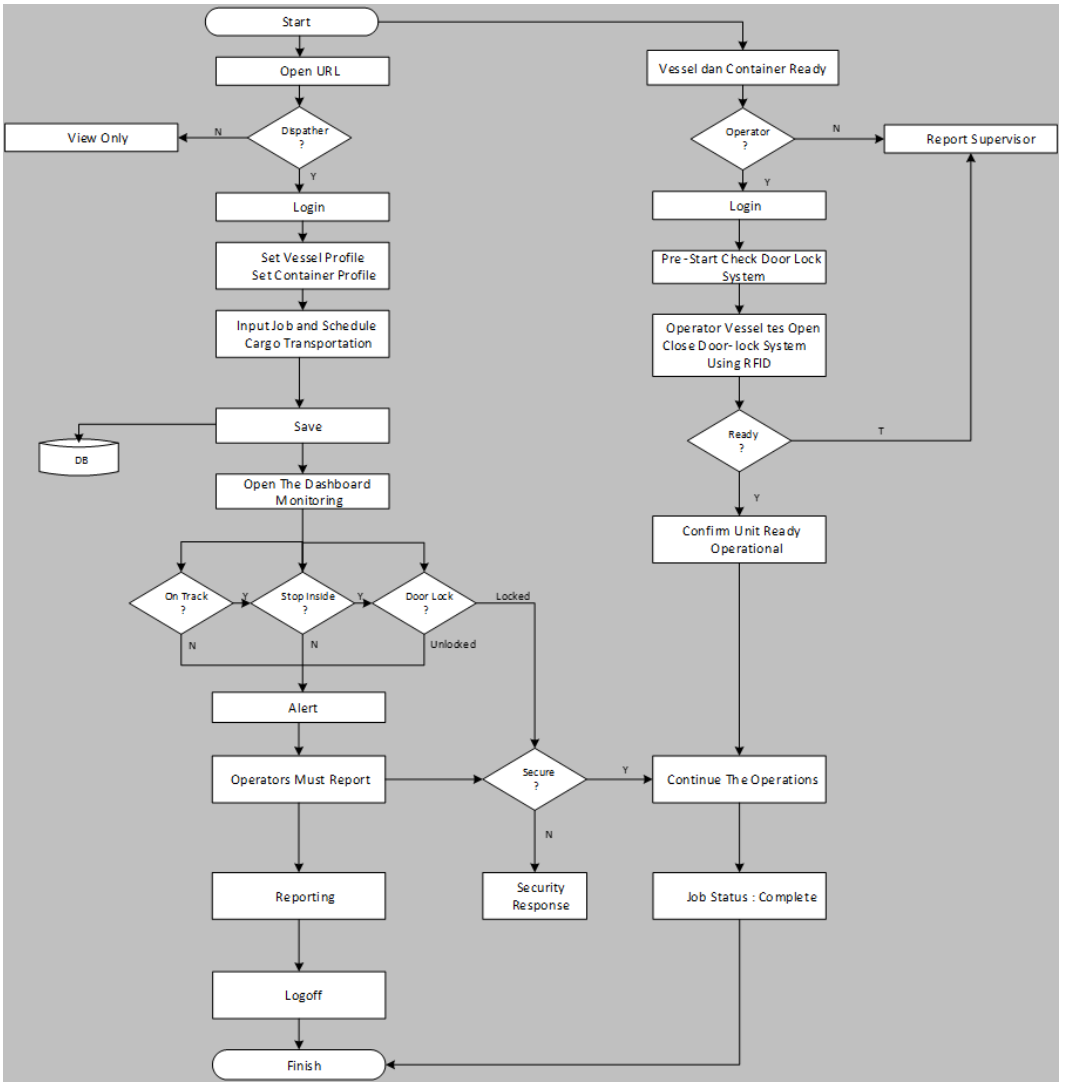
### *Process Design*

The next stage is to design the process as depicted in Fig 3. Proposed use case diagram and activity diagram Fig 4. and Fig 5., respectively. The dispatcher logs into the Monitoring System Application, selects Resources including Operator, Truck and Container which are then determined in the Resource Assignment. Then the dispatcher selects the job, where the system has received information on the cargo freight forwarding operational plan. Among other things, the loading location is the initial place for pick-up container cargo, and the target destination is the destination of the container cargo, which is then determined in the job assignment.

Operators receive assignment information through the system (Tam & Jones, 2019). Operators log in to the mobile device to start activities and provide activity status updates. Operators run truck and container units according to the destination location specified in the job assignment. The dispatcher opens the monitoring view, which is displayed on the monitoring screen. In addition, create a report to obtain a report on operational monitoring results management teams, such as level managers, can monitor operations in real time from their respective desktops and filter reports as needed (Christensen et al., 2022).

The activity begins when the dispatcher carries out a job assignment for the operator by appointing a specified fleet of trucks and containers. Then, the dispatcher determines the initial location and destination of the trip that will be taken during freight forwarder operations. After the job assignment is completed, the operator who is on standby in the fleet pool gets job information and goes to the fleet unit that has been assigned. In the unit cabin, the operator logs in on the mobile device to activate the work. The specified activity has been taken and is ready to be carried out by the designated operator. The status of the activity must also be confirmed by the operator. Next, the operator confirms the RFID on the Digital Lock device installed on the container before the unit operates. And it ensures that the initial GPS coordinates are at

**Figure 3. Proposed process design**




the location of the departure point; in this case, the system has set a geofence boundary on the map so that the tracking device can recognize the coordinates of the unit's starting point. When the unit is running, the dispatcher and team management can carry out real-time monitoring from the head office or branch office. This operational tracking and asset security report can be downloaded from the web portal by filtering.

