sciendo

POLISH MARITIME RESEARCH 1 (121) 2024 Vol. 31; pp. 135-145
10.2478/pomr-2024-0014

BLOCKCHAIN-ENABLED TRANSFER LEARNING FOR VULNERABILITY DETECTION AND MITIGATION IN MARITIME LOGISTICS

Chandra Priya J [1]
Krzysztof Rudzki [2]
Xuan Huong Nguyen [3]
Hoang Phuong Nguyen [4]
Naruphun Chotechuang [5]
Nguyen Dang Khoa Pham [6*]

[1] Department of Computer Science and Engineering, Mepco Schenk Engineering College, Sivakasi, India
[2] Faculty of Marine Engineering, Gdynia Maritime University, Gdansk, Poland
[3] Nguyen Tat Thanh University, Ho Chi Minh City, Viet Nam
[4] Academy of Politics Region II, Ho Chi Minh City, Viet Nam, Viet Nam
[5] Faculty of International Maritime Studies, Kasetsart University, Sri Racha Campus, Chonburi, Thailand
[6] PATET Research Group, Ho Chi Minh City University of Transport, Ho Chi Minh City, Viet Nam

* Corresponding author: *khoapnd@ut.edu.vn (Nguyen Dang Khoa Pham)*

ABSTRACT

With the increasing demand for efficient maritime logistic management, industries are striving to develop automation software. However, collecting data for analytics from diverse sources like shipping routes, weather conditions, historical incidents, and cargo specifications has become a challenging task in the distribution environment. This challenge gives rise to the possibility of faulty products and traditional testing techniques fall short of achieving optimal performance. To address this issue, we propose a novel decentralised software system based on Transfer Learning and blockchain technology named as BETL (Blockchain -Enabled Transfer Learning). Our proposed system aims to automatically detect and prevent vulnerabilities in maritime operational data by harnessing the power of transfer learning and smart contract-driven blockchain. The vulnerability detection process is automated and does not rely on manually written rules. We introduce a non-vulnerability score range map for the effective classification of operational factors. Additionally, to ensure efficient storage over the blockchain, we integrate an InterPlanetary File System (IPFS). To demonstrate the effectiveness of transfer learning and blockchain integration for secure logistic management, we conduct a testbed-based experiment. The results show that this approach can achieve high precision (98.00%), detection rate (98.98%), accuracy (97.90%), and F-score (98.98), which highlights its benefits in enhancing the safety and reliability of maritime logistics processes. Additionally, the computational time of BETL (the proposed approach) was improved by 18.9% compared to standard transfer learning.

Keywords: Logistic management, Blockchain, Transfer Learning, Marine ecosystem, Vulnerability detection

INTRODUCTION

In recent years, maritime-related issues have been paid much attention since maritime has been known to play an important role in developing the economy [1]–[4]. However, maritime activities, including shipping and port activities, have a large number of disadvantages, such as high pollutant emissions (including ship and port activities), low operational efficiency, high-cost logistical activities, high fuel consumption, maritime safety… etc. [5]–[11]. Containerisation has played a crucial role in accelerating global trade and establishing extensive global supply chains, contributing significantly to economic globalisation in the 20th century [12][13]. However, progress in container shipping has not kept up with the rapid advancements in international trade and supply chains [14][15]. Businesses now demand more timely and transparent deliveries with enhanced traceability, which traditional container shipping struggles to meet [16][17]. The movement of containers involves complex bilateral interactions among various entities in the logistics ecosystem, resulting in delays, inefficiencies, and susceptibility to fraud

[18][19]. Paper-based processes and numerous permissions and transactions further contribute to inefficiencies towards hard evidence of its effectiveness [20]. As a result, there is a need for innovative solutions to address these vulnerabilities in maritime logistics [21]. To tackle these challenges, this manuscript introduces a groundbreaking solution: Blockchain-Enabled Transfer Learning. By leveraging the transparency and immutability of blockchain and the analytical capabilities of AI, the proposed system aims to detect and mitigate vulnerabilities in real time, enhancing the security and reliability of the logistics ecosystem [22][23]. The integration of blockchain and Transfer Learning introduces a decentralised architecture with smart contracts, automating trust and collaboration among multiple stakeholders in the logistics chain [24]. A comprehensive testbed-based experiment validates the efficacy of the solution, fortifying the logistics industry against vulnerabilities and disruptions, while improving global maritime trade security and efficiency [25][26].

In traditional maritime logistics, the seamless coordination among diverse entities relies on efficient communication and monitoring within a shared workspace [27]. As cargo is transported by ship from one port to another, several pieces of documentation must also be moved and verified by multiple parties such as bill of lading, packing lists, certificates of origin, commercial invoices, and export licenses [28]. In addition, a vessel's crew, who are not necessarily nationals of the flag state, needs to manage, verify, and validate seafaring crew certificates in compliance with global regulations such as the IMO's International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) and the Convention on Safety of Life at Sea (SOLAS) [29][30]. However, in a remote working environment, ensuring seamless synchronisation becomes more challenging, leading to potential code errors, oversights, and mistakes [31]. Blockchain adoption in the maritime supply chain for containerised international trade faces several barriers [32][33]. These barriers include a lack of support from influential stakeholders and a lack of government regulations [34]. The key stakeholders in this adoption process are container lines, ports, beneficial cargo owners, freight forwarders/third-party logistics, and customs authorities [35][34]. Additionally, there are non-technical barriers such as resistance to change and a lack of awareness and understanding that should not be underestimated [36]. To successfully implement blockchain in the shipping industry, certain design principles should be considered, including immutability, decentralisation, security, privacy, compatibility, scalability, inclusiveness, and territoriality [37][38]. The implementation phase can be influenced by different approaches, which can affect the likelihood of adoption by industry stakeholders [39]. Actually, intelligent methods such as machine learning and artificial intelligence, which could be successfully applied to many fields such as waste and energy management, optimization, planning, prediction, and error detection aiming to generate a powerful collaboration [40]–[44], could have the potential to revolutionise the maritime sector through improved efficiency, safety, and environmental sustainability [45]–[47].

Secure supply chain management methods (to protect blockchain from attack) can be achieved through the implementation of blockchain technology. Blockchain provides decentralised and immutable data storage, enabling trust and transparency in supply chain networks [48][49]. By using blockchain, a digital log of all propagating information can be maintained, allowing for the validation of official updates and the rejection of potentially malicious payloads [50][51]. Additionally, the use of attribute-based access control models, in combination with blockchain, can enable decentralised, fine-grained, and dynamic access control management in supply chain systems, ensuring data privacy and network scalability [52]. The integration of blockchain with supply chain management also helps minimise the interference of middleman attacks and allows the discarding of forged products, thereby maintaining integrity and authentication throughout the supply chain. To summarise the state-of-the-art literature, the problem scenarios are listed below.

Over-centralisation: Consider S as the comprehensive set encompassing all entities actively engaged in maritime logistics, C is the set of all communication channels between the entities in S, and R is the set of all associated risks. The problem of centralised maritime logistics is the minimisation of the following expression:

$$f(S, C, R) = \Sigma (r * p(r)) \tag{1}$$

where p(r) is the probability of risk r occurring.

