DockChain: An IoT-based Approach to Port Security and Optimization

Shwetanshu Chakraborthy
Maritime Cybersecurity
UNCW
Wilmington, NC, USA
chashwet@ad.unc.edu

Aadarsh Jena
Maritime Cybersecurity
UNCW
Wilmington, NC, USA
aadarsh.jena2008@gmail.com

Leon Baiye
Maritime Cybersecurity
UNCW
Wilmington, NC, USA
leon032020@gmail.com

Taizhe Zhu
Maritime Cybersecurity
UNCW
Wilmington, NC, USA
zhutaizhe@gmail.com

***Abstract*—Port operations are severely hindered by outdated systems and a lack of interconnectivity, increasing wait times for cargo pickup and dropoff. Wait times create significant opportunity costs for ports, shipping companies, and the global cargo industry. This project aimed to reduce port wait times and their economic impact, utilized Arduino hardware components, Internet-of-Things connectivity, and a three-tier architecture web application to develop DockChain, an integrated port security system. Hardware consisted of two Arduino UNO R4 WiFi boards and other components. The proposed application is built upon the Python Django module and standard web development languages. The application communicates with Arduino hardware at port entrance/exit terminals and at cargo ports utilizing HTTP requests. Visitor information is pre-recorded within a personalized web interface and securely compared with component data to verify identities, while logistics are tracked with a MySQL database to coordinate streamlined dropoff and pickup at cargo bays. DockChain is expected to reduce wait times by 5 – 10 minutes per cargo operation, increasing efficiency and expanding economic opportunities at ports.**

***Index Terms*—Smart and Intelligent Systems, Autonomous Shipping Operations, IoT-Based Port Security, Online Cargo Services**

I. Introduction

Inefficiencies in maritime port logistical systems - especially in Commercial Motor Vehicle (CMV) scheduling - have delayed operations and damaged the reliability of shipment, causing billion-dollar losses in revenue annually [17]. These disruptions undermine the core objective of commercial operations: to maximize profits. Thus, the operations of any such business must be optimized in a way that each individual task is completed in the most efficient way possible. At global scales, any inefficiency in business is analogous to lost revenue, customers, and more. This is nowhere more apparent than in the global shipping & cargo transport industry, where Commercial Motor Vehicles such as semi-trucks spend excessive amounts of time waiting and idling at ports to carry out cargo pick-up and drop-off jobs. [2]. Major global ports reported increasing wait times in 2025, with congestion at select ports nearly 300% higher than the historical average [11]. As waiting times increase, shipping corporations face greater losses, the environment sees rising idling-based pollution, and the $14 trillion global shipping industry encounters greater inefficiency [12].

Various factors contribute to the rising wait times at shipping ports. Chief among them are the disjointed communications between port administrators and commercial vehicle operators, as well as inefficient analog security systems. In the United States, most small to mid-sized ports operate on a first-come, first-served basis for arriving CMVs [13], and port authorities often do not receive details about CMV arrival time, necessary cargo for the job, and the status of the job (pick-up, drop-off, or both) until CMVs reach port entrances [14]. Next, security systems at port gates often consist of three steps: identity verification, potential cargo scanning, and a check-in system for cargo. Across many American ports, these steps have to be completed manually by port security officers, contributing to further increased wait times. The National Planning Guide for Port Security Operations mentions minimal automation and technology when implementing port security measures. Instead, reliance on port personnel and senior management is encouraged [15]. Both of these factors actively detriment cargo transactions and processing times in ports across the country, and the novel solution outlined in this paper will target both factors to optimize driver check-in and cargo operations.

Hypothesis: An IoT-driven port security and check-in system—utilizing biometric data, license plate recognition, and a universal online platform—will decrease wait and turnaround times for CMVs at marine ports.

A. Motivation

The impact of shipping on the day-to-day lives of people is clear. Following the 2021 blockage of the Suez Canal that cost $89 million to the Maersk shipping company, people all around the world felt the effects of the supply chain shortage caused [16]. This was an extreme case of supply chain blockage, but such delays in cargo transportation take place every day in small but compounding amounts, with truck congestion at ports. At the Port of Wilmington, specifically, truck congestion is the largest issue impacting operations. However, the impact reaches far beyond marine ports, affecting consumers and manufacturers both [17]. Thus, it is necessary to explore the systems that contribute to these delays and develop a solution to reduce them. There have been many past explorations reviewing the optimization of CMV arrival at marine ports [10], but the automation of

CMV security procedures and a universal platform to connect CMV operators, port authorities, cargo brokers, and cargo transport corporations has not been the topic of past discussion. The novel system discussed in this paper is based on Internet of Things (IoT)—a sensor and embedded system approach—alongside edge computing to solve the increasingly relevant CMV wait-time problem at marine ports.