## DATABASE DESIGN

Database design was carried out using nine entities whose interrelationships are depicted in Figure 4.

**Figure 4. Use case diagram**

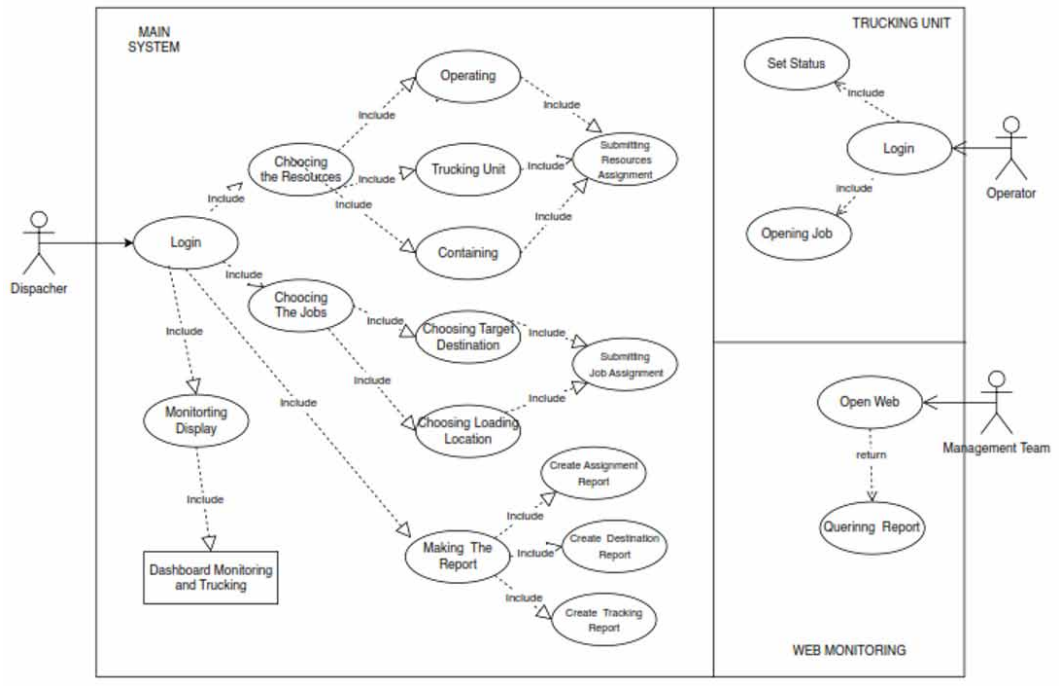
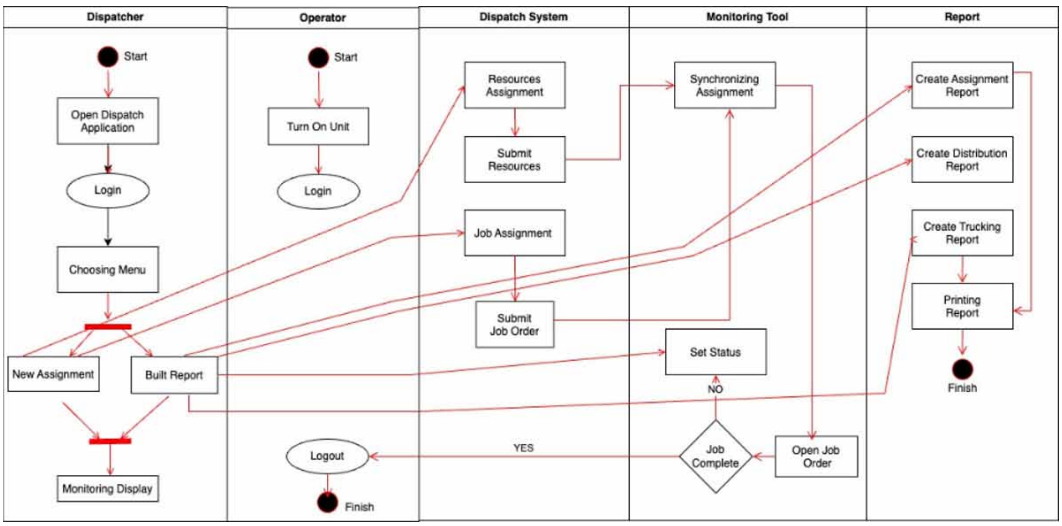


