Grenze International Journal of Engineering and Technology, June Issue

Data Sharing Techniques for Maritime Traffic Route Detection and Transport Communication (MTRTC)

KN Balasubramanian[1], S Sanjeet[2], B Bharath[3] and M R Sumalatha[4]
[1-4]Department of Information Technology, Anna University -MIT Campus, Chennai, India
Email: balasubramaniankn11@gmail.com, ssanjeet2001@gmail.com, bbharathboopathy@gmail.com, sumalatha@annauniv.edu

***Abstract*—Maritime is one of the most interconnected indus- tries in the world, this sector involves the international transit of a wide range of commodities and documents. There is also a probability of intruders with nefarious intentions who may try to modify the data which is to be shared. Human errors are very likely to happen while transmitting confidential information across any network. Maritime transport not only involves cargo shipping, but, Navy also falls under this category. The messages are to be transferred between the ships as well as on the shores. In those situations the messages can be tampered in between and the confidential data can be spoofed by any intruder in the middle. For that purpose , a social community network of maritime users that can aid ships in distress situations is created. These communities are secured using public blockchain and cryptographic tools (RSA and DSA). Route detection techniques are used to map the correct distance between two ships. If a user observes any illegal activity in ships docked off-shore, he/she can choose to share the relevant information to the authorities very securely after validating the users on both ends of the network.**

***Index Terms*— Blockchains, Digital Signature, Community Net- work, Geolocation, Route Detection.**

I. INTRODUCTION

In the maritime industry, and the exponential development of the Marine Internet-of-Things(MIoT), ships still face many types of difficulties like shortage of food, fuel or any accidents etc. There is also a probability of intruders with nefarious intentions who may try to modify the data which is to be shared. Maritime transport accounts for roughly 90% of global trade volume. With the persistent increase in economy at global level, this industry has proportionally grown in terms of vessel capacity and volume [1]. In such situations, the security of the messages to be transferred is much more important. For assurance of security to the user, RSA cryptographic algorithm and Digital Signature has been used for validation purposes. RSA [2] is a well-known, and well-established asymmetric cryptography protocol. Current state-of-the-art RSA algorithms are sufficient to protect many digital assets. The concept of RSA is based on the fact that it is difficult to factorize a large integer. The public key is made up of two numbers, one of which is a multiplication of two large prime numbers. Furthermore, the private key is derived from the same two prime numbers. If someone can factorize the large number, the private key is compromised. As a result, encryption strength is entirely dependent on key size, and increasing the key size doubles or triples the encryption strength exponentially. Digital Signature checks the authenticity and integrity of digital messages and documents using a sophisticated mathematical technique. It

Grenze ID: 01.GIJET.9.2.22_1

guarantees that the contents of a message are not altered while in transit and aids in the prevention of impersonation and tampering in digital communications. Digital signatures also include additional information such as the message's origin, status, and signer consent. Digital signatures are legally binding and have the same value as traditional document signatures in many regions, including parts of North America, the European Union, and APAC. In addition to digital document signing, they are used in financial transactions, email service providers, and software distribution, all of which require the authenticity and integrity of digital communications. Public key technology is an industry standard infrastructure which ensures a digital signature's data authenticity and integrity. Digital signing solution providers will generate two keys: a public key and a private key using a mathematical algorithm. When a signer digitally signs a document, a cryptographic hash is generated for the document. This cryptographic hash is then encrypted with the sender's private key, which is kept safe in an HSM box. It is then appended to the document and forwarded to the recipients, along with the sender's public key. The recipient can use the sender's public key certificate to decrypt the encrypted hash. On the recipient's end, another cryptographic hash is generated. Both cryptographic hashes are compared to ensure their authenticity. If they match, it means the document hasn't been tampered with and is therefore valid. Social communities are made up of a group of people who share similar interests. They are formed for many reasons—keeping each other up to date on relevant topics, forming bonds with like-minded people, or even just enter- tainment. Most online communities are not created to easily expand to other groups and topics, and this is according to the intended design. Rather, they are typically tight-knit and consist of devoted users who discuss a subject more deeply and technically than the general public.