II. Literature Review

Citation	Review of Maritime Cybersecurity Literature					
	Theme	**Features Checked**	**Methodology**	**Prototype**	**Key Findings**	**Limitation**
[1]	Toll Technology Comparison	Transaction time, throughput	Comparative analysis of tech types	No	ETC has highest throughput	No implementation or real-world testing
[2]	Port Drayage Congestion Classification	Gate waiting, operations, truck arrivals	Literature review survey of 71 papers	No	Optimizing arrival control	No empirical prototype
[3]	Port Congestion Logistics	Congestion measures, throughput, delays	Empirical & case study	No	Congestion reduces throughput	Limited intermodal analysis
[4]	Appointment Systems Scheduling	Delivery/pickup times, arrival	Optimization by using simulation	No	Appointment system reduces waiting times	No real-world tests
[5]	Export Container Deliveries	Slot assignments, truck turnaround	Optimization model & simulation	No	Optimized slots increase efficiency	The model assumes a perfect scenario
[6]	Gate Automation at Container Terminal	Gate processing time, errors	Case study with real data	Yes	Automated system reduced queue length	Site-specific, could be lacking generalizability
[7]	Reducing Truck wait time with appointments	Simulation effectiveness,	Using simulation to test efficacy	Yes	Prototype showed high accuracy and speed	Does not focus much on port logistics
[8]	Biometric Data Security	Data confidentiality	Cryptographic scheme evaluation	No	Combined cryptography and steganography to secure data	No performance benchmarks
[9]	Congestion Management at Terminal	Queue lengths, throughput	Discrete event simulation	No	Simulation shows that the system changes can cut queuing by ~30%	Lacks real world implementation
[10]	Review of Terminal Strategies	Appointment, scheduling	Literature review	No	Strategies such as appointment improves efficiency	Literature based, no new experiment

Port congestion is a global issue that creates significant delays, leading to widespread economic loss. Lange et al [2] proposed various ways to reduce congestion and determined that scheduling commercial vehicles can improve congestion. Port congestion is more severe in many developing nations [3] as many African ports experience significant congestion that causes trade to become unreliable and increases overall operation costs.

Researchers have proposed various methods to optimize Commercial Motor Vehicle arrivals by using an appointment-based system. Huang et al [4] experimented with an appointment system that allowed more efficient time slot usage. Similarly, Li et al [5] displayed a scheduling system for containers that reduced queuing time and improved overall efficiency. Moszyk et al [6] used an automatic gate system at DCT Gdańsk SA to improve container processing speed. Various studies used simulation tools [9] and computer programs [10] in order to validate recent technologies before implementing them in the field.

The majority of these innovations have high costs and low adaptability. In comparison, the proposed project is affordable, scalable, and supports various existing port security schemas. By integrating biometric data [7] and scheduling systems, DockChain ensures confidentiality and secure data handling [8] while optimizing cargo dropoff and pickup.

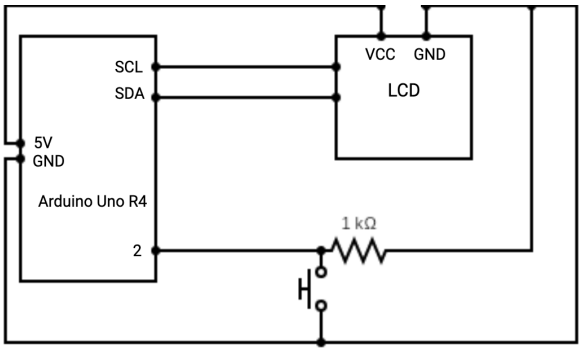

Fig. 1: Circuit Diagram of Entrance/Exit Components.

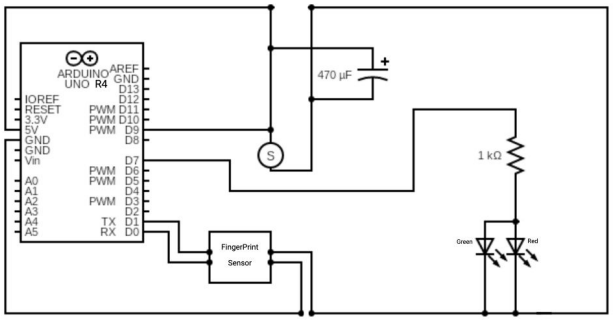

Fig. 2: Circuit Diagram of Crane LCD Components.

III. Proposed Solution

A. Microcontroller

The DockChain system's architecture consists of a servo-motor connected with a capacitor to stabilize the power supply, a biometric sensor to collect the driver's fingerprint data, and two red/green led to indicate to the operator the validity of the driver. This is all connected with an Arduino Uno R4 microcontroller that receives, and sends the data from the biometric sensors to the cloud. The microcontroller then receives the processed information from the cloud and sends it to the servo-motor, and sends it to the correct colored led.

The Liquid Crystal Display (LCD) is connected to an Arduino UNO R4 microcontroller to receive job information for crane operators. The push-switch allows for the operator to indicate the completion of the job which is connected to the Arduino UNO R4 microcontroller to send the information to the cloud.

B. Flowcharts

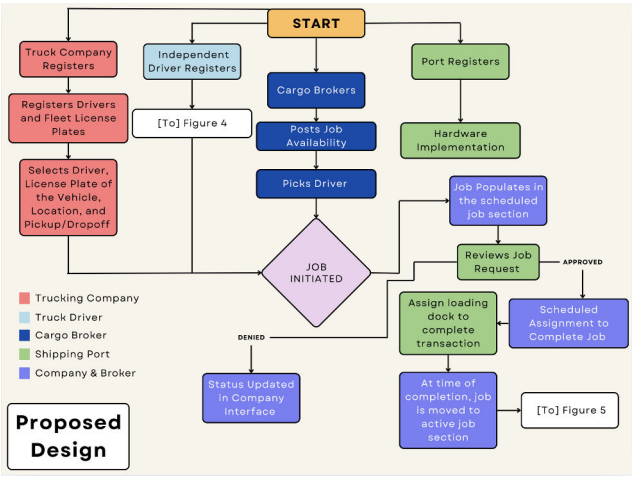

Fig. 3: Initial Job Flowchart.