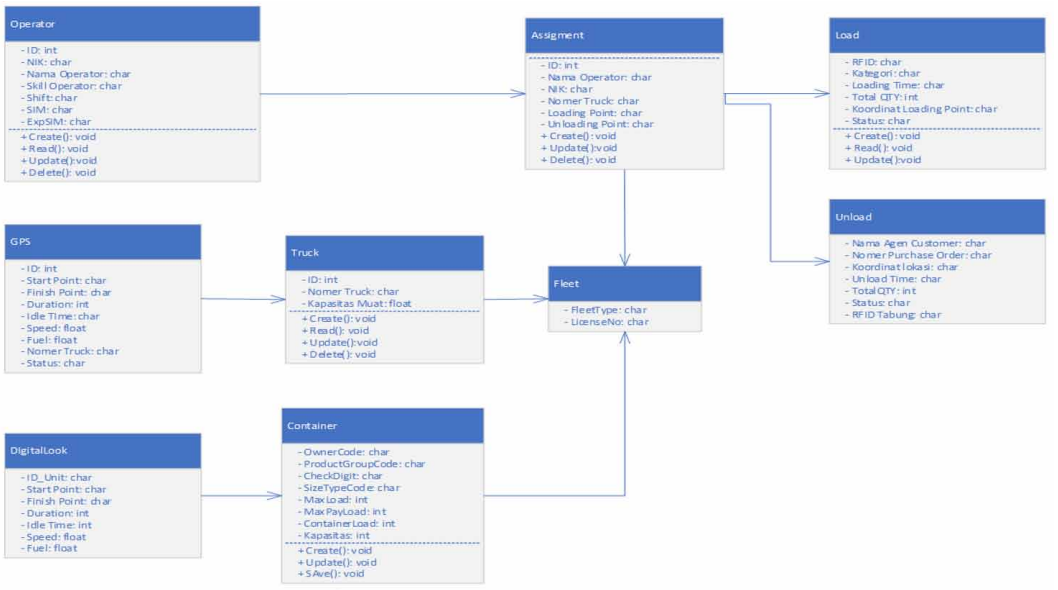

**Figure 5. Activity diagram**




## INTERFACE DESIGN

Interface design here is the design of interface sub-systems between humans and machines. Interface design here is the design of the interface subsystem between humans and machines. In this sub-system, nine interface forms are created, namely:

**Figure 6. Class diagram**




1. Operator Data Form
2. Truck Specification Form
3. Container Specification Form
4. Job Assignment Form
5. Monitoring Dashboard Display
6. Map View

## Hardware

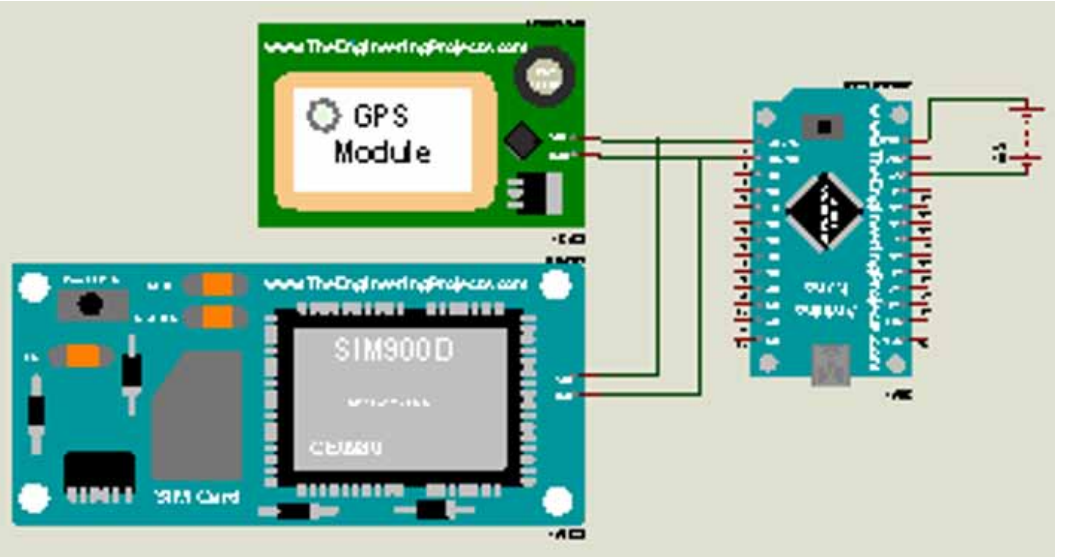
The design consists of the hardware used in the system, along with its connectivity. The hardware design can be seen in Fig. 7. In this research, trucks as a means of transporting cargo can be replaced with any moving vehicle, they must be equipped with the following hardware:

a. GPS Locator
b. GSM phone connected to monitoring center.
c. Silent panic button
d. Automatic door lock system
e. Alarm connected to monitoring center Alarm in case tractor and trailer are separated.
f. GPS navigation system with geofencing functionality

Meanwhile, the trailer must be equipped with the following hardware:

a. Trailer ID in reflective figure of roof
b. GPS locator
c. Door sensors connected to monitoring center
d. 4-pneumatic door locks
e. Lock-down system

**Figure 7. IoT digital lock device**




f. Reinforced trailer doors
g. Electronic Lock
h. RFID Cards

The software used for this system is:

a. Digital Lock System Software
b. Google Chrome: to display map tracking from the system

## Implementation

This monitoring system will be built using:

### *IoT Devices*

a. Option 1: Arduino Uno R2
b. Option 2: Raspberry PI
c. Python 56
d. MySQL Databases

### *Monitoring System Dashboard*

This web-based application will be built with JAVA.

### *Client Interface*

On the client side, where the application is accessed by operators, shippers and consignees can use smartphones which can be opened with a web browser.

### Testing

System testing will use the following methods:

#### *Hardware Testing*

IoT (Internet of Thing) devices will be carried out by first assembling them partially, that is, they are not integrated with the application. The goal is to ensure the tool functions properly.

#### *Software Testing*

After the hardware is proven to work normally, it is then connected to the application to carry out system testing.

#### *Black Box Testing*

Black box testing can be done when the infrastructure is created and then without looking at the content, testing is carried out to ensure the infrastructure is functioning well.

## RESULT AND DISCUSSION

The results of the implementation of the design carried out can be seen in Figs. 8-12. This form contains the attributes:

- No. Operator ID
- Operator name
- Operator position
- Skill level
- Driving license
- Driving license validity period
- Operator gender

Furthermore, the form for the vehicle for transport and can be seen in Fig. 8. and Fig, 13. This form contains the attributes:

- Truck ID contains the truck number registered with the company.
- The police number contains no. trucks registered with the Republic of Indonesia Police Institution.
- Brand is the vehicle brand.
- Unit Type is the type of transport vehicle.
- Owner is the owner of the vehicle.
- Unit Status is the status of the vendor's vehicle, whether owned or leased.