II. Related Works

Keke Gai et al [3] implemented blockchain-based data sharing for maritime IoT, protecting privacy and enabling decision-making. The approach uses zero-knowledge proofs and commitment-based privacy to protect vessel identities while allowing data sharing. The system was implemented by decentralizing Edge Computing Nodes and using blockchain contracts to provide Common Positioning Vessels with accurate positioning data. The project prioritizes privacy, unlikability, and fairness, with confidential information hidden, sender-receiver linkage restricted, and account balances validated before transactions. The project did not focus on real-time deployment or routing rules. Security and performance evaluations show the effectiveness of the approach.

J.S. Lee et al [4] have analyzed country and geographic factors as well as the qualities of the ships, several maritime commerce routes are used by ships. There are restricted routes in oceanic zones. This study derives quantitative traffic routes using data from an automatic identification system (AIS). Pre-processing done on the AIS data. The waypoints of vessels are identified using density-based spatial clustering of applications with noise (DBSCAN), and routes are then built by connecting waypoints. Initial AIS data analysis by KDE appears to have almost passed in the ocean region. In general, it is possible to establish which parts of the ocean ships can navigate. The Douglas-Peucker algorithm simplifies the AIS trajectory by employing a similar pattern. Additionally, density-based spatial clustering of applications with noise (DBSCAN) can be applied.

B. Murray et al [5] have suggested that the presence of numerous comparable clusters has a negative impact on the overall method . The automated identification system (AIS) monitors vessel movement through the computerized exchange of navigational data between vessels. The study investigates AIS data sources and relevant navigational elements, such as traffic anomaly detection and route estimation, in situations where such data are or may be used to ensure the safety of seafarers. The effectiveness and capability of online learning. With new data, the normality models can be dynamically modified. Users understand the learned model because it is simple to superimpose on a map of a location. Using anomaly detection methods, it creates normality models from historical data. divided into two groups: Methods based on geographic models (map-dependent) which construct region- specific computer models trained on local traffic data and superimposed on a geographical map of the locale to de- tect anomalies. Parametrical (map-independent) model-based methods construct normalcy parametric models independent of training region maps.

According to Enmei Tu et al [6], the Potential Field Method (PFM) has a limitation in the formulation of normalcy because it does not take ship direction information into account. The maritime transportation system is just one of many industries that has benefited greatly from the ongoing development of internet of things (IoT) technology (MTS). However, there are other concerns, such as attacks on interruption, security, and privacy. As a potential solution to this problem, an IoT- enabled maritime transportation communication system has been proposed. This system takes advantage of blockchain's unique features to address network security and reliability concerns. It is suggested that a distributed IoT-enabled maritime transportation communication system

be developed that takes advantage of the blockchain's unique structure to address network security and reliability issues.

According to Tingting Yang et al [7], a decentralized network is robust and can withstand node outages. The use of blockchain technology allows the network as a whole to incorporate computational resources to support a variety of tasks. The problem cannot be modified if the restrictions do not include any priority constraints. Due to the buoy's limited energy, a trade-off between performance and energy must be made. The scheme proposed by Y.Lu. et al. [8] outperforms and is more accurate than the two baseline methods with which it was compared. The results show that the proposed scheme achieves good accuracy and convergence. Providers face significant data security and privacy risks when using centralized methods. The cost of running the blockchain scheme rises in direct proportion to the number of participants and transactions. A blockchain network is used to help the cloud server store data, and smart contracts are used to provide dependable storage interfaces. Another important aspect addressed in the paper was the introduction of an efficient consensus mechanism to improve the efficiency of the consensus process.

Hongzhi Li et al. [9] have proposed a blockchain-assisted secure storage scheme for logistics data; this scheme can be divided into two parts. The first stage entails data generation and aggregation, session establishment, record encryption and storage, and the use of a blockchain network to assist the cloud server with data storage, and the deployment of smart contracts to provide reliable storage interfaces. The use of asymmetric encryptions and the establishment of session communication ensure the privacy of logistics data. The immutability and auditability of logistics data is ensured by a consortium blockchain based on edge devices. As the logistics information system involves numerous processes and entities, the proposed scheme only considers the most basic scenario abstraction, making it far from practical logistics application. The data storage capacity of distributed blockchain nodes is not fully considered.