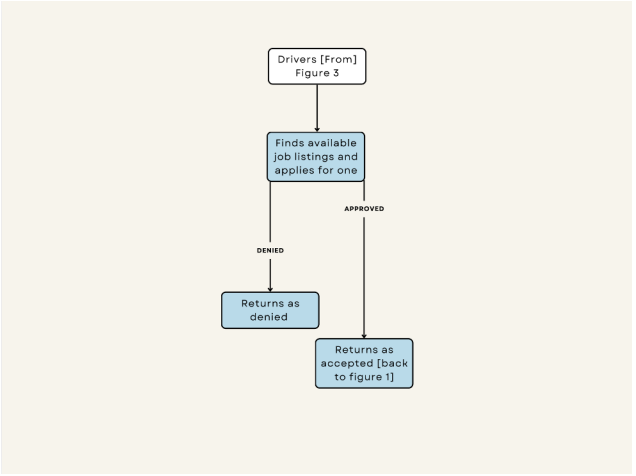

Fig. 4: Driver Registration & Job Flowchart.

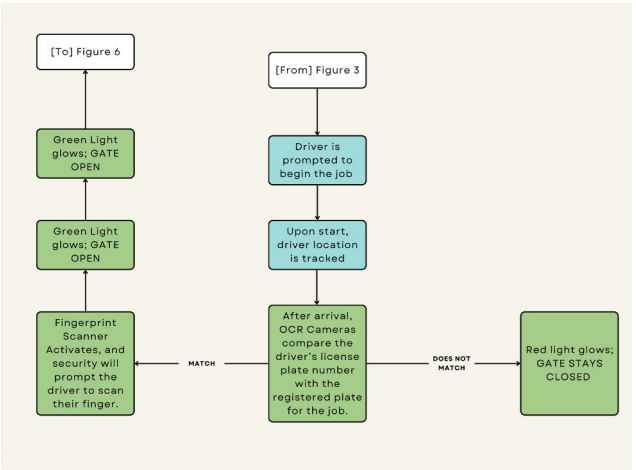

Fig. 5: Entrance Gate Interaction Flowchart.

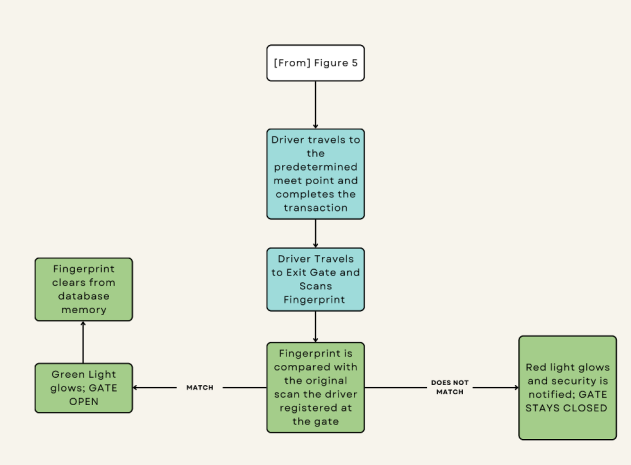

Fig. 6: Exit Gate Interaction Flowchart

Fig. 3 indicates the registration process for all platforms. As the solution is geared towards improving the port-infrastructure system, port operators will have to register their location and identifying information first. Next, the DockChain team will work with the port's security department to install OCR and fingerprint sensors into already existing port hardware.

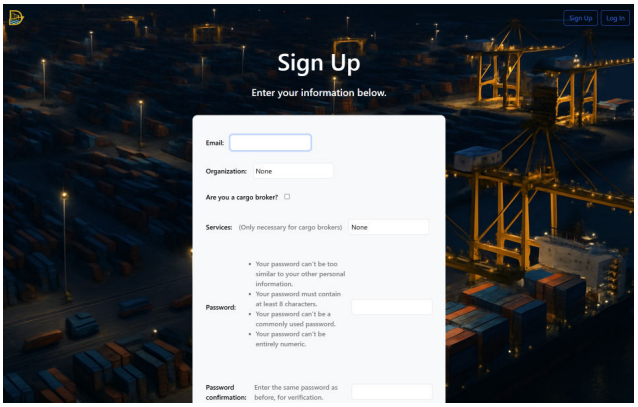

Fig. 7: Trucking Company Registration.
Source: Primary

Following this, truck companies entering the port will register their business. Similarly, they also provide all pertinent information to their operations (Fig. 7). Trucking companies also register individual drivers and their fleet of vehicles through the driver directory and license plate pages (Fig. 8).