The Container Specification Form interface consists of the following attributes:

- Owner code
- Product group code
- Registration number
- Check digits.
- Size and type code
- Maximum Load
- Carrying load
- Container load
- Cubic capacity

**Figure 8. Operator data form interface**

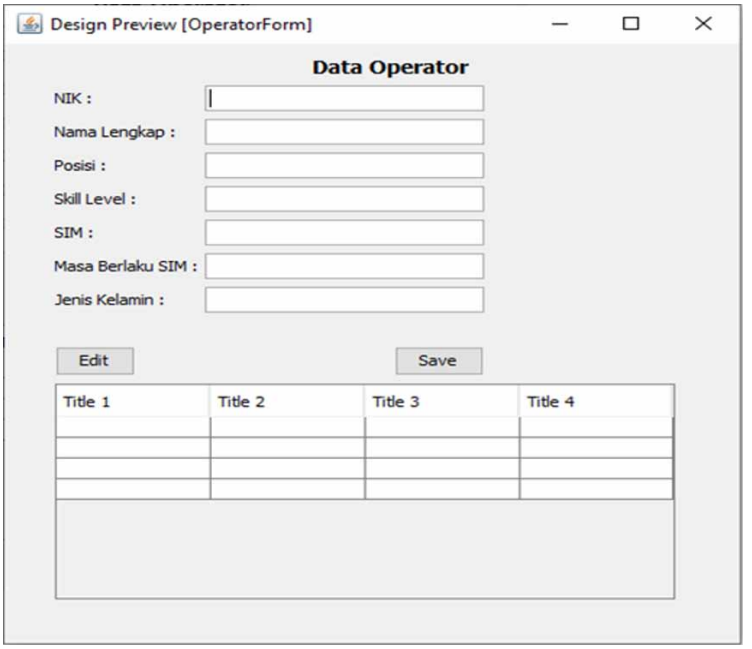
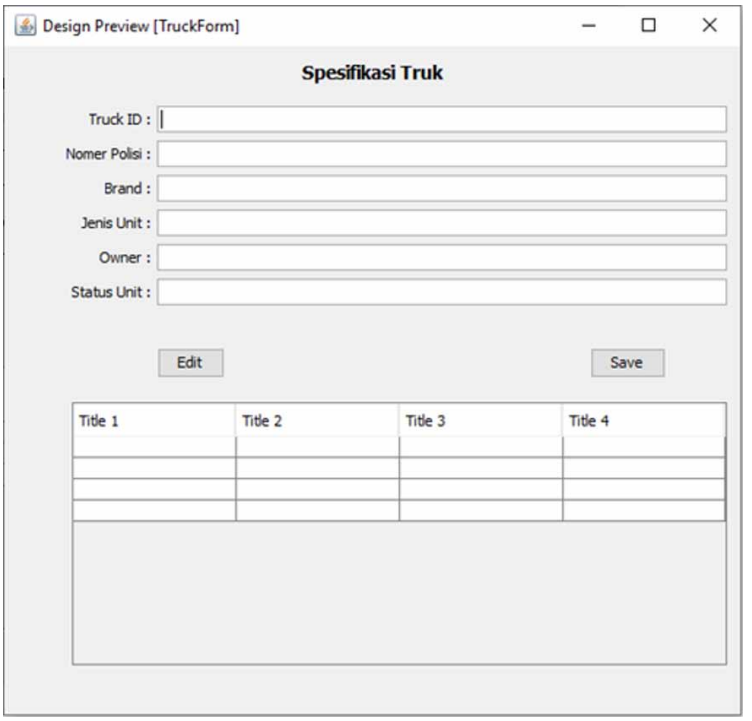



**Figure 9. Truck specification form interface**



The Job Assignment Form interface for dividing cargo transportation work can be seen in Fig. 10.

Monitoring of the position of the cargo transport vehicle and the position of the cargo can be observed on the Dashboard Monitoring and Map Interface forms. Each interface form can be seen in Figure 11 and Figure 12.

Meanwhile, the hardware made can be seen in Fig 14.

Based on the results of black box testing, it can be seen in Table 1 for the Monitoring System application. All tests have a successful status.

Scenario monitoring system application testing is carried out starting with the application connection to the database server, where the test results are obtained. The client server application can connect to the MySQL database server. Next, the dispatcher logs into the application and the test results are obtained. The dispatcher officer can enter the application. When the system performs a job assignment, the results obtained are that the application can access operator, truck, container data and create job tickets. Finally, when testing the operator logging into the application, the results obtained were that the operator knew there was a job assignment and logged in. Next, testing was carried out on the IoT-Digital Lock device through the stage of creating a connection between the DigitalLock and the PC Server. Tests were carried out on the Arduino Board device, SIM808 GPS/GPRS Module, RC522 RFID Module, Solenoid Push Pull device, and IoT Digital Lock device, the respective test results can be seen in Tables 2, 3, 4, 5, and 6.

GPS calibration is carried out, with the result that the GPS location matches the point of existence. The next stage is to carry out data communication with the SIMCard and the results obtained can be sent and received messages. Finally, when the system performs an RFID scan to open the lock, the result is that the lock can be opened by an RFID scan.