P. Zhang et al [10] has proposed a scheme using Marine Transportation Systems (MTS). MTS also requires a shared and controlled access mechanism that cannot be manipulated or tampered with by unauthorized parties. Because of its non- tampering and non-forgery properties, blockchain has emerged as a critical tool in data security protection. Keeping this in mind, this paper proposes an IoT-based collaborative pro- cessing system based on blockchain for marine transportation flow scheduling and management. In addition, the authors propose a novel consensus mechanism based on Verifiable Random Function (VRF) and reputation voting to reduce the communication cost in the blockchain consensus communication process. The proposed scheme was validated in a simulated environment, and the results show that the scheme has a noticeable effect in resisting replay attack and camouflage.

Yi Yang et al. [11] attempted to address the issue of the IoT-enabled Maritime Transportation System (IMTS) in order to improve its ability to maintain privacy, continuously perform, and add the function of joint management. Despite the fact that many aggregate signcryption (ASC) schemes have been proposed to meet this requirement, they all have performance or security flaws. Based on this network model, the authors propose an efficient identity-based aggregate sign- cryption scheme with blockchain (B-ID-ASC) for PNA-IMTS. According to the security analysis, the B-ID-ASC scheme can provide confidentiality and unforgeability. It can also withstand existing known attacks (impersonation attack, modification attack, man-in-the-middle attack). According to the results of the performance analysis, our B-ID-ASC scheme has lower computation and communication costs than current ASC schemes and thus is more applicable for PNA-IMTS. The authors created a secure information sharing scheme based on identity for the maritime transportation system while maintaining proper authentication measures. For authentica- tion management, the proposed method employs the concept of identity-based encryption. The approach is IND-sID-CCA secure and works well with maritime IoT devices.

According to B. B. Gupta et al. [12] since the maritime transportation system ensures the safety of the vessel's pas- sengers, manages the vessel's route to avoid collisions, and monitors the vessel's condition during the journey. All tasks performed by the maritime transportation system necessitate continuous monitoring of the vessel's performance, which is accomplished through the use of IoT devices. The IoT devices collect and transmit data about the vessel's physical parame- ters to coast-side servers. Because the shared data contains sensitive information about the vessel, secure data sharing techniques are required, allowing only authorized individuals to access the data received from maritime IoT devices.

P. Rahimi et al. [13] proposed a secure communication system for Maritime IoT applications using blockchain technology. The proposed system uses different layers such as the application, blockchain, and communication layers. The system aims to provide secure and reliable communication between IoT devices and nodes involved in maritime applications.

III. Proposed Work and System Design

In the maritime industry, and the exponential development of the Marine Internet-of-Things(MIoT), ships still face many types of difficulties like shortage of food, fuel or any accidents etc. There is also a probability of intruders with nefarious intentions who may try to modify the data which is to be shared. Maritime approximately supports ninety percent of the trade volume globally. With the persistent increase in economy at global level, this industry has proportionally grown in terms of vessel capacity and volume. In such situations, the security of the messages to be transferred is much more important. The proposed solution starts off with the creation of a social community network-i.e. the network comprises the ships and respective authorities registered under the community. The ship, which is in an emergency situation, sends a public message through the multi-channel interface (many to many communication) to all the registered users in the community. The messages are stored in the public blockchain using smart contracts. Any nearby vessel can locate them and provide the necessary help after retrieving the messages from the block. Similarly, the ship which requires a help can use the navigate option available and search for the nearest ships within the community and send a private message to that particular person alone.

In the second case, when a ship is standing on shore and detects any illegal activity taking place in the nearby ship or besides it, then it can send a two step secured private message to the higher authorities. When a ship wants to communicate privately, then the captain of the ship signs in to the interface and navigates to the particular authority chat interface. Before the confidential messages are sent they are encrypted using the public key of the receiver and they are stored as a block using the smart contract. The messages sent by any user are tagged with the geo-location such that to perform easy navigation by the authorities. The contract address of the blocks are sent via the channel. On the receiver end, the contract address is first converted, then the private key of the receiver is used to unlock the message. Thus these processes ensure two step security at both the levels. This process is represented in Fig. 1.