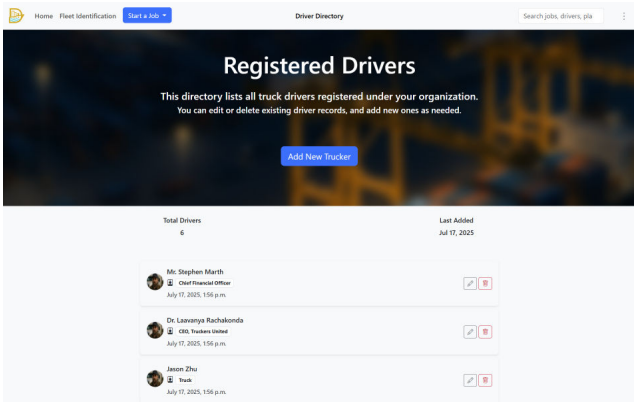

Fig. 8: Driver Registration Plate - Company-Specific.
Source: Primary

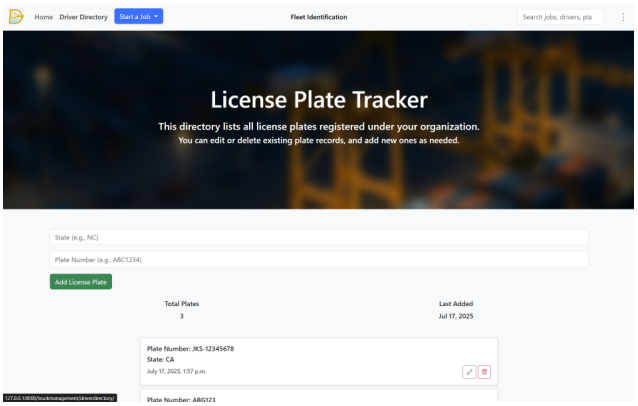

Fig. 9: License Plate Creation - Company-Specific.
Source: Primary

When creating drivers, a corporate login is automatically generated for individual drivers to sign in, who can then edit their account information and change passwords (Fig. 9). Regardless of the edits that drivers make, trucking companies will retain access to the login information of these drivers. License plates are independent of CMV operator signup (Fig. 10), meaning any CMV operator can be assigned to any license plate registered by a company.

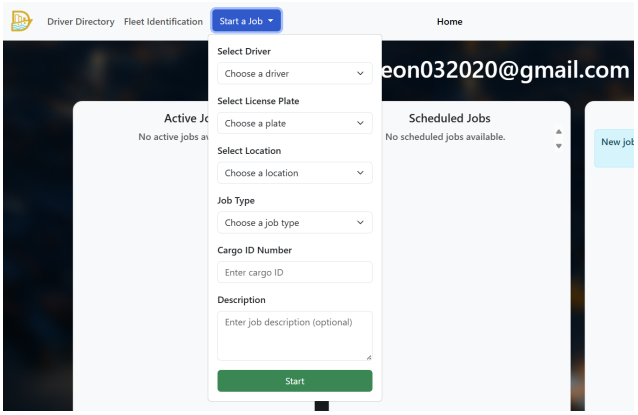

Fig. 10: Cargo Operation Registration Dropdown.
Source: Primary

After the port, company, and driver ecosystem has been created, companies can start creating jobs (Fig.

10). To do so, trucking companies choose options for selecting location, assigning drivers, license plates, distinguishing between drop off and pick up, cargo identification for handling, and job descriptions. After completing these fields, the job request is sent to the port interface. For trucking companies, jobs receive a "pending" status in the "scheduled jobs" section of their interface until further action is taken by the port.

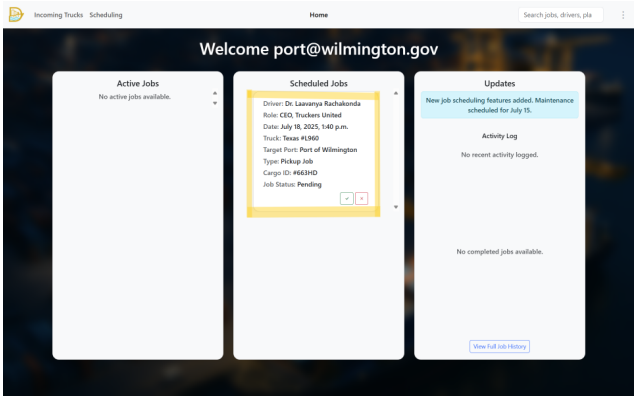

Fig. 11: Approval/Denial of Cargo Jobs.
Source: Primary

Port managers can view every job request directed towards their port location, and have the power to approve or deny each request (Fig. 11). If the job is approved, the card status is updated in the CMV operator interface, and officially assigned to the assigned driver. In this process, ports also assign a specific time and date to arrive for curbside transactions.

When the CMV operator gets a request to pick up or drop off a package, they open the app and start a "job". The app will send information about the job to the driver: job, location, cargo, and etc. The CMV operator is then assigned a truck from their organization that would have the license plate details. The CMV operator would turn on their location for the app and then it would send ETA information to the port.

DockChain acknowledges the presence of independent drivers who transport goods without affiliation with a management organization, and cargo brokers who demand such services. As such, these platforms are integrated into the web interface system.

Brokers looking to hire can register through the same trucking company sign-up page. Similar to trucking companies, they provide relevant information regarding their services. When starting a job, they post a listing of availability as opposed to assigning a driver.