**Figure 10. Container specification form interface**

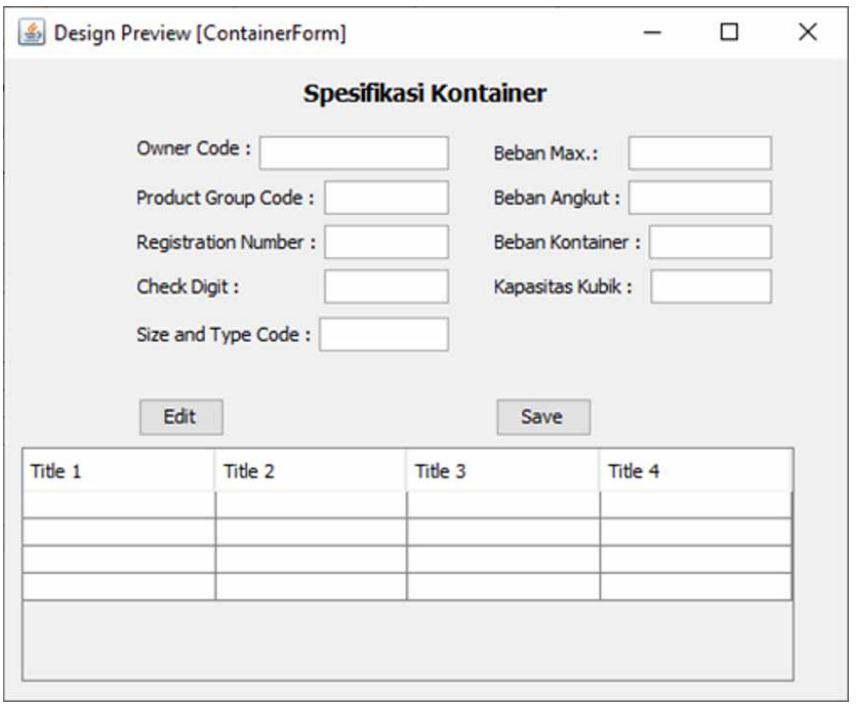


**Figure 11. Job assignment form interface**

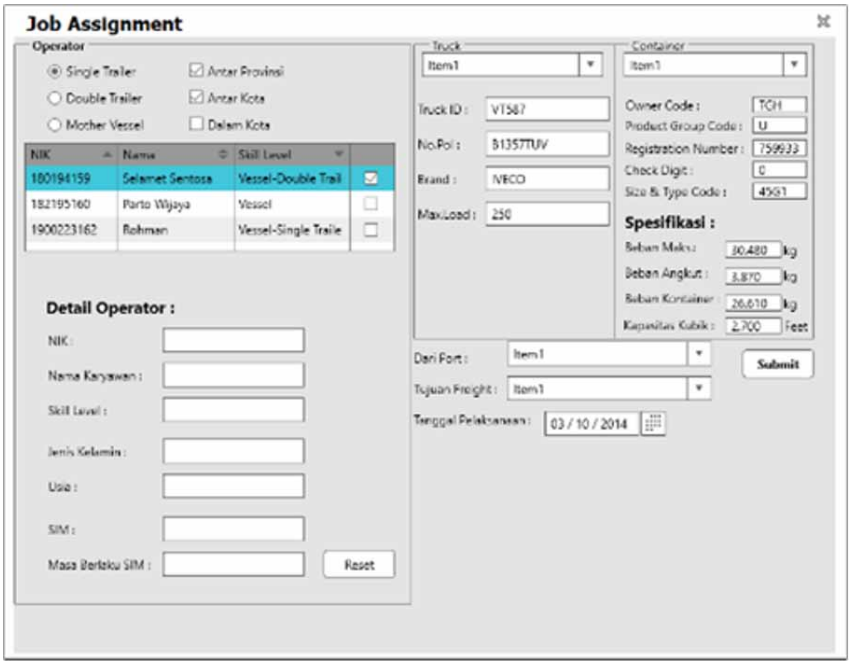



**Figure 12. Job assignment form interface**

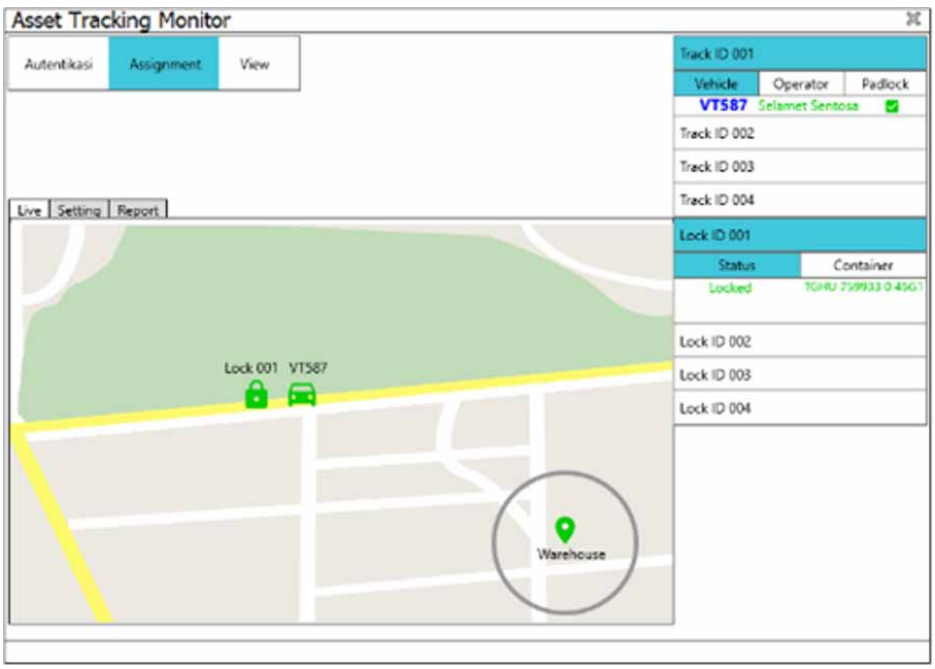


**Figure 13. Job assignment form interface**

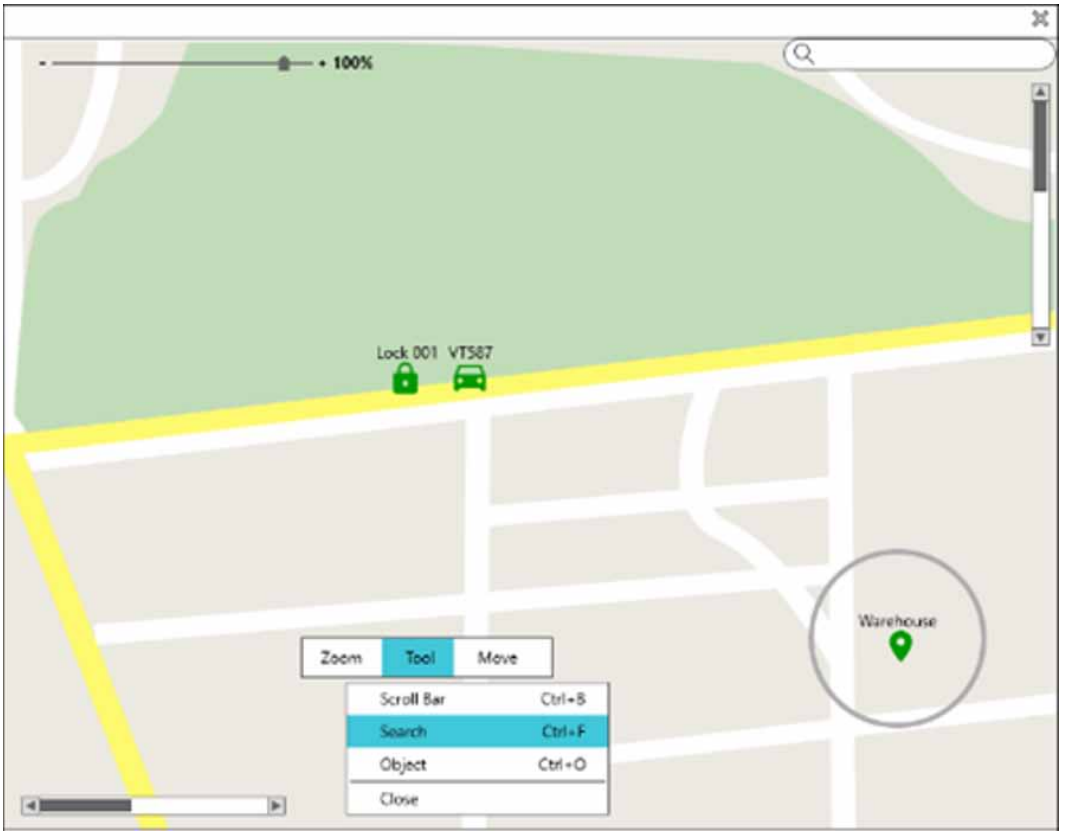



**Figure 14. Job assignment form interface**

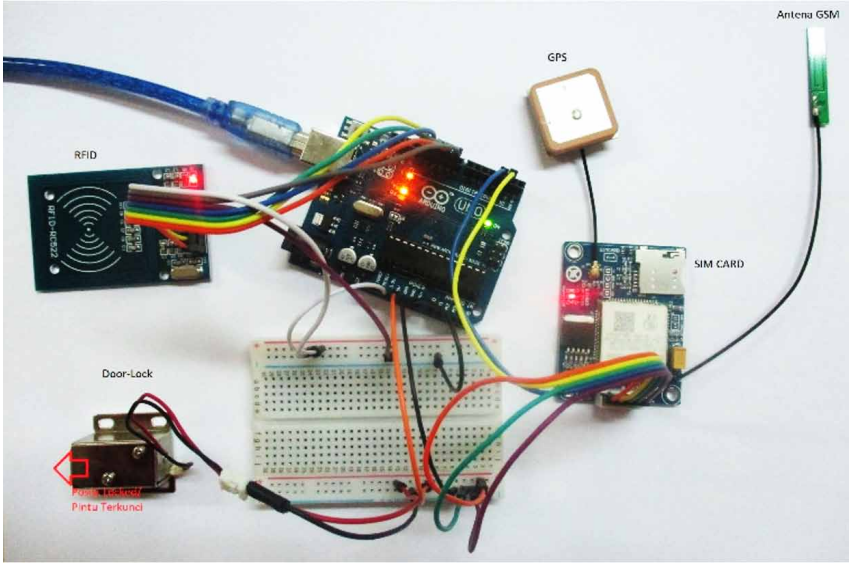


**Table 1. Monitoring system application test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | Application Connection to Database Server | The client server application can connect to the MySQL database server | Successful |
| 2 | Dispatcher logs into the application | Dispatcher officers can log into the application | Successful |
| 3 | Carrying out job assignments | The application can access Operator, Truck, Container data and create job tickets | Successful |
| 4 | Operator Data Entry | The dispatcher fills in the operator's detailed data | Successful |

**Table 2. Arduino board device test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | Arduino Power Test | LED power indicator response | Successful |
| 2 | Arduino connection test | Response on the terminal when inputting a command | Successful |
| 3 | Check Communication Port Status | Port Status is working properly | Successful |
| 4 | Upload the program to Arduino | Programs can be received by Arduino via the COM port | Successful |
| 5 | Arduino RX and TX test | Response on the terminal when inputting a command | Successful |