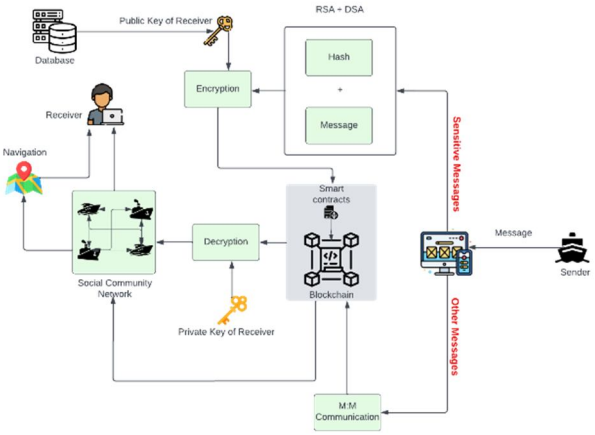

Figure 1. MTRTC Architecture Diagram

IV. Scope of this Proposal

The scope of the project involves these following steps:

1. Creation of the Social Community Network: Using the location of the ship in question, identifying the nearest cluster of ships or higher authorities which can offer assistance in case of any emergency. Social community network is to be established because these ships are clustered in a particular area and will have common features among them and to share the information among them.
2. Route Detection: In order to guide a rescue ship to a ship that has relayed a distress call, a route detection algorithm is used by the rescue ship to find the shortest path to the other ship for a quick rescue or any other emergency operations.
3. Secure Communications with Blockchains: All and any type of communications transmitted and received by the ship is to be secured by blockchain technology at the first level. This is done to prevent any outside interference which can manipulate important data or sensitive information. Providing an additional layer of protection to important data of the ship can help in a much safer trip.
4. User Validation: The messages needed to be passed through a second layer of security such that the message goes on to the valid or correct receiver. A RSA based signature is developed to validate the

receiver. As public blockchain is used in this proposal, so the contract address of the messages are encrypted, such that no other user within the same community can spoof the details.

V. Experimental Analysis

Various new strategies have been implemented in this proposal to bring out new changes in the technology of information sharing within a social community. The data needs to be secured when the information is sensible and on the other hand they need to be delivered to the right person within the community of similar domain. These processes are carried out in this proposal and they have been explained below.

A. Blockchain

A simple public Block chain has been implemented using the ganache suit. Smart contracts are built such that it could store the required message in terms of bytes and the geoloca- tion information for navigation purposes. The smart contract has been created using solidity language and deployed with the usage of python libraries. Web3 package is used to connect the Ganache suite, It is used to quickly launch a private Ethereum blockchain on which to execute tests, commands, and to observe state while managing how the chain functions, using solidity code. After the implementation of the smart contracts, they are converted into json format using solcx. From this json file, the bytecode and abi value are retrieved for processing purposes. Now, from the ganache suit, a dedicated account is chosen and its address and private key are copied such that to create contracts on that particular account.

The process of blockchain includes: Building, Signing and Sending and getting receipt of the transaction. Once these processes have been completed, then, the data stored in the contracts are accessed separately using the contract address of a particular block. The values of each member are accessed using separate function calls. When a transaction is completed, the required number of ethers gets reduced accordingly.

B. Message Confidentiality and User Integrity

The sensitive messages are sent when a ship anchored on the shore or moving on the water surface watches any illegal activity happening nearby. The ship captain has the responsibility to send secure information or the details related to the activity to the higher authorities. As the messages are to be kept confidential, they are passed through two level security processes and sent over the network. When the security bleach happens then the information can be read by others in the same community as public blockchain is used in this proposal. The sensitive messages are sent through the one to one interface privately to the higher authorities or the receiver. The information along with the geoinformation tag are first hashed using the SHA 1 hash function. The result hash value and the original message are combined and sent to the encryption step. The public key of the receiver is used to encrypt the information from the previous step using Rivest Shamir Adleman(RSA) algorithm. This encrypted message is stored inside the blocks. The representation of these steps are shown in Fig. 2