Data Security in remote workplace: Let G be the probability of a collaborative effort being successful, D is the distance between the collaborating entities and H is the disparity in hardware and software accessibility between remote and in-office workers. Then, the problem of the probability of a collaborative effort can be modelled as follows:

$$P = f(D, H) \tag{2}$$

where f is a function that maps the distance and disparity to the probability of collaboration, and D and H are continuous variables that represent the distance between the collaborating entities and the disparity in software accessibility, respectively. The statistical analysis for the estimating function f has the inferences that G decreases as D increases and as H increases.

Data sharing dilemma: Maritime supply chain stakeholders are concerned with sharing key business information, such as customer, supplier, and freight data. This is because many forwarders and intermediaries benefit from information asymmetry, which could impede widespread adoption. If we let T be the time it takes to complete a task, then it can be modelled as follows:

$$T = g(H) \tag{3}$$

where g is a function that maps the disparity to the time taken to complete a task. The problem is that T is directly proportional to H.

RELATED WORKS

The use of electronic bills of ladings has been shown to enhance the efficiency of shipping operations, ship finance, and marine

insurance. In contrast, Papathanasiou et al. [52] proposed that the shipping industry could derive advantages from blockchain technology in areas such as document exchanges, optimising container utilisation, intelligent transportation, and precise container weighing. Hamidi et al. [53] and Zhong et al. [54] suggested that the adoption and effective use of blockchain by container lines could contribute to reducing price competition between them. Furthermore, Hasan et al. [55] demonstrated a smart-contract solution involving smart containers equipped with Internet of Things (IoT) sensors to efficiently manage shipments. They showcased how blockchain enables real-time tracking of items like vaccines, including monitoring temperature, humidity, and air pressure. In their conceptual study, Lambourdiere and Corbin [56] proposed that blockchain can have a positive impact on information exchange, supply chain coordination, visibility, and performance within maritime supply chains.

Taking a sustainability perspective, Jovi´c et al. [57] conducted a literature review and categorised the benefits of blockchain in maritime supply chains into economic, social, and environmental advantages. Meanwhile, Li et al. [58] explored pilot applications in maritime supply chains and identified significant benefits from blockchain, including expediting processes, reducing costs related to documentation, ensuring secure records for food safety, enabling real-time tracking, facilitating efficient coordination across various modes of transport, and improving compliance with shipment regulations and marine insurance requirements. Lastly, Munim et al. [59] conducted a review of blockchain literature in a maritime context, revealing 17 potential uses of blockchain technology. The state-of-the-art studies focused on the risk analysis of blockchain-integrated systems (BISs) in container shipping. However, it failed to capture the full range of risks and uncertainties associated with other aspects of maritime logistics services [60][61]. The study does not provide a comprehensive analysis of the potential mitigation strategies or recommendations for managing the identified risks in container shipping BISs. In general, the cause and effect of malicious software is presented in Fig. 1.

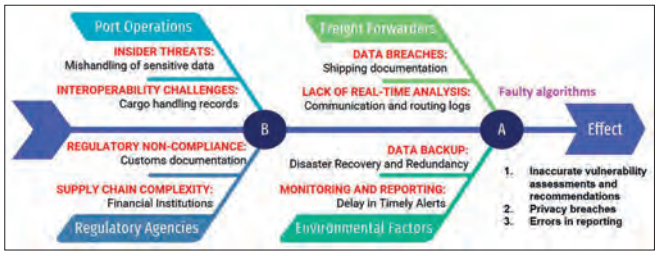

Fig. 1. Cause and effect of malicious software

BLOCKCHAIN-ENABLED TRANSFER LEARNING (BETL): GENERIC ARCHITECTURE

The proposed architecture ensures efficient and accurate vulnerability detection, security, scalability, trust, transparency, and reliability in a multiparty maritime logistics ecosystem [62] [63]. The overall system is divided into two parts: a transfer learning (TL) model that predicts software vulnerabilities, and a blockchain-based system that ensures security, trust, and transparency [64] [65]. InterPlanetary File System (IPFS) is integrated to improve the scalability and efficiency of data storage. The TL model is trained on a large dataset of software vulnerabilities to learn the patterns of vulnerabilities. The model can then be used to predict vulnerabilities in new software. The blockchain-based system uses a distributed ledger to store vulnerability information. This ensures that the information is secure, transparent, and tamper resistant. An IPFS peer-to-peer file storage system is used for scalable and efficient storage. The BETL architecture assumes a multiparty ecosystem, as shown in Fig. 2. The distinctive roles of various stakeholders include the following.

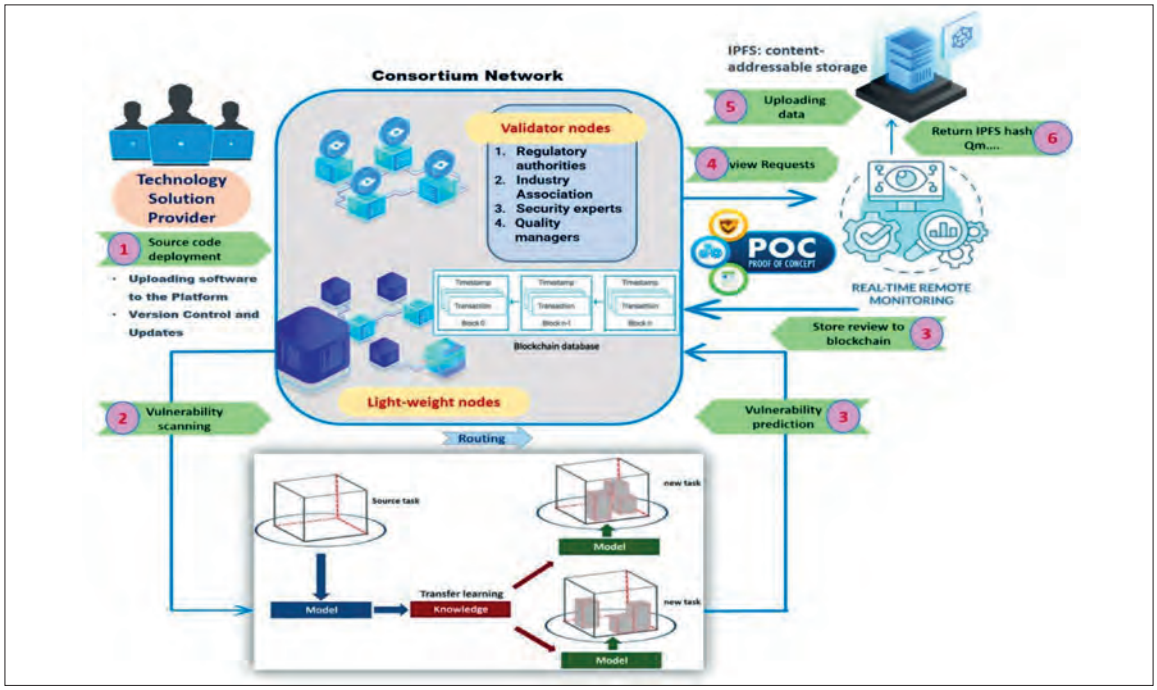

Fig. 2. BETL system architecture

Technology Solution Provider (TSP): The TSP is an authenticated entity in the logistics ecosystem with a unique identifier. It is responsible for writing code, following the requirements of the assigned module. The choice of programming languages depends on the requirements and varies widely based on the application. The TSP is provided with login credentials to access the code submission platform and has the privilege of performing unit testing. It is assumed that the TSP submits its code over a secure network in a remote scenario.