Drivers who register independently through the sign-up page are directed to a different interface [Fig. 4]. They must register their personal vehicles, credentials, and available services, similar to a resume. They can then view the job listings available in their area and submit application requests. Brokers can then approve one driver, continuing the job process at the port interface.

When the CMV arrives at the port, the CMV operator will stop for security and register their biometric data with a fingerprint sensor (Fig. 5). While the CMV is stopped, an OCR camera will scan the license plate of the CMV. Biometric fingerprint data and license plate information is then transmitted to a remote MySQL database. The Arduino microchip retrieves job information from the cloud and identifies the job based on the recorded license plate. If the license plate and job match, it sends a green light to security, and a servo-motor would open the gate. If not, it will send a red light, and the CMV will have to wait for a human operator.

Information about the truck, cargo number, and location will be sent to the crane operator on an LCD display utilizing MySQL and a separate Arduino board. The operator will see a list of jobs for them to do, and if completed, they will press a button to finish a job.

Once cargo operations are complete and the CMV operator has reached the exit gate, their credentials will be verified, similar to the entrance gate (Fig. 6). The CMV operator will scan their fingerprint again, and the Arduino backend will compare the fingerprint to the initially recorded fingerprint. Simultaneously, the OCR camera will scan the license plate again and identify its corresponding job. The information will then be sent to the outgoing security gate. If all data is successfully verified, a green LED lights up. If not, a red LED lights up. Following this, a servo-motor will open the exit gate. Fig. 12 below visualizes this method in the real-world context of a port.

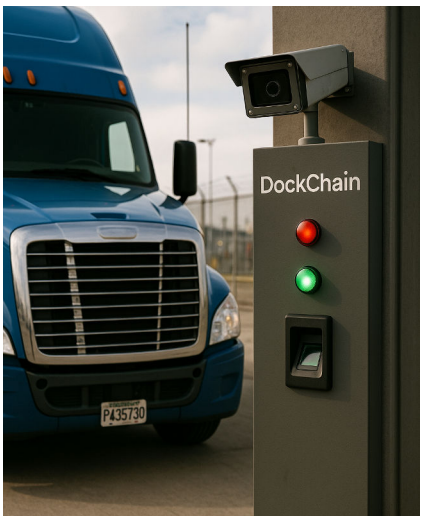

Fig. 12: Real-Life Concept Implementation of DockChain at Port Gates. Source: ChatGPT

IV. Implementation And Validation

A. Implementation

1) Hardware: As a proof-of-concept, the DockChain system is implemented with the following Arduino components:

- Two (2) Arduino UNO R4 WiFi boards
- Two (2) Resistor LEDs, green and red
- One (1) GR2904 fingerprint scanner
- One (1) SER0006 servo motor
- One (1) 10-volt electrolytic capacitor
- One (1) digital push button
- One (1) 1602 I2C LCD screen

The component setup for the entrance/exit component of the DockChain system is pictured below, in Fig. 13.

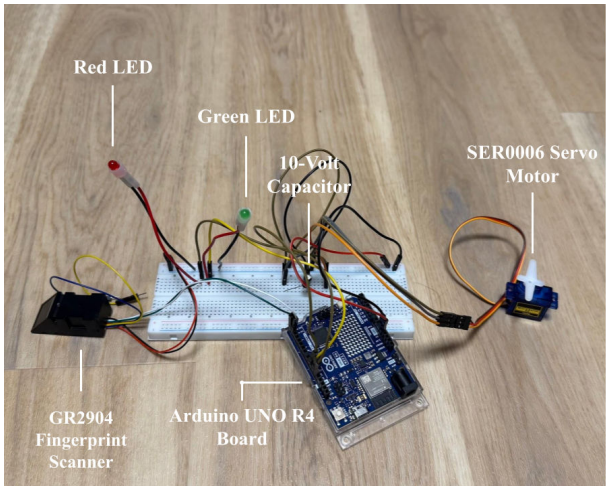

Fig. 13: Labeled Image of Entrance/Exit Hardware.
Source: Primary

The component setup for the crane operator component of the DockChain system is pictured below, in Fig. 14. A second Arduino board was utilized to ensure that entrance/exit hardware components are sufficiently distanced from the crane operator.

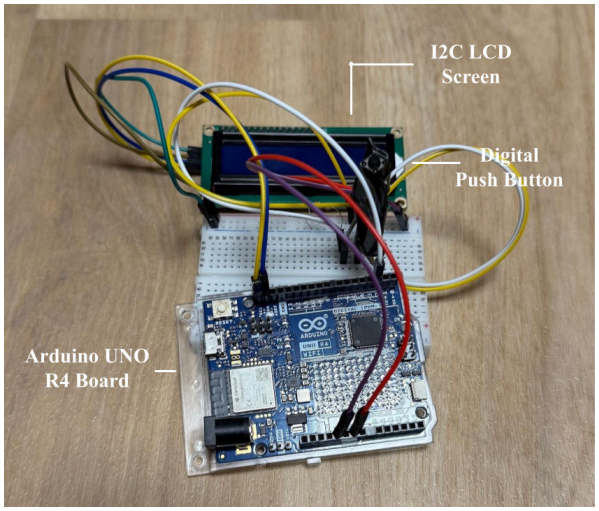

Fig. 14: Labeled Image of Crane Operator Hardware.
Source: Primary

All hardware components operate within a standard "loop" of cargo operations, explained in Section III. Proposed Solution. This loop is implemented utilizing Arduino code uploaded to each board.