**Table 3. SIM808 GPS/GPRS module test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | 5V module power test | Module LED power indicator response | Successful |
| 2 | Module connection test | Response on terminal | Successful |
| 3 | Upload programs | The program can be accepted by SIM808 module | Successful |
| 4 | Check GPS Status | GPS Status Info | Successful |
| 5 | Check GPS coordinate status | Location coordinates information | Successful |

**Table 4. RC522 RFID module test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | 3.3V module power test | Module LED power indicator response | Successful |
| 2 | Upload RFID program | The program can receive RFID modules | Successful |
| 3 | RFID Card Read Test | Card ID number read | Successful |
| 4 | RFID Tag Read Test | The tag ID number is read | Successful |
| 5 | RFID Card Personal Data Write Test | Personal Data can be updated | Successful |

**Table 5. Push pull solenoid device test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | Upload the Solenoid program into Arduino | The program can be accepted by Arduino | Successful |
| 2 | Push Pull Solenoid Test | Push/Pull Solenoid Response | Successful |

**Table 6. IoT digital lock device test results**

| No | Testing Scenarios | Expected Results | Test Result |
|---|---|---|---|
| 1 | Make a connection between DigitalLock and the PC Server | The device and PC Server can be connected | Successful |
| 2 | Perform GPS calibration | GPS location corresponds to the point of existence | Successful |

## CONCLUSION

In logistics transportation, truck ships are usually the only ships that use tracking. However, the loading and unloading operations from inside the container are not tracked by the system in real time because the container body which stores the valuable goods is not equipped with a security system, thus allowing the theft of assets from the container to occur. This system was created as a proposed Internet of Things-based technology solution in the logistics transportation sector to monitor the movement of assets from origin to destination in real time, integrated with GPS. To track asset movements in real time from the point of origin to the point of destination, this system was developed as an Internet of Things-based technology solution that is recommended for the logistics and transportation industry. It is integrated with GPS. In order to obtain something better, in the future, the hardware can be developed to be even more optimal; for example, devices with a resistance index of IP67 can be used, which means they can withstand all installation and operating situations. hybrid communications network that uses GSM and VHF radio bands. As a result, operational costs for data packages can be reduced. Apart from that, when the truck unit is on the way, it is necessary to make the monitoring equipment packaging that is strong against shocks and resistant to weather.

## REFERENCES

Akyuz, E. (2017). A marine accident analysing model to evaluate potential operational causes in cargo ships. *Safety Science*, *92*, 17–25. doi:10.1016/j.ssci.2016.09.010

Almomani, A., Al-Nawasrah, A., Alomoush, W., Al-Abweh, M., Alrosan, A., & Gupta, B. B. (2021). Information Management and IoT Technology for Safety and Security of Smart Home and Farm Systems. *Journal of Global Information Management*, *29*(6), 1–23. doi:10.4018/JGIM.20211101.oa21

Arya, V., Almomani, A., & Han, C. (2022). Analysis of Quantum Computing-Based security of Internet of Things(IoT) Environment. *Insights2Tecinfo*.

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1–14. doi:10.1109/TITS.2022.3164678

Casola, V., De Benedictis, A., Riccio, A., Rivera, D., Mallouli, W., & de Oca, E. M. (2019). A security monitoring system for internet of things. *Internet of Things : Engineering Cyber Physical Human Systems*, *7*, 100080. doi:10.1016/j.iot.2019.100080

Castro, N., Ramalhosa, P., Jiménez, J., Costa, J. L., Gestoso, I., & Canning-Clode, J. (2020). Exploring marine invasions connectivity in a NE Atlantic Island through the lens of historical maritime traffic patterns. *Regional Studies in Marine Science*, *37*, 101333. doi:10.1016/j.rsma.2020.101333

Ceynowa, W., Przybylowski, A., Wojtasik, P., & Ciskowski, Ł. (2023). ICT Adoption for Sustainable Logistics Development in the HoReCa and Wholesale Sectors. *Sustainability (Basel)*, *15*(4), 3746. doi:10.3390/su15043746

Chircop, A. (2016). Sustainable Arctic Shipping: Are Current International Rules for Polar Shipping Sufficient? *Journal of Ocean Technology*, 11.

Christensen, M., Georgati, M., & Arsanjani, J. J. (2022). A risk-based approach for determining the future potential of commercial shipping in the Arctic. *Journal of Marine Engineering & Technology*, *21*(2), 82–99. doi:10.1080/20464177.2019.1672419

Ekwall, D., & Lantz, B. (2015). Cargo theft at non-secure parking locations. *International Journal of Retail & Distribution Management*, *43*(3), 204–220. doi:10.1108/IJRDM-06-2013-0131

Ekwall, D., & Lantz, B. (2016). Supply Chain Risk Analysis and Assessment: Cargo Theft. *Transportation Journal*, *55*(4), 400–419. doi:10.5325/transportationj.55.4.0400

Ekwall, D., & Lantz, B. (2019). The moderating role of transport chain location in cargo theft risk. *The TQM Journal*, *32*(5), 1003–1019. doi:10.1108/TQM-01-2019-0025

Eliopoulou, E., Alissafaki, A., & Papanikolaou, A. (2023). Statistical Analysis of Accidents and Review of Safety Level of Passenger Ships. *Journal of Marine Science and Engineering*, *11*(2), 410. doi:10.3390/jmse11020410