Consortium Network: We opted for a consortium blockchain as it balances the security of a private blockchain and the flexibility of a public blockchain. The network is formed and operated by a group of trusted entities, regulatory authorities, industry associations, security experts, and quality managers. This ensures that the blockchain is highly secure and resistant to attack. *Validator nodes* are responsible for reaching a consensus on the order of transactions and ensuring that no unauthorised changes are made to the blockchain. They do this by using a voting mechanism to approve new blocks of transactions. *Lightweight nodes* can participate in the network by reading the blockchain and querying information. However, they cannot participate in the consensus process.

InterPlanetary File System: An IPFS private network provides secure and decentralised storage and access to data about the supply chain. This can help to improve the efficiency of learning models by reducing the need to transfer data between different systems.

ARCHITECTURAL DESIGN

The BETL architecture consists of three main components: a vulnerability scanner, a blockchain-based decentralised infrastructure, and a private IPFS network shared by the validators. There are four major entities including technology solution providers, validator nodes, lightweight nodes, and IPFS storage architecture. Data and information exchanged among entities are stored on the blockchain as immutable transactions. A smart contract deployed on the blockchain governs the interactions and automates various functionalities. The core functionalities of the proposed architecture are twofold:

- **Transfer Learning-based source code vulnerability scanning:** This component uses artificial intelligence to identify vulnerabilities in the source code.
- **Blockchain-based decentralisation for vulnerability prevention:** This component uses the blockchain to store information about vulnerabilities and to prevent vulnerabilities from being exploited.

TRANSFER LEARNING-BASED VULNERABILITY SCANNING

During the outsourcing of the development process, developers may purposefully or inadvertently make certain mistakes that could result in a vulnerable application. Traditional vulnerability detection in software testing requires human intervention, making it time-consuming. There is also the possibility of human error in the reviewing process. In such a scenario, transfer learning can greatly help reduce this risk-oriented human intervention in the testing process of vulnerabilities. In the proposed system, a transfer learning model is trained on a dataset of 20,724 source code files from the six most common languages (C, C^{++}, Python, Java, Ruby, and C#). The dataset is categorised into vulnerable and non-vulnerable codes, based on vulnerability thresholds. The National Institute of Standards and Technology (NIST) categorises the level of severity as low, medium, or high. In this work, we propose a non-vulnerability score range mapping with a reverse threshold manner to that of the NIST standard. This is mainly for the following reasons:

- The transfer learning model performs learning for a non-vulnerability score, i.e. the prediction score tells us how well the source code is written.
- Software Development LifeCycle (SDLC) is concerned with ensuring error-free code at the production level. Having a non-vulnerability score, rather than a vulnerability score, for mapping the category range is more intuitive for the lead developerto make better decisions.

We mapped the non-vulnerability score range with the category of secureness of source code files, as shown in Table 2. This mapping can be customised, according to the requirements and policies of the organisation, and is controlled by the blockchain validator nodes. Once source codes are uploaded, the smart contract invokes the transfer learning model to check for vulnerability. The model predicts the non-vulnerability score for the source code and the score is mapped to the secureness category. The lead developer can then take appropriate action, based on the secureness category of the source code. This transfer learning-based vulnerability detection system can help to improve the efficiency and accuracy of vulnerability detection in maritime logistics. It can also help to reduce the risk of human error in the reviewing process. Table 2 summarises the differences between AI-based and transfer learning-based vulnerability detection.

Tab. 1. AI-based learning versus transfer learning

Feature	AI-based learning	Transfer learning
Model training F: $Z \rightarrow R^d$ $Z \subseteq Rd$, $d \rightarrow$ # vulnerabilities	$\{(z_i, y_i)\}_{i=1}^{n}$ where $\in Z$ is the i^{th} vulnerability and is its label. AI requires n to be high	Let Z_s and Z_t be the source and target domains, respectively. Let f_s be a pre-trained model on source domain Z_s. TL leverage f_s to reduce training time
Accuracy	$Accuracy(f) = \frac{\sum_{z \in Z} I(f(x) = y)}{\lvert Z \rvert}$ where I(x) is an indicator function	$Accuracy(f_t) = \frac{\sum_{z_t \in Z_t} I(f_t(z_t) = y_t)}{\lvert Z_t \rvert}$ f_t is a model learned on Z_t by leveraging knowledge from f_s. $f_t(z_t)$ is the prediction of the model for the vulnerability z_t
Scalability	$T = a \times D^b$ where T is the training time, D is the dataset size with a and b as constants	$T = a \times S^b + c \times T^d$ where T is the fine-tuning time with S and T as the source and target dataset size involving the constants a, b, c, and d
Cost-effectiveness	Can be expensive to develop and deploy	Can be more cost-effective than AI-based vulnerability detection

BLOCKCHAIN-BASED DECENTRALISATION FOR VULNERABILITY PREVENTION

The blockchain-based decentralised system for prevention consists of a smart contract that acts as the core logic unit of the system [66][67]. The smart contract is used to automate certain tasks on the blockchain, such as testing code for vulnerabilities and storing the results of the testing securely. When a developer uploads code for testing, the smart contract invokes a transfer learning to test the code for vulnerabilities. The neural network is trained on a dataset of known vulnerabilities, so that it can identify vulnerabilities in new code [68][69]. If the model detects vulnerability in the code, the smart contract stores the vulnerability information in the blockchain. The smart contract also stores the results of the testing, which indicates whether the code is vulnerable or not. If the code passes the test, the smart contract stores the results of the testing in the blockchain and stores the source code file in IPFS. IPFS is a distributed file storage system that makes it difficult to modify or delete files.

The access control mechanism of the smart contract ensures that only authorised users can access the data stored in the blockchain. This helps to protect the confidentiality and integrity of the data. The blockchain-based decentralised system for prevention provides several benefits, including:

Automated testing: The smart contract can automate the process of testing code for vulnerabilities. This can help to save time and improve the efficiency of the testing process.

Secure storage: The blockchain is a secure and tamper-proof distributed ledger. This helps to ensure that the data stored in the blockchain is protected from unauthorised access and modification.

Traceability: The blockchain provides a tamper-proof record of all changes to the data stored in the blockchain. This helps to ensure that the data is always accurate and reliable.

Pseudo-transparency: The blockchain is a pseudo-transparent ledger that is accessible to everyone. This helps to ensure that the testing process is transparent and accountable.