2) Basic Software: The entrance/exit hardware and crane operator hardware communicate utilizing MySQL, a standard relational database management system (RDBMS). During a cargo operation loop, the Arduino boards interface with the DockChain MySQL database, accessing cloud information utilizing HTTP requests. Fig. 15 highlights an example of MySQL requests made by the Arduino boards.

```
FUNCTION getData(path):
    urlWithData ← "/truckmanagement/arduino_endpoint/?" + path
    response ← ""

    IF client connects to server on given port THEN
        SEND "GET {urlWithData} HTTP/1.1"
        SEND "Host: {server}:{port}"
        SEND "Connection: close"
        SEND empty line (indicates end of headers)

        timeout ← current time

        WHILE no data available from client:
            IF current time - timeout > 20 seconds THEN
                PRINT "Client timeout!"
                CLOSE client connection
                RETURN "TIMEOUT"

        headersEnded ← FALSE

        WHILE data is available from client:
            line ← read line from client

            IF headersEnded IS TRUE THEN
                response ← response + line + newline

            IF line is just a carriage return THEN
                headersEnded ← TRUE

        CLOSE client connection
    ELSE
        RETURN "CONNECTION_FAILED"

    RETURN response
```

Fig. 16: Example of HTTP Request in Pseudocode.
Source: Primary

To gain access to cloud information in Fig. 10, the Arduino microcontroller:

1) connects to the local network,
2) sends the HTTP request and reads the resulting response, and
3) closes the HTTP client.

Upon the Arduino board controlling crane operator components, a user interface (UI) is created to facilitate interaction between operators and the database. Said UI retrieves upcoming jobs from the DockChain MySQL database with HTTP requests similar to the code in Fig. 9, and displays these jobs within a loop, providing crane operators with instant updates on information changes within the MySQL database.

3) DockChain Website: While the Arduino board communicates with the DockChain database, a central website facilitates a variety of other database interactions. This website (1) allows CMV operators, cargo companies, and port authorities to create accounts, (2) creates and updates cargo jobs by passing information between users, and (3) manages all job and cargo information, including license plate data and CMV operator data. The DockChain website is built upon common programming languages, including HTML, CSS, JavaScript, and Python. The Python Django module is used within the website to render HTML templates, facilitate data entry and retrieval from the MySQL database, and manage users. Each 'rendered' webpage is provided with information from Django hooks that connect to separate Python files to complete a variety of tasks. Fig. 12 details an example of one such webpage, while Fig. 14 depicts the backend code rendering the webpage and providing it with data.

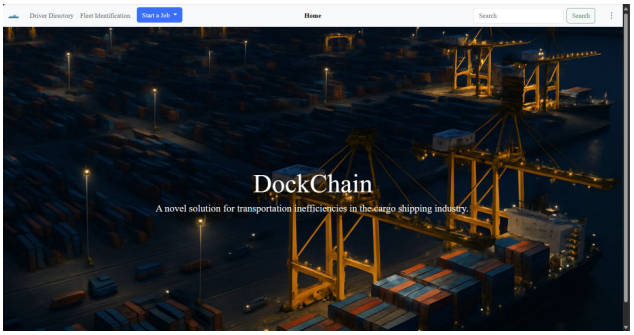

Fig. 16: The DockChain Homepage.
Source: Primary

Fig. 16 depicts the DockChain homepage, auto-formatted with Django enterprise templates and styled with additional CSS. There are 3 main registration interfaces, one for each user type: CMV operators, shipping companies, and port authorities. Shipping companies are further designated into two categories: regular shipping companies and cargo brokers, which post jobs for individual CMV operators to complete, rather than assigning jobs to hired workers. Each registration interface is customized to collect role-specific information. For example, shipping companies are required to provide a valid email, company title, shipping type (regular vs brokers), and password. To promote security, passwords are required to be 8 characters long, unique from the inputted email, and contain numbers or special characters.

Django code within role-specific HTML templates ensures that only authenticated users can access operative interfaces. Any other website guests are denied access to these pages. Additionally, users cannot visit pages designated for other user types (for example, a port authority cannot view a CMV operator's list of current jobs).

Further, Django code matches template 'requests,' which are identified by HTML tags, to the correct action. For example, the 'Start Job' button in Fig. 11 has an HTML tag titled 'start_job, corresponding to the 'start_job' action within Python code written for the homepage.

4) Cybersecurity: Data access is secure across the DockChain website, due to 2 main cybersecurity protocols: hashing and CSRF tokens.

a) Hashing: Once submitted, user registration information (i.e., username, password, etc.) is transformed into fixed-length hash sequences based on a predetermined mathematical formula. These hash sequences serve as a "fingerprint" for user data. Instead of information being stored in plaintext within the MySQL environment, the generated hash sequences are stored instead, ensuring data is secure and protected from all sources, including website administrators (Fig. 17).