On the receiver end, the message from the block is retrieved using the block contract address and decrypted using the private key of the receiver. Once the information is decrypted, then they are split up into the message and the hash value. Now this message is passed on to the SHA 1 hash function and the corresponding hash value is obtained. At this stage the two hash values are compared, if they are matching then the user validation is successful, such that the message is received by the valid user. If the hash values are not matched then the messages will not be delivered to that person. The basic flow of the above mentioned steps are shown in the Fig. 3

The message at the sender side to ensure confidentiality and authenticity is first hashed and this is combined with the original message. This new combination is now encrypted using the public key of the receiver and stored inside the blockchain as blocks. On the receiver end, first the blocks are decrypted using the block address followed by decryption of the combined message using the private of the receiver. Then the splitting of the message and hash is carried out such that the message is further hashed and compared with the received hash to check the correctness of the message. Later the message is received by the receiver. The overall algorithm for data sharing after ensuring confidentiality using Blockchain and RSA is explained in Algorithm 1.

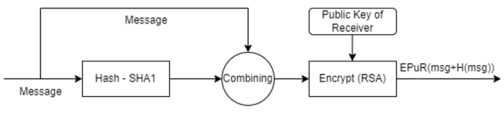

Figure 2. Encrypting the information

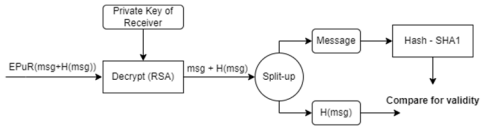

Figure 3. Decryption and user validation

C. Social Community Formation

Social networks are necessary for every domain application. In this proposal, the navy community has been chosen as a domain and a network is built within the organization to maintain a secure and safe communication. A common definition of social community has usually included three ingredients: Interpersonal networks that offer social support, sociabil- ity and social capital to their members, Residence in a populated area, for instance a neighborhood and Solidarity feelings and actions. When a message needs to be transmitted just to their groups, social interactions become vital so that people outside the community are unaware of it.

A community is built using the django framework such that it provides the server to process the requests. When a super user sends the message to the respective receiver, at that time, the sensible messages and the user's geolocation are digitally signed and stored inside the blockchain in the form of hashed bytes and they are sent through the network. Once the block is created, its contract address is used to receive the sent message on the other hand and the messages are decrypted. The respective sender and receiver nodes details are stored accordingly, such that they can be loader everytime. Ajax is used on the web pages to create asynchronous web pages and the contents get refreshed every few seconds. A navigation button is provided in this interface to track where the receiver and the senders are present. The recent message sent by the sender is noted and along with this the receiver's geolocation is noted and the navigation map is displayed on the receivers user interface for easy tracking.

A social community along with blockchain is built to send and receive messages and other information securely. Here the nodes are represented as the super users in the community. First the respective persons are selected and they are required to sign up as the super users such that they can alone access the community communication interface. Once the process is completed, the users are ready to send or receive the messages effectively.

Algorithm 1 Data Sharing in the Community

Input: User Message: M_0, Sender Location: G_s
Output: Messages sent from the user: M_r

Initialisation : Pu_{rec} ← Public key of the receiver
Pr_{rec} ← Private key of the receiver
Pr_{bck} ← Private key of the blockchain account
M_r ← Received message from the network
B_{msg} ← Retrieving data from block with M_r and Pr_{bck}
D_{msg} ← Decrypting the B_{msg} using RSA and Pr_{rec}
C ← counter to keep track of message
H_n ← Generating hashcode with M_{rec}

while $True$ **do**
  if $Sending$ **then**
    M_c ← Combining M_o and G_s.
    H_{sha1} ← Generating hashcode with M_c
    $M_{nc} \leftarrow H_{sha1} + M_c$
    E_{msg} ← Encrypting the M_{nc} using RSA and Pu_{rec}
    B_{add} ← Storing E_{msg} in blocks using Pr_{bck}
    B_c ← Creating a contract address with the block B_{add}
    $M_r \leftarrow B_c$
  else
    for $M_0 = 0$ to length(D_{msg}) **do**
      if $D_{ms}[M0] =$ '+' **then**
        $C \leftarrow 1$
      else if $C = 0$ **then**
        M_{rec} ← append $D_{msg}[M_0]$
      else
        M_{hash} ← append $D_{msg}[M_0]$
      end if
    end for
    if $H_n = M_{hash}$ **then**
      M_r ← Message successfully received
    else
      Print user invalid
    end if
  end if
end while
return M_r =0