IPFS STORAGE FOR ANALYTICS

The IPFS 'DHT' is a Distributed Hash Table used to store the hashes of all the files that are stored in the Kademlia overlay network. *N* is the set of nodes in the IPFS DHT network [70]. Each node n∈N maintains a routing table T_n that stores the location of other nodes in the network. The routing table is a hash table that maps the hashes of the nodes to the addresses of the nodes. To search for a file, a node *n* sends a query *q* to the DHT. The query is a hash of the file that is being searched for. The query is routed to the nodes that store the hash of the file. The routing table is a distributed hash table, so the query is routed to the nodes that are most likely to store the hash of the file. When a file is stored in the DHT, it is split into blocks and distributed to multiple nodes. The blocks of a file are replicated using a hash function to multiple nodes to ensure availability. The hash function is used to generate a unique identifier for each block. The blocks are then replicated to nodes that have the same hash identifier. The fault tolerance of the IPFS DHT network is achieved through replication. The internal working of IPFS can be represented by the following functions:

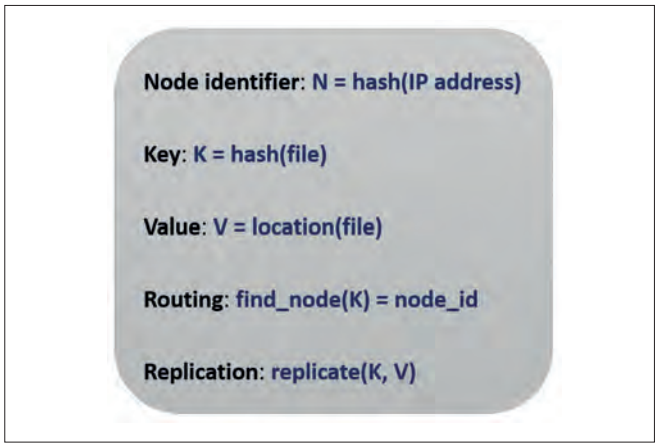

Fig. 3. IPFS-DHT network parameters

Content Publishing:

1. The blockchain validator imports the content into its local IPFS private network and assigns it a unique content identifier (CID).
2. The IPFS instance performs a DHT traversal to locate the closest peers to the CID by XORing the distance of the Peer ID from the SHA256 hash of the CID.
3. The IPFS instance stores the peer record with the closest peers.

Content Retrieval:

1. The requester performs opportunistic Bitswap requests to already connected peers for the CID.
2. If the requester does not find the content, the DHT performs a multi-round iterative lookup to resolve a CID to a peer's Multi-addresses as a traversal, to find a provider record storing the peer.
3. The requester connects to the peer and fetches the content that maps CID using Bitswap.

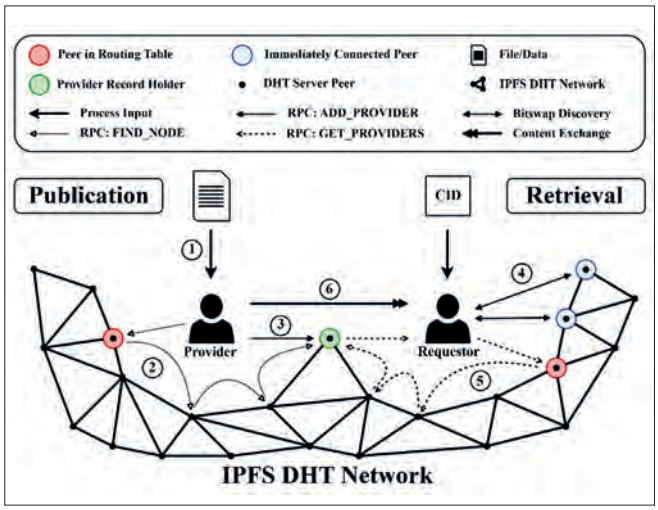

Fig. 4. Content publication and retrieval in IPFS

EXPERIMENTAL SETUP

We conducted experiments on a testbed that integrated transfer learning, blockchain, smart contracts, and private IPFS. The testbed consisted of 8 nodes, which simulated 2 blockchain validators, 4 lightweight nodes, and 2 technological solution providers with the specified system configuration.

Transfer learning environment: A gated recurrent units (GRU) model was used to extract features from the source code to learn long-term dependencies, which is important for source code analysis. We selected the Robustly Optimised BERT Approach (RoBERTa) model with AdamW optimiser, to classify the features extracted by the GRU model and for pre-training, to detect code vulnerabilities. The base model was instantiated using ResNet architectures to extract features from the ISO image and learn deep features. We also employed convolutional neural networks (CNN) to classify the features extracted by the ResNet model and identify vulnerabilities in the ISO image. It was important to freeze the layers from the pre-trained model because we did not want the weights in those layers to be re-initialised. We performed experiments on three sets of datasets containing vulnerable and non-vulnerable C and C^{++} functions. The first three datasets (LibPNG, PidGIN, and VLC) were collected from publicly available resources. They contained a total of 118 vulnerable and 15,318 non-vulnerable source code files. To address the class imbalance problem, the researchers also included 5,200 vulnerable sample C/C^{++} files from the Draper Vulnerability Detection in Source Code (VDISC) dataset. The collected files were split into a 9:5:5 ratio to get the training, validation, and test sets. The resulting dataset consisted of 9817, 5453, and 5453 source files for the training, validation, and test sets, respectively.

Tab. 2. Technology stack

Software / Hardware	Version
Platform/OS	Ubuntu 18.04.6 LTS
Processor	Intel Core i7-9700K, frequency 3.6 GHz, maximum turbo frequency 4.90 GHz, 8 CPU cores, 8 threads
System architecture	64-bit operating system and processor
Memory (RAM)	16 GB
Framework	Ganache, Truffle, Plasma, Pre-trained model: RoBERTa,
Ganache	2.5.4 Lightweight Ethereum blockchain network
Node.js	16.15.0 JavaScript runtime environment for building blockchain network
Truffle	5.5.16 Framework for writing and deploying smart contracts
Web3.js	1.7.3 JavaScript library for interacting with the Ethereum blockchain
IPFS	0.13.0 Distributed peer-to-peer file system for storing data
IPFS HTTP Client	53.0.1 JavaScript library for interacting with IPFS
Smart contract	Solidity v0.8.21

Blockchain-based decentralised environment: An Ethereum client was locally instantiated by deploying ganache-cli and with JSON RPC live at port 8545. Ganache enabled the upload of smart contracts onto Ethereum and launched custom-built DApp. The Truffle framework hosted the DApps with a nested chain structure that had contract codes, migrations, and truffle.js. Web3.js facilitated interaction between smart contracts and the blockchain [71]. The Metamask extension was used for browser support. The plasma contract was designed to track and archive only final on-chain proofs, to counteract multiple exits at an indistinguishable range. The contract maintained a list of exitable maps that were updated on the issue of each on-chain proof and the transaction hosted at Ethereum [72]. A plasma contract called main_chain was deployed to the Ethereum core. MainChain.sol had functions to generate Merkle proof of the issued transactions, validate the signature from the physical nodes, and handle submitted blocks. The child_chain console managed transactions and blocks that were posted when an event was triggered in the main_chain. The child chain contract hosted an RPC server on an 8546 port, that smoothed client interfacing. A Python-based wrapper was scripted for client applications, to wrap with child_chain RPC API.