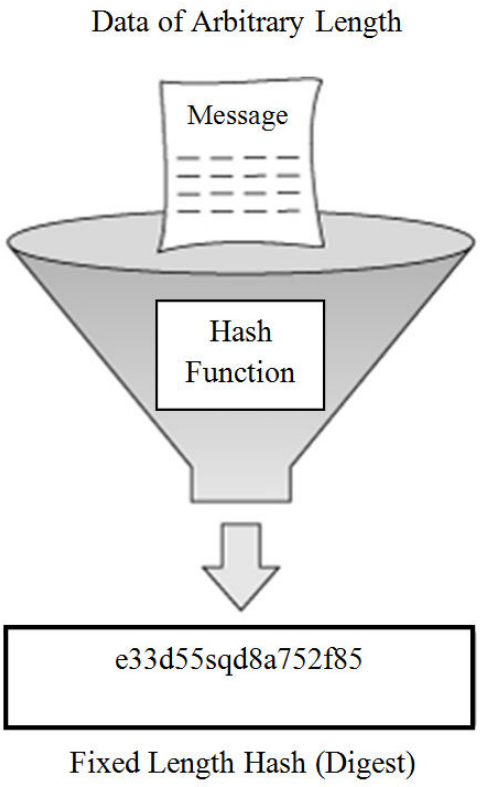

Fig. 17: Depiction of Hashing Algorithm.
Source: Adapted from [20]

b) Cross-Site Reference Forgery Tokens: Cross-Site Reference Forgeries are malicious attacks on websites that attempt to gain access to user information. These attacks create malicious URLs containing false web cookies. When a user attempts to access a valid website with a CSRF URL, their data is stolen and transmitted to the attacker. To address this vulnerability, each form within the DockChain website utilizes CSRF tokens to provide additional verification of submitted data. Fig. 18 further illustrates the purpose and procedure behind CSRF tokens.

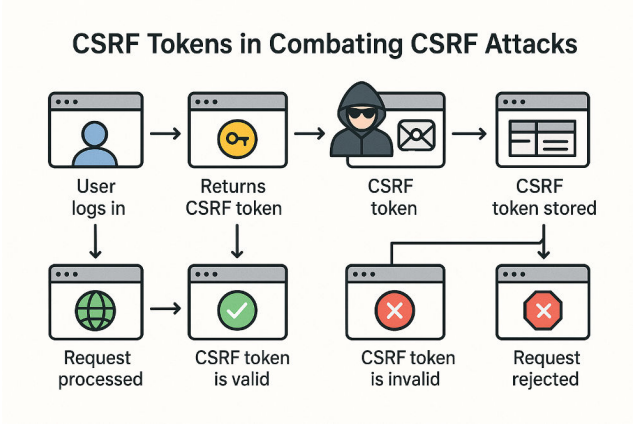

Fig. 18: Flowchart Illustrating Cross-Site Reference Forgery Tokens.
Source: ChatGPT

When a user submits a form on the DockChain website (for example, registration), a secure CSRF token is generated and stored on the server. When logging in, this token is processed and verified with that user's cookies. If an attacker attempts to create a login request, the CSRF token will be invalid, and said request will be rejected.

B. Validation

The solution detailed in this paper targets two issues in overall port operations: the vague scheduling of CMVs entering ports and the time-consuming analog security systems. CMV scheduling has been implemented in other applications and is effective in decreasing inefficiency. A Truck Appointment System (TAS) resulted in a 62% decrease in maximum queue length at ports and reduced carbon emissions by 785 tons in one year [19]. This type of appointment scheduling has been tested, but not implemented alongside automation within port security systems.

As for validating the automation part of this solution, one such application is with electronic tolling on roads in the United States. For years, tolls have been collected through human employees, with cars on highways having to wait in lines to pay tolls and then get back on their way. However, Electronic Toll Collection (ETC) systems have been increasingly implemented in highways across the United States, including in North Carolina. ETC systems have been shown to decrease operation costs and lines of traffic at toll booths [18]. The tolling situation in North America reflects a similar situation in marine ports, with wait times in both industries. However, automation like ETC has been shown to be effective at optimizing traffic flow on toll roads, so it can be assumed with confidence that similar automation through the solution can optimize traffic flow and similar systems in ports, as well.

V. Conclusion And Future Work

The DockChain system described above utilizes multiple sensors, actuators, and an edge computing system to incorporate automation into marine port security and communications. The IoT system can be split up into two parts: the universal platform for connecting all 4 groups of users, as well as the sensors and actuators that help to streamline the check-in and security process for CMVs. The universal platform utilizes SQL databases to store values for every type of user. Among these values are license plate numbers, active jobs, a list of drivers, the location of the port, usernames, and more. The platform is currently built upon a website and web server, but may be expanded to a mobile application. As for the hardware aspect, an OCR sensor is used to scan the license plates of CMV arrivals and check with the database to verify CMV operator identity. The same occurs with the fingerprint sensor, and an LED that flashes green if the information is correct. The LCD is used by crane operators to see which type of cargo is needed, and at what time and order. In the future, the DockChain website could be expanded to a mobile app that CMV operators will be able to download. Furthermore, DockChain could be implemented in a simulated port environment to collect data on its impact on CMV turnaround time. Additionally, this technology could be implemented at inland warehouses, giving warehouse administrators important organizational information about CMV arrival time, order, and cargo needs. DockChain could also be implemented in small to mid-sized ports in addition to inland warehouses to optimize cargo transactions and decrease cargo inefficiency across the country. Through continued testing, development and improvements, DockChain has the potential to significantly modernize maritime ports across the globe and strengthen the security and efficiency of global port operations.