Many to many communications or insensible help messages interface has been implemented in Django by the creation of a room in which multiple users can interact with each other by logging in using the similar group name. After entering, the credentials are obtained using the cookies, one can use the common interface in which all the users who have entered the room can see their previous history of messages if they have entered the same room. All the participants can interact with each other simultaneously, such that the messages are stored inside the blocks and the messages are refreshed continuously every time. These messages are sent along with the timestamp. If a user wants to check for other closer users, then he can click on to the navigate button and can view the list of information about various users within the network along with their distance from the sender's vessel.

VI. Performance and Results

An interactive application that simulates a social community network is built so that it can respond to emergency situations quickly and efficiently. In case of a ship capsize or any other untoward situation, this app can be used to send alerts to all the users in the network using the second part of the proposal. The location of the ship in crisis and the network members is found and the location is mapped for easy identification. The coordinates of both the party ships along with the distance between them are also displayed. There is also an option of one-one

interaction enabled to send any private messages using two layer security. For each message sent, the location coordinates are tagged and sent through the network. Getting the coordinates of the ship with a high percentage of accuracy will be useful in saving lives. The application uses a database to store the details of all the ships in the network. In case of a SOS situation, there is an option for the ship captain to interact with other users privately or to interact with other users simultaneously in a room-like interface. For the both use cases, the first layer of security is that messages sent have been secured using blockchains.These codes will be converted into the real message at the receiver side. The second layer of security is user validation using RSA enabled digital signature.

The User Interface for the one to one communication and many to many communications has been implemented using Ajax, HTML and CSS with a Django as the backend server. All the users connected can interact with each other simultaneously. The MTRTC system performance is analyzed by using the time module available in python to make a note on the time taken for the message or the data to be shared from a particular sender to the receiver. The messages are divided into 4 categories based on the bytes of data ranging from 50 to 200 with increments of 50. Four algorithms namely Direct, using Blockchain alone, using RSA alone and combination of RSA and Blockchain are used to test the performance of the system effectively. Direct here refers to the messages that are not encrypted or stored using any of the other algorithms. The time taken for message sharing depending on the bytes transferred is shown in Table I.

TABLE I. PERFORMANCE OF MTRTC

Input size (bytes)	Time Taken for Message Sharing			
	Direct	Blockchain	RSA	RSA + Blockchain
50	0.958	2.164	1.054	2.215
100	0.994	2.451	1.364	2.451
150	1.004	2.658	1.565	2.864
200	1.014	3.021	1.805	4.161

From the above it is evident that the time taken for sharing the messages attains its maximum value of 4.161 sec when 200 bytes of data is sent. It is evident that the execution time nearly depends on the complexity of the process to share the messages within the network. The line graph plotted in Fig. 4 represents the effectiveness of the MTRTC system. The graph contains x-axis as the byte size and y-axis as the time taken to send and receive messages. The graph represents the efficiency and the performance analytics of the security measures used to secure the messages. It is very clear that RSA+ Blockchain combination takes the most time but is the most efficient.

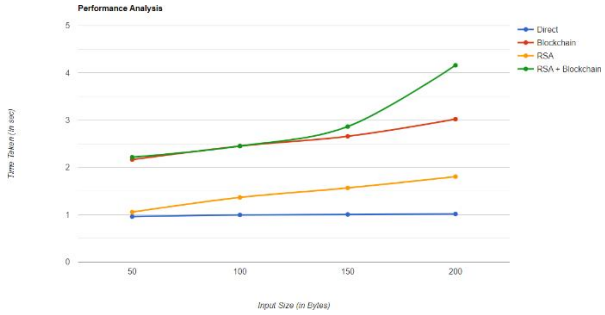

Figure 4. Performance of MTRTC in message sharing

VII. CONCLUSIONS

Communication among ships through a social community is secured using blockchain such that the users registered within the same community can use it effectively for one to one or many to many types of communication during emergency situations. A two layer security approach is also implemented for transferring sensitive information within the community. This project work discusses in depth about the methods that have been used to implement the transmission and reception of the information and to provide services during emergency in an effective way. The preliminary results of the proposed work out performs the existing system.