RESULTS AND DISCUSSION

The development environment was set up in accordance with the technical details listed in Table 2. We evaluated the performance of RoBERT on GRU architecture using different epochs and model sizes. The experiments were conducted on a training set of 9817 source code files and a validation set of 5453 source code files. The model sizes were 8, 32, 64, 128, 256, and 512. The model performance was evaluated on a test set of 5453 source code files. We observed that the accuracy of the models increased linearly with the number of epochs. The accuracy results on the training, validation, and test sets with RoBERTa, for an epoch of 10 and 30, are shown in Fig. 5 and Fig. 6, respectively. GRU with RoBERTa with a model size of 512 achieved a test accuracy of 98% and 97% for an epoch of 10 and 30, respectively. The training accuracy increased with the model size, as larger models can make more complex adjustments to fit the training data. However, this can lead to overfitting, where the model becomes too attuned to the training data and does not generalise new data well. Our findings suggest that the optimal model size for avoiding overfitting is 280. This is the size where the validation accuracy, which measures the model's ability to generalise new data, is highest. The testing accuracy, which measures the model's performance on unseen data, is highest at a model size of 515. This suggests that a model size of 515 strikes a good balance between fitting the training data and generalising it to new data. Model sizes of 10 and 80 show signs of overfitting, as the training accuracy is much higher than the validation accuracy. This is because these models are too complex and have memorised the training data too well. Model sizes 415 and 515 show signs of underfitting, as the training accuracy is much lower than the validation accuracy. This is because these models are not complex enough to capture the inherent complexity of the data.

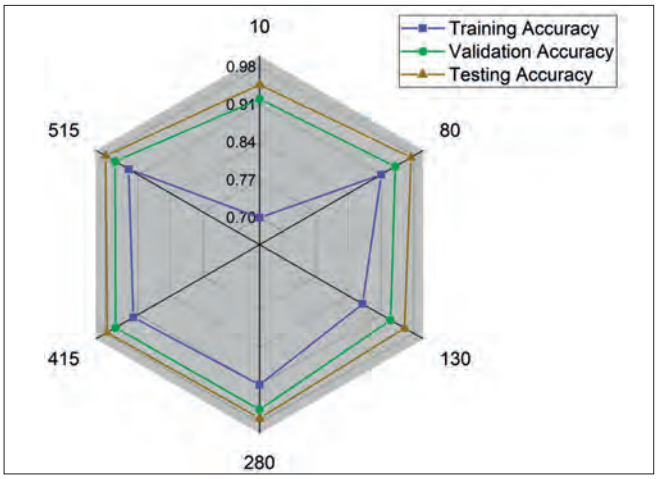

Fig. 5. Accuracy for RoBERTa with 10 epochs on different model sizes

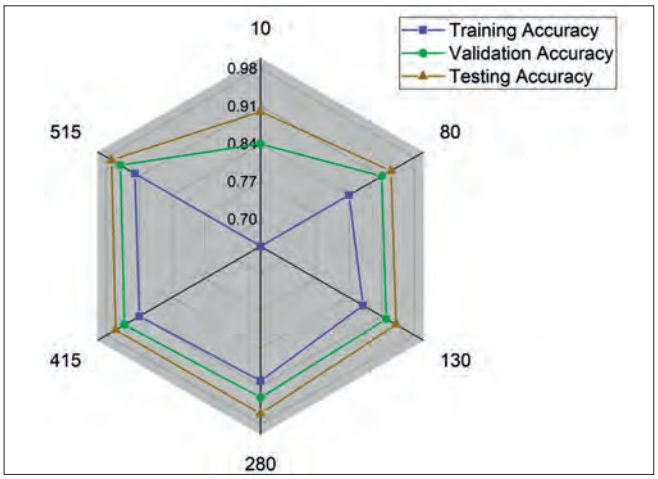

Fig. 6. Accuracy for RoBERTa with 30 epochs on different model sizes

Table 3 shows the performance of the proposed BETL method on two vulnerability datasets: LibPNG and PidGIN. The performance metrics are precision, detection rate, accuracy, and F-score. The results show that BETL on LibPNG has a slightly higher precision and accuracy than on PidGIN. However, the proposed method on PidGIN has a higher detection rate, while BETL on LibPNG is better at avoiding false positives. The computation time of BETL on LibPNG is slightly higher than PidGIN on BETL.

Tab.3. Performance Analysis of Vulnerability Datasets for Proposed BETL method

Measures	LibPNG	PidGIN
Precision	98.99	97.97
Detection Rate	98.98	97.68
Accuracy	97.98	97.12
F-score	98.98	99.02
Computation Time (s)	51.89	49.64

The training loss is the loss that is calculated on the training data, while the validation loss is the loss that is calculated on the validation data. The validation loss is a more accurate measure of the model's performance on unseen data. The results show that the training loss decreases as the model size increases. This is because larger models are able to learn more complex patterns in the data. However, the validation loss does not decrease at the same rate. This suggests that the models are overfitting the training data. The best model size is the one that has the lowest validation loss. In this case, the best model size is 415. This model has a validation loss of 0.0125, as shown in Fig. 7, which is the lowest of all the models. The training loss is always lower than the validation loss. This is because the training loss is calculated on the data that the model has already seen, while the validation loss is calculated on the data that the model has not seen before. The training loss decreases more rapidly than the validation loss, as the model size increases. This is because larger models are able to learn more complex patterns in the data, but they are also more likely to overfit the training data. The validation loss eventually plateaus as the model size increases. This suggests that there is a limit to the amount of improvement that can be achieved by simply increasing the model size.

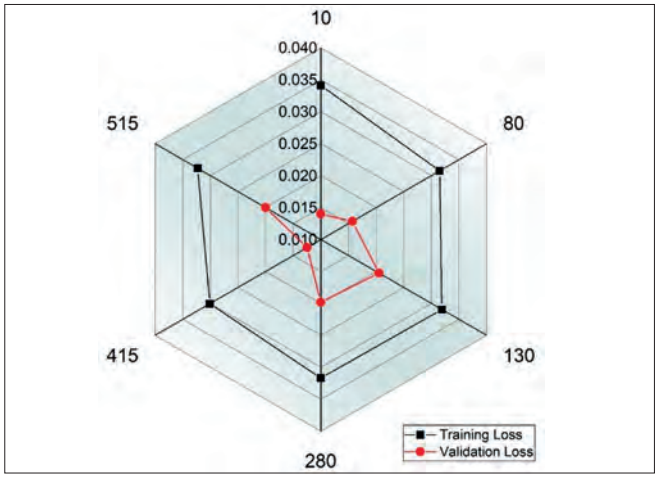

Fig. 7. Loss in RoBERTa pre-training on different model sizes

The training loss decreases as the number of epochs increases for all CNN architectures. This is because the model is able to learn the features of the data better as it is trained for more epochs. The validation accuracy increases as the number of epochs increases for all CNN architectures. This is because the model is able to generalise unseen data better as it is trained for more epochs. ResNet-50 has the lowest training loss and highest validation accuracy for all numbers of epochs. This is because ResNet-50 has more layers and parameters than the other CNN architectures, which allows it to learn more complex features of the data. The difference in training loss and validation accuracy decreases as the number of epochs increases. This is because the model becomes more confident in its predictions as it is trained for more epochs. ResNet-18 has the lowest number of parameters, followed by ResNet-34, ResNet-50, ResNet-101, and ResNet-152. This is because ResNet-18 has the fewest layers. The training time increases as the number of epochs and the number of parameters increases, as depicted in Fig. 8. This is because the model must do more computations to train for more epochs and with more parameters. It is inferred that the ResNet-50 architecture is the best choice since we are dealing with only limited ISO images that require high accuracy.