Fjørtoft, K., & Berge, S. P. (2019). ICT for Sustainable Shipping. In *Sustainable Shipping* (pp. 137–166). Springer International Publishing. doi:10.1007/978-3-030-04330-8_4

Gupta, B. B., Gaurav, A., Panigrahi, P. K., & Arya, V. (2023). Analysis of cutting-edge technologies for enterprise information system and management. *Enterprise Information Systems*, *17*(11), 2197406. Advance online publication. doi:10.1080/17517575.2023.2197406

Gupta, B. B., & Panigrahi, P. K. (2023). Analysis of the Role of Global Information Management in Advanced Decision Support Systems (DSS) for Sustainable Development. *Journal of Global Information Management*, *31*(2), 1–13. doi:10.4018/JGIM.320185

Jain, A. K., & Gupta, B. B. (2019). A machine learning based approach for phishing detection using hyperlinks information. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 2015–2028. doi:10.1007/s12652-018-0798-z

Khan, A. (2021). All about Geographic Information System (GIS). *Insights2Tecinfo*.

Kolçak, İ. Ç., Çetín, O., & Saka, M. (2022). Environmental Impact of Cruise Shipping in Arctic Region. *International Journal of Environment and Geoinformatics*, *9*(1), 1–10. doi:10.30897/ijegeo.957262

Mahmood, F., Zeeshan Khan, F., Ahmed, M., Ahmad, I., & Gupta, B. B. (2022). GreenCloudNet++: Simulation framework for energy efficient and secure, green job scheduling in geographically distributed data centers. *Transactions on Emerging Telecommunications Technologies*, *33*(4), e4232. Advance online publication. doi:10.1002/ett.4232

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. doi:10.3390/jmse9121384

Sharma, S., & Singh, S. K. (2022). IoT and its uses in Security Surveillance. *Insights2Tecinfo*.

Singh, D. (2021). Captcha Improvement: Security from DDoS Attack. *Insights2Tecinfo*.

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2021). InFeMo: Flexible Big Data Management Through a Federated Cloud System. *ACM Transactions on Internet Technology*, *22*(2), 1–22. Advance online publication. doi:10.1145/3426972

Stevenson, T. C., Davies, J., Huntington, H. P., & Sheard, W. (2019). An examination of trans-Arctic vessel routing in the Central Arctic Ocean. *Marine Policy*, *100*, 83–89. doi:10.1016/j.marpol.2018.11.031

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. doi:10.1007/s13437-019-00162-2

Uğurlu, Ö. (2016). Analysis of fire and explosion accidents occurring in tankers transporting hazardous cargoes. *International Journal of Industrial Ergonomics*, *55*, 1–11. doi:10.1016/j.ergon.2016.06.006

Wang, L., Li, L., Li, J., Li, J., Gupta, B. B., & Liu, X. (2019). Compressive Sensing of Medical Images With Confidentially Homomorphic Aggregations. *IEEE Internet of Things Journal*, *6*(2), 1402–1409. doi:10.1109/JIOT.2018.2844727

Wu, X., Zhang, L., & Luo, M. (2020). Discerning sustainability approaches in shipping. *Environment, Development and Sustainability*, *22*(6), 5169–5184. doi:10.1007/s10668-019-00419-z

Zou, L., Sun, J., Gao, M., Wan, W., & Gupta, B. B. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. *Multimedia Tools and Applications*, *78*(7), 7965–7980. doi:10.1007/s11042-018-6444-0

*Agung Mulyo Widodo received his PhD degree in Computer Science and Information Engineering, Asia University, Taiwan, and works as lecturer at Universitas Esa Unggul, Indonesia. His previous projects were with Caltex Pacific Indonesia, Siemens Telecommunications, and Nokia Siemens Networks (NSN). Currently, his research focuses on artificial intelligence, data science, and wireless communication technologies, including NOMA, OMA, NB-IoT, back-scattering systems, cognitive radio, artificial intelligence, and information security.*

*Riya Widayanti, as a lecturer at the University of Esa Unggul's Information Systems Study Program. My research fields have been data science, information systems audit and IT governance. My last project was to do an assessment in the ministry of PANRB RI.*

*Andika Wisnujati received the B.S. and M.S degree in Mechanical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia in 2008 and 2014. He is also received the Ph.D degree in Computer Science and Information Engineering, Asia University, Taiwan in 2023. He had been the Assistant Professor in Department of Automotive Engineering Technology, Universitas Muhammadiyah Yogyakarta, Indonesia since 2012. His research interests include Artificial Intelligence and Material Science. His previous research includes Neural Network and Automatic Control in Antilock Braking System and Grey Prediction Model in Welding Distortion.*

*Mosiur Rahaman received the Bachelor of Technology degree and the Master of Technology degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, India. He received subsequently Master of Business administration (M.B.A) degree in Human Resource Management with IT (HRM-IT) from Osmania University, India. He is currently pursuing a Ph.D. degree in Computer Science and Information Engineering department at Asia University, Taichung, Taiwan. He is serving as a lecturer College of Humanities and Social Science Department, Asia University Taiwan from 2020. From 2014 to 2015, he was a assistant professor in the Dept. of Computer Science and Engineering at the Royal Institute of Technology and Science, India. His research interests include Information Security, Blockchain, and Artificial Intelligence, IoT Security, Supply chain, Food Safety. He is also working as program manager and assisting with ASEAN and South Asian Countries - AI R&D Elite Class/ Doctoral Class. He worked and cooperated with various R&D projects under MOST, Taiwan. He is also serving as a Session Chairs for FICT 2021, FICT 2022, General Chair for ICRAMLET22, International A.M in MIMSE23.*