Additionally route detection strategies have been used with the help of folium maps python library in order to guide the users about the location. In the future, additional route optimization algorithms can be used and also Artificial Intelligence and Machine Learning can be integrated in order to bring more stability and intelligence to this project.

REFERENCES

[1] Zhang, X., Fu, X., Xiao, Z., Xu, H. and Qin, Z., 2022. Vessel trajectory prediction in maritime transportation: current approaches and beyond. IEEE Transactions on Intelligent Transportation Systems.

[2] R. Patgiri and L. D. Singh, ”An Analysis on the Variants of the RSA Cryptography,” 2022 International Conference on Information Network- ing (ICOIN), 2022, pp. 40-45, doi: 10.1109/ICOIN53446.2022.9687262.

[3] K. Gai et al., ”Blockchain-Based Privacy-Preserving Positioning Data Sharing for IoT-Enabled Maritime Transportation Systems,” in IEEE Transactions on Intelligent Transportation Systems, 2022, doi: 10.1109/TITS.2022.3190487.

[4] J. -S. Lee, H. -T. Lee and I. -S. Cho, ”Maritime Traffic Route Detection Framework Based on Statistical Density Analysis From AIS Data Using a Clustering Algorithm,” in IEEE Access, vol. 10, pp. 23355-23366, 2022, doi: 10.1109/ACCESS.2022.3154363.

[5] B. Murray and L. P. Perera, “An AIS-based deep learning framework for regional ship behavior prediction,” Rel. Eng. Syst. Saf., vol. 215, Nov. 2021, Art. no. 107819.

[6] E. Tu, G. Zhang, L. Rachmawati, E. Rajabally and G. -B. Huang, ”Ex- ploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey From Data to Methodology,” in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, pp. 1559-1582, May 2018, doi: 10.1109/TITS.2017.2724551.

[7] T. Yang, Z. Cui, A. H. Alshehri, M. Wang, K. Gao and K. Yu, ”Distributed Maritime Transport Communication System With Re- liability and Safety Based on Blockchain and Edge Computing,” in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3157858.

[8] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous Federated learning for secure data sharing in internet of vehicles,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4298–4311, Apr. 2020.

[9] H. Li, D. Han and M. Tang, ”A Privacy-Preserving Storage Scheme for Logistics Data With Assistance of Blockchain,” in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4704-4720, 15 March15, 2022, doi: 10.1109/JIOT.2021.3107846.

[10] P. Zhang, Y. Wang, G. S. Aujla, A. Jindal and Y. D. Al-Otaibi, ”A Blockchain-Based Authentication Scheme and Secure Architecture for IoT-Enabled Maritime Transportation Systems,” in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3159485.

[11] Y. Yang, D. He, P. Vijayakumar, B. B. Gupta and Q. Xie, ”An Efficient Identity-Based Aggregate Signcryption Scheme With Blockchain for IoT-Enabled Maritime Transportation System,” in IEEE Transactions on Green Communications and Networking, vol. 6, no. 3, pp. 1520-1531, Sept. 2022, doi: 10.1109/TGCN.2022.3163596.

[12] B. B. Gupta, A. Gaurav, C. -H. Hsu and B. Jiao, ”Identity-Based Au- thentication Mechanism for Secure Information Sharing in the Maritime Transport System,” in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3125402.

[13] P. Rahimi, N. D. Khan, C. Chrysostomou, V. Vassiliou and B. Nazir, "A Secure Communication for Maritime IoT Applications Using Blockchain Technology," 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, CA, USA, 2020, pp. 244-251, doi: 10.1109/DCOSS49796.2020.00047.