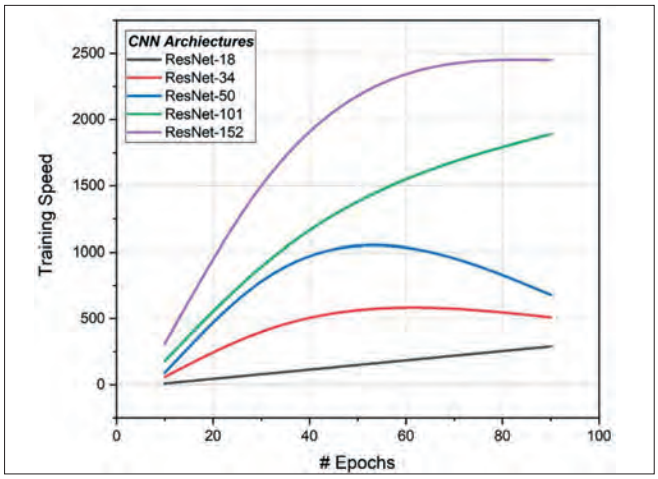

Fig. 8. Model training speed on different epochs

CONCLUSION

We propose a novel BETL system for optimising maritime logistics by harnessing the transparency and immutability of blockchain and the analytical capabilities of transfer learning. We developed a non-vulnerability score range map for the effective classification of operational factors. To ensure efficient storage over the blockchain, we seamlessly integrated IPFS with the blockchain and conducted a testbed-based experiment to demonstrate the effectiveness of BETL for secure logistic management. The results of the experiment show that BETL can achieve high precision (98%), detection rate (98.98%), accuracy (97.9%), and F-score (98.98). This highlights the benefits of BETL in enhancing the safety and reliability of maritime logistics processes. Additionally, the computational time of BETL was improved by 18.9%, compared to standard transfer learning. Beyond its present application, BETL has the potential to extend its utility to other areas of maritime logistics, such as port operations and cargo management. Furthermore, we envision enhancing the usability by incorporating a user-friendly graphical interface for a seamless experience.

REFERENCES

1. A. T. Hoang *et al.*, "Technological solutions for boosting hydrogen role in decarbonization strategies and net-zero goals of world shipping: Challenges and perspectives," *Renew. Sustain. Energy Rev.*, vol. 188, p. 113790, Dec. 2023, doi: 10.1016/j.rser.2023.113790.

2. S. C. Nita and A. Hrebenciuc, "The Importance of Maritime Transport for Economic Growth in the European Union: A Panel Data Analysis," *Sustainability*, vol. 13, no. 14, p. 7961, 2021.

3. S. Gómez, A. Carreño, and J. Lloret, "Cultural heritage and environmental ethical values in governance models: Conflicts between recreational fisheries and other maritime activities in Mediterranean marine protected areas," *Mar. Policy*, vol. 129, p. 104529, 2021.

4. A. Vineetha Harish, K. Tam, and K. Jones, "BridgeInsight: An asset profiler for penetration testing in a heterogeneous maritime bridge environment," *Marit. Technol. Res.*, vol. 6, no. 1, p. 266818, Sep. 2024, doi: 10.33175/mtr.2024.266818.

5. N. Agarwala and C. Saengsupavanich, "Oceanic Environmental Impact in Seaports," *Oceans*, vol. 4, no. 4, pp. 360–380, Nov. 2023, doi: 10.3390/oceans4040025.

6. A. T. Hoang *et al.*, "Energy-related approach for reduction of CO2 emissions: A critical strategy on the port-to-ship pathway," *J. Clean. Prod.*, vol. 355, p. 131772, Jun. 2022, doi: 10.1016/j.jclepro.2022.131772.

7. S. Vakili, A. I. Ölçer, A. Schönborn, F. Ballini, and A. T. Hoang, "Energy-related clean and green framework for shipbuilding community towards zero-emissions: A strategic analysis from concept to case study," *Int. J. Energy Res.*, vol. 46, no. 14, pp. 20624–20649, Nov. 2022, doi: 10.1002/er.7649.

8. F. A. Barata, "High cost of logistics and solutions," in *17th International Symposium on Management (INSYMA 2020)*, 2020, pp. 407–410.

9. A. T. Hoang, V. D. Tran, V. H. Dong, and A. T. Le, "An experimental analysis on physical properties and spray characteristics of an ultrasound-assisted emulsion of ultra-low-sulphur diesel and Jatropha-based biodiesel," *J. Mar. Eng. Technol.*, vol. 21, no. 2, pp. 73–81, Mar. 2022, doi: 10.1080/20464177.2019.1595355.

10. L. Bilgili and V. Şahin, "Emission and environmental cost estimation of ferries operating in Lake Van," *Marit. Technol. Res.*, vol. 5, no. 3, p. 262215, Feb. 2023, doi: 10.33175/mtr.2023.262215.

11. V. V. Pham and A. T. Hoang, "Technological perspective for reducing emissions from marine engines," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 9, no. 6, pp. 1989–2000, 2019, doi: 10.18517/ijaseit.9.6.10429.

12. D. M. Bernhofen, Z. El-Sahli, and R. Kneller, "Estimating the effects of the container revolution on world trade," *J. Int. Econ.*, vol. 98, pp. 36–50, Jan. 2016, doi: 10.1016/j.jinteco.2015.09.001.

13. V. D. Bui and H. P. Nguyen, "Role of Inland Container Depot System in Developing the Sustainable Transport System," *Int. J. Knowledge-Based Dev.*, vol. 12, no. 3/4, p. 1, 2022, doi: 10.1504/IJKBD.2022.10053121.

14. T. T. Le *et al.*, "Management strategy for seaports aspiring to green logistical goals of IMO: Technology and policy solutions," *Polish Marit. Res.*, vol. 30, no. 2, pp. 165–187, 2023, doi: 10.2478/pomr-2023-0031.

15. J. Mangan and C. Lalwani, *Global logistics and supply chain management*. John Wiley & Sons, 2016.

16. Y. Shou, M. Kang, and Y. W. Park, "A Systematic Literature Review of Supply Chain Integration," in *Supply Chain Integration for Sustainable Advantages*, Singapore: Springer Singapore, 2022, pp. 9–29. doi: 10.1007/978-981-16-9332-8_2.