REFERENCES

[1] Khali, C. Walton, and S. Hussain, "Toll Collection Technology and Best Practices," 2006. Available: https://ctr.utexas.edu/wp-content/uploads/pubs/0_5217_P1.pdf

[2] A.-K. Lange, A. Schwientek, and C. Jahn, "Reducing Truck Congestion at Ports - Classification and Trends CC-BY-SA 4.0." Available: https://tore.tuhh.de/dspace-cris-server/api/core/bitstreams/b685b7a5-1124-4f71-ac4d-7b7fc5dceb57/content

[3] "Consequences of Port Congestion on Logistics and Supply Chain in African Ports." Available: https://core.ac.uk/download/pdf/234682294.pdf

[4] P. Huang, H. Wang, F. Tan, Y. Jiang, and J. Cai, "Optimization of external container delivery and pickup scheduling based on appointment mechanism," PLOS ONE, vol. 20, no. 2, p. e0318606, Feb.2025, doi:https://doi.org/10.1371/journal.pone.0318606.

[5] N. Li, G. Chen, M. Ng, W. K. Talley, and Z. Jin, “Optimized appointment scheduling for export container deliveries at marine terminals,” Maritime Policy & Management, vol. 47, no. 4, pp. 456–478, Nov. 2019, doi: https://doi.org/10.1080/03088839.2019.1693063.

[6] K. Moszyk, M. Deja, and M. Dobrzynski, “Automation of the Road Gate Operations Process at the Container Terminal—A Case Study of DCT Gdańsk SA,” Sustainability, vol. 13, no. 11, p. 6291, Jun. 2021, doi:https://doi.org/10.3390/su13116291.

[7]N. Huynh, “Reducing Truck Turn Times at Marine Terminals with Appointment Scheduling,” Transportation Research Record: Journal of the Transportation Research Board, vol. 2100, no. 1, pp. 47–57, Jan. 2009, doi: https://doi.org/10.3141/2100-06..

[8] S. Malipatolla, D. Aeloor, and A. A. Manjrekar, “Securing biometric data with visual cryptography and steganography,” in Security in Computing and Communications: Proc. Int. Symp. SSCC 2013, Mysore, India, Aug. 2013, vol. 1. Berlin, Germany: Springer Berlin Heidelberg, 2013, pp. 1-9.

[9] M. Neagoe, H.-H. Hvolby, M. S. Taskhiri, and P. Turner, “Using discrete-event simulation to compare congestion management initiatives at a port terminal,” Simulation Modelling Practice and Theory, vol. 112, p. 102362, Nov. 2021, doi: https://doi.org/10.1016/j.simpat.2021.102362.

[10] A. Maguire, S. Ivey, M. M. Golias, and M. E. Lipinski, “Relieving Congestion at Intermodal Marine Container Terminals: Review of Tactical/Operational Strategies,” RePEc: Research Papers in Economics, Mar. 2010, doi: https://doi.org/10.22004/ag.econ.207280.

[11] “Port Congestion 2025: The most congested ports right now - Conqueror Blog,” *Conqueror Blog*, May 07, 2025. https://www.conquerornetwork.com/blog/2025/05/07/port-congestion-2025-the-most-congested-ports-right-now/

[12] International Chamber of Shipping, “Shipping and world trade: driving prosperity,” *www.ics-shipping.org*, 2020. https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/

[13] O. US EPA, “Virtual Vessel Arrival Systems at Ports Improves Air Quality and Saves Fuel,” *www.epa.gov*, Aug. 20, 2020. https://www.epa.gov/ports-initiative/virtual-vessel-arrival-systems-ports-improves-air-quality-and-saves-fuel

[14] “Port Access - NC Ports,” *NC Ports*, Oct. 16, 2024. https://ncports.com/customer-tools/port-access/

[15] U. States., “Port Security: A National Planning Guide,” *Bts.gov*, 1997. https://rosap.ntl.bts.gov/view/dot/13693

[16] University of Gothenburg, “The cost of the Suez Canal blockage,” *University of Gothenburg*, Jan. 22, 2025. https://www.gu.se/en/news/the-cost-of-the-suez-canal-blockage

[17] V. Veleda and A. Llop, “Port congestion Explained: Why Delays Happen and How to Mitigate Them,” *Alg-global.com*, 2025. https://alg-global.com/blog/maritime/port-congestion-why-delays-happen-and-how-mitigate-them

[18] “Toll Roads in the United States: History and Current Policy History.” Available: https://www.fhwa.dot.gov/policyinformation/tollpage/documents/history.pdf

[19] F. Bouyahia, S. Belaqziz, Youssef Meliani, Saâd Lissane Elhaq, and Jaouad Boukachour, “A Novel Truck Appointment System for Container Terminals,” Sustainability, vol. 17, no. 13, pp. 5740–5740, Jun. 2025, doi: https://doi.org/10.3390/su17135740

[20] M. Turcanik and M. Javurek, “Hash algorithm III. HASH FUNCTION,” ResearchGate. [Online]. Available: https://www.researchgate.net/figure/Hash-algorithm-III-HASH-FUNCTION_fig1_310624366. [Accessed: 18-Jul-2025].