17. M. D. Nguyen, K. T. Yeon, K. Rudzki, H. P. Nguyen, and N. D. K. Pham, "Strategies For Developing Logistics Centres: Technological Trends and Policy Implications," *Polish Marit. Res.*, vol. 30, no. 4, pp. 129–147, 2023, doi: 10.2478/pomr-2023-0066.

18. Y. Zhou, Y. S. Soh, H. S. Loh, and K. F. Yuen, "The key challenges and critical success factors of blockchain implementation: Policy implications for Singapore's maritime industry," *Mar. Policy*, vol. 122, p. 104265, Dec. 2020, doi: 10.1016/j.marpol.2020.104265.

19. V. Isaienko, M. Hryhorak, D. Bugayko, and Z. Zamiar, "Ecosystem Approach to the Formation of Goods Express Delivery Supply Chains in Aviation Logistics," *Logist. Transp.*, vol. 45, no. 1–2, pp. 19–42, 2020.

20. N. Wagner and B. Wiśnicki, "Application of Blockchain Technology in Maritime Logistics," *DIEM Dubrovnik Int. Econ. Meet.*, vol. 4, no. 1, pp. 155–164, 2019.

21. V. Yalama, O. Yakovleva, V. Trandafilov, and M. Khmelniuk, "Future Sustainable Maritime Sector: Fishing Carriers and their Adoption to the Environmental Regulations. Part I," *Polish Marit. Res.*, vol. 29, no. 3, pp. 69–77, Sep. 2022, doi: 10.2478/pomr-2022-0027.

22. H. Fajri, H. Fakhrurroja, and M. Lubis, "Social Media Analysis on Aquaculture SupplyChain Management: A Case Study on Freshwater Lobsters," in *2022 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, Nov. 2022, pp. 01–06. doi: 10.1109/ICADEIS56544.2022.10037283.

23. N. D. K. Pham, G. H. Dinh, H. T. Pham, J. Kozak, and H. P. Nguyen, "Role of Green Logistics in the Construction of Sustainable Supply Chains," *Polish Marit. Res.*, vol. 30, no. 3, pp. 191–211, Sep. 2023, doi: 10.2478/pomr-2023-0052.

24. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

25. H. P. Nguyen, P. Q. p. Nguyen, and V. D. Bui, "Applications of Big Data Analytics in Traffic Management in Intelligent Transportation Systems," *Int. J. Informatics Vis.*, vol. 6, no. 1–2, pp. 177–187, 2022.

26. H. P. Nguyen, P. Q. P. Nguyen, and T. P. Nguyen, "Green Port Strategies in Developed Coastal Countries as Useful Lessons for the Path of Sustainable Development: A case study in Vietnam," *Int. J. Renew. Energy Dev.*, vol. 11, no. 4, pp. 950–962, Nov. 2022, doi: 10.14710/ijred.2022.46539.

27. M. Lind et al., "The future of shipping: Collaboration through digital data sharing," in *Maritime informatics*, Springer, 2020, pp. 137–149.

28. T. Jensen, J. Hedman, and S. Henningsson, "How TradeLens Delivers Business Value With Blockchain Technology," *MIS Q. Exec.*, vol. 18, no. 4, pp. 221–243, Dec. 2019, doi: 10.17705/2msqe.00018.

29. M. E. Manuel and R. Baumler, "The Evolution of Seafarer Education and Training in International Law," 2020, pp. 471–494. doi: 10.1007/978-3-030-31749-2_22.

30. J. Choi, S. Lee, and S. Kim, "Improving the current regulatory issues concerning training ships for maritime institutions: The South Korean case," *Asian J. Shipp. Logist.*, vol. 38, no. 3, pp. 125–134, Sep. 2022, doi: 10.1016/j.ajsl.2022.02.001.

31. S. S. Norman and M. R. Othman, "Reviving the Klang Valley Economy During Pandemic Through Digitalisation of the Maritime Logistics Industry," *J. Marit. Logist.*, vol. 1, no. 2, pp. 40–55, Apr. 2022, doi: 10.46754/jml.2021.12.003.

32. A. Noor, "Adoption of Blockchain Technology Facilitates a Competitive Edge for Logistic Service Providers," *Sustainability*, vol. 14, no. 23, p. 15543, Nov. 2022, doi: 10.3390/su142315543.

33. E. Surucu-Balci, Ç. Iris, and G. Balci, "Digital information in maritime supply chains with blockchain and cloud platforms: Supply chain capabilities, barriers, and research opportunities," *Technol. Forecast. Soc. Change*, vol. 198, p. 122978, Jan. 2024, doi: 10.1016/j.techfore.2023.122978.

34. G. Balci and E. Surucu-Balci, "Blockchain adoption in the maritime supply chain: Examining barriers and salient stakeholders in containerized international trade," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 156, p. 102539, Dec. 2021, doi: 10.1016/j.tre.2021.102539.

35. H. Pyykkö, J. Kuusijärvi, B. Silverajan, and V. Hinkka, "The Cyber Threat Preparedness in the Maritime Logistics Industry," *Proc. 8th Transp. Res. Arena TRA 2020*, 2020.

36. P. Howson, "Building trust and equity in marine conservation and fisheries supply chain management with blockchain," *Mar. Policy*, vol. 115, p. 103873, May 2020, doi: 10.1016/j.marpol.2020.103873.

37. D. Ivanov and A. Dolgui, "Viability of intertwined supply networks: extending the supply chain resilience angles

towards survivability. A position paper motivated by COVID-19 outbreak," *Int. J. Prod. Res.*, vol. 58, no. 10, pp. 2904–2915, May 2020, doi: 10.1080/00207543.2020.1750727.

38. F. Lorenz-Meyer and V. Santos, "Blockchain in the shipping industry: A proposal for the use of blockchain for SMEs in the maritime industry," *Procedia Comput. Sci.*, vol. 219, pp. 807–814, 2023.

39. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.

40. P. Sharma *et al.*, "Comparative evaluation of AI-based intelligent GEP and ANFIS models in prediction of thermophysical properties of Fe3O4-coated MWCNT hybrid nanofluids for potential application in energy systems," *Int. J. Energy Res.*, vol. 46, no. 13, pp. 19242–19257, Oct. 2022, doi: 10.1002/er.8010.

41. Y. Shen, N. Zhao, M. Xia, and X. Du, "A Deep Q-Learning Network for Ship Stowage Planning Problem," *Polish Marit. Res.*, vol. 24, no. s3, pp. 102–109, Nov. 2017, doi: 10.1515/pomr-2017-0111.

42. Q. Shi, Y. Hu, and G. Yan, "Fault Diagnosis of ME Marine Diesel Engine Fuel Injector with Novel IRCMDE Method," *Polish Marit. Res.*, vol. 30, no. 3, pp. 96–110, Sep. 2023, doi: 10.2478/pomr-2023-0043.

43. Z. Said *et al.*, "Intelligent approaches for sustainable management and valorisation of food waste," *Bioresour. Technol.*, vol. 377, p. 128952, Jun. 2023, doi: 10.1016/j.biortech.2023.128952.

44. V. G. Nguyen et al., "An extensive investigation on leveraging machine learning techniques for high-precision predictive modeling of CO 2 emission," *Energy Sources, Part A Recover. Util. Environ. Eff.*, vol. 45, no. 3, pp. 9149–9177, Aug. 2023, doi: 10.1080/15567036.2023.2231898.

45. W. Tarelko and K. Rudzki, "Applying artificial neural networks for modelling ship speed and fuel consumption," *Neural Comput. Appl.*, vol. 32, no. 23, pp. 17379–17395, Dec. 2020, doi: 10.1007/s00521-020-05111-2.

46. K. Rudzki and W. Tarelko, "A decision-making system supporting selection of commanded outputs for a ship's propulsion system with a controllable pitch propeller," *Ocean Eng.*, vol. 126, pp. 254–264, Nov. 2016, doi: 10.1016/j.oceaneng.2016.09.018.

47. T. Kowalewski, A. Podsiadło, and W. Tarełko, "Application of fuzzy inference to assessment of degree of hazard to ship power plant operator," *Polish Marit. Res.*, vol. 14, no. 3, pp. 7–14, Jul. 2007, doi: 10.2478/v10012-007-0012-2.

48. A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "AccessChain: An access control framework to protect data access in blockchain enabled supply chain," *Futur. Gener. Comput. Syst.*, vol. 148, pp. 380–394, Nov. 2023, doi: 10.1016/j.future.2023.06.009.

49. P. Centobelli, R. Cerchione, P. Del Vecchio, E. Oropallo, and G. Secundo, "Blockchain technology for bridging trust, traceability and transparency in circular supply chain," *Inf. Manag.*, vol. 59, no. 7, p. 103508, Nov. 2022, doi: 10.1016/j.im.2021.103508.

50. M. Kandpal, C. Das, C. Misra, A. K. Sahoo, J. Singh, and R. K. Barik, "Blockchain assisted Supply Chain Management System for Secure Data Management," in *2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, Nov. 2022, pp. 1–6. doi: 10.1109/ASSIC55218.2022.10088404.

51. A. S. M. S. Hosen *et al.*, "Blockchain-based transaction validation protocol for a secure distributed IoT network," *IEEE Access*, vol. 8, pp. 117266–117277, 2020.

52. J. Liu, G. Yeoh, L. Gao, S. Gao, and O. Ngwenyama, "Designing a Secure Blockchain-Based Supply Chain Management Framework," *J. Comput. Inf. Syst.*, vol. 63, no. 3, pp. 592–607, May 2023, doi: 10.1080/08874417.2022.2089774.

53. S. M. M. Hamidi, S. F. Hoseini, H. Gholami, and M. Kananizadeh, "Blockchain Capabilities to Improve the Productivity of Maritime Logistics Processes: Review, Taxonomy, Open Challenges and Future Trends," *J. Inf. Technol. Manag.*, vol. 14, no. Special Issue: The business value of Blockchain, challenges, and perspectives., pp. 144–170, 2022.

54. H. Zhong, F. Zhang, and Y. Gu, "A Stackelberg game based two-stage framework to make decisions of freight rate for container shipping lines in the emerging blockchain-based market," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 149, p. 102303, May 2021, doi: 10.1016/j.tre.2021.102303.

55. H. Hasan, E. AlHadhrami, A. AlDhaheri, K. Salah, and R. Jayaraman, "Smart contract-based approach for efficient shipment management," *Comput. Ind. Eng.*, vol. 136, pp. 149–159, Oct. 2019, doi: 10.1016/j.cie.2019.07.022.

56. E. Lambourdiere and E. Corbin, "Blockchain and maritime supply-chain performance: dynamic capabilities perspective," *Worldw. Hosp. Tour. Themes*, vol. 12, no. 1, pp. 24–34, Jan. 2020, doi: 10.1108/WHATT-10-2019-0069.

57. M. Jović, E. Tijan, D. Žgaljić, and S. Aksentijević, "Improving Maritime Transport Sustainability Using Blockchain-Based Information Exchange," *Sustainability*, vol. 12, no. 21, p. 8866, Oct. 2020, doi: 10.3390/su12218866.

58. L. Li and H. Zhou, "A survey of blockchain with applications in maritime and shipping industry," *Inf. Syst. E-bus. Manag.*,

vol. 19, no. 3, pp. 789–807, Sep. 2021, doi: 10.1007/s10257-020-00480-6.

59. Z. H. Munim, O. Duru, and E. Hirata, "Rise, Fall, and Recovery of Blockchains in the Maritime Technology Space," *J. Mar. Sci. Eng.*, vol. 9, no. 3, p. 266, Mar. 2021, doi: 10.3390/jmse9030266.

60. S. Nguyen, p. Shu-Ling Chen, and Y. Du, "Risk assessment of maritime container shipping blockchain-integrated systems: An analysis of multi-event scenarios," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 163, p. 102764, Jul. 2022, doi: 10.1016/j.tre.2022.102764.

61. D. Kim, C. Lee, S. Park, and S. Lim, "Potential Liability Issues of AI-Based Embedded Software in Maritime Autonomous Surface Ships for Maritime Safety in the Korean Maritime Industry," *J. Mar. Sci. Eng.*, vol. 10, no. 4, p. 498, Apr. 2022, doi: 10.3390/jmse10040498.

62. K. H. Kwak, J. T. Kong, S. I. Cho, H. T. Phuong, and G. Y. Gim, "A study on the design of efficient private blockchain," *Comput. Sci. Appl. Informatics 5*, pp. 93–121, 2019.

63. U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 181, p. 103007, 2021.

64. S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2019.

65. M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, 2023.

66. R. Xu, Y. Chen, and E. Blasch, "Decentralized access control for IoT based on blockchain and smart contract," *Model. Des. Secur. Internet Things*, pp. 505–528, 2020.

67. R. Xu, Y. Chen, and E. Blasch, "Decentralized Access Control for IoT Based on Blockchain and Smart Contract," in *Modeling and Design of Secure Internet of Things*, Wiley, 2020, pp. 505–528. doi: 10.1002/9781119593386.ch22.

68. G. Lin, S. Wen, Q.-L. Han, J. Zhang, and Y. Xiang, "Software vulnerability detection using deep neural networks: a survey," *Proc. IEEE*, vol. 108, no. 10, pp. 1825–1848, 2020.

69. B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "iBlock: An Intelligent Decentralised Blockchain-based Pandemic Detection and Assisting System," *J. Signal Process. Syst.*, vol. 94, no. 6, pp. 595–608, Jun. 2022, doi: 10.1007/s11265-021-01704-9.

70. D. Trautwein *et al.*, "Design and evaluation of IPFS," in *Proceedings of the ACM SIGCOMM 2022 Conference*, Aug. 2022, pp. 739–752. doi: 10.1145/3544216.3544232.

71. S. K. Panda and S. C. Satapathy, "An investigation into smart contract deployment on Ethereum platform using Web3.js and solidity using blockchain," in *Data Engineering and Intelligent Computing: Proceedings of ICICC 2020*, 2021, pp. 549–561.

72. G. D'ANGELO and p. F. COSTA, "Ethereum blockchain as a decentralized and autonomous key server: storing and extracting public keys through smart contracts," 2017.