Enhanced Cyber threat intelligence in IOT enabled maritime transportation systems through deep learning-based modelling and Identification

Madhav Krishna[1], Dr. V. Uma Rani[2]
[1] *Student, M. Tech (Computer Networks and Information Security), Department of Information Technology, JNTU Hyderabad, Hyderabad, India*
[2]*Proffesor, CSE, Department of IT, JNTUH*

Abstract: **The proliferation of IoT technologies in the maritime sector has revolutionized Maritime Transportation Systems (MTS), enabling seamless communication between smart maritime objects and associated infrastructure. However, this interconnectedness exposes MTS to cyber threats, underscoring the need for advanced security measures. Traditional CTI-based solutions often suffer from low detection rates and high false alarms, highlighting the necessity for innovative approaches. The primary objective of this project is to develop an automated framework, DLTIF, to enhance the security of IoT-enabled MTS. DLTIF aims to address the limitations of existing CTI-based solutions by employing deep learning techniques for threat detection and identification. Specifically, the framework focuses on improving detection accuracy, reducing false alarms, and providing early warning of cyber threats. The proposed DLTIF framework demonstrates promising results, achieving up to 99% accuracy in threat detection. Through rigorous evaluation and comparison with traditional and state-of-the-art approaches, DLTIF consistently outperforms existing methods, highlighting its effectiveness in enhancing the security posture of IoT-enabled MTS. And also added CNN and ensemble methods, like CNN+LSTM and Stacking Classifier (RF+MLP+LGBM), are incorporated for boosting accuracy and robustness. Stacking Classifier's impressive 100% accuracy validates ensemble approaches. Additionally, a Flask-based interface streamlines user testing, with built-in authentication ensuring security and access control. This broadens project capabilities with advanced modeling techniques and user-friendly implementation.**

Index Terms: Cyber-attack, cyber threat intelligence, deep learning, the Internet of Things (IoT), maritime transportation systems (MTS), threat type identification.

I. INTRODUCTION

Due to the affordability, and availability of low-cost Internet of Things (IoT) sensor, the number of embedded devices used in maritime world is rapidly increasing [1], [2]. This raises interest in Maritime Transportation Systems (MTS), which is a vast network of sensors or infrastructure associated with ship, port, or the transportation itself, such as bridge navigation systems, containers, cranes, shore-based facilities, autonomous underwater vehicles etc., [3]. Typically, such system is connected to enterprise network via heterogeneous communication infrastructure over an open channel Internet [4].

This integration gives immense flexibility and versatility in the management of inter-maritime processes intelligently, resulting in improved productivity and resource utilization [5]. However, this convergence, and always online nature of IoT devices exposes the MTS network to serious security risk and makes entire transportation system vulnerable to devastating cyber-attacks [6]. In IoT-enabled MTS, there are two types of attacks: physical and cyber. Physical attacks attempt to manipulate hardware components directly, whereas cyber threats generally employ malware or malicious programs or gain access to IoT network elements [7].

The sophisticated cyber threats have shown the flaws of current cyber defenses, including firewalls and intrusion prevention and detection schemes. Moreover, since their strategies are based on routine heuristic and static attack signatures and therefore are unable to identify recent threats in the network [8]–

[13]. As there is no security mechanism available for defending the diverse, and dynamic systems and processes. IoT-enabled MTS network are vulnerable to a new category of threats that take advantage of embedded devices, attack surfaces and network protocols [14]–[16]. The openness of IoT-enabled MTS network makes them extremely unprotected to zero-day attacks. Thus, it requires intelligent security solutions that can detect new cyber threats automatically [17], [18]. Cyber Threat Intelligence (CTI) refers to evidence-based threat analysis, that can be used to develop actionable strategies and minimize the disparity between sophisticated attackers and the capabilities of an organization defenses [19]. An efficient CTI can present information that is both valid and reliable (revealing credible threats) as well as actionable (implies a clear course of action for threat remediation) [20]. The main goal of CTI is to develop a threat detection process by allowing security controls to be changed in real time, improving the probability of identifying and preventing malicious behavior before it happens [21].

Existing conventional security solutions are based on statistical and classical Machine Learning (ML) techniques for designing intelligent CTI models [19], [22]–[24], [13], [25]. Unfortunately, these models were complex, had lower detection accuracy, suffered with high false alarm rate and lacked generalization capability that made them difficult to use against the dynamic threats [4], [26], [27]. Other research used manual analysis to collect relevant threat information from non-traditional sources including hacker forums and “dark-web” media networks. However, manual processing of non-traditional sources to obtain CTI is time-consuming, error-prone procedure, and requires a large investment of resources [19], [21], [28], [29]. Deep Learning (DL) techniques can effectively work with heterogeneous, unstructured, and large amount of IoT data and can be used to design an adaptive CTI model [30]. From the extremely massive data, DL techniques can automatically extract hidden threat indicators without any human interference [17], [18]. The research towards DL-enabled CTI models, particularly for IoT-enabled MTS networks, is still in its early stage [31].

II. LITERATURE SURVEY

A key application of the Internet of Things (IoT) paradigm lies within industrial contexts. Indeed, the emerging Industrial Internet of Things (IIoT), commonly referred to as Industry 4.0, promises to revolutionize production and manufacturing through the use of large numbers of networked embedded sensing devices, and the combination of emerging computing technologies, such as Fog/Cloud Computing and Artificial Intelligence. The IIoT is characterized by an increased degree of inter-connectivity, which not only creates opportunities for the industries that adopt it, but also for cyber-criminals. Indeed, IoT security currently represents one of the major obstacles that prevent the widespread adoption of IIoT technology. Unsurprisingly, such concerns led to an exponential growth of published research over the last few years. To get an overview of the field, we deem it important to systematically survey the academic literature so far, and distill from it various security requirements as well as their popularity. This paper [1] consists of two contributions: our primary contribution is a systematic review of the literature over the period 2011-2019 on IIoT Security, focusing in particular on the security requirements of the IIoT. Our secondary contribution is a reflection on how the relatively new paradigm of Fog computing can be leveraged to address these requirements, and thus improve the security of the IIoT.

With increase in the demand for Internet of Things (IoT)-based services [16, 25, 38, 39], the capability to detect anomalies such as malicious control, spying and other threats within IoT-based network has become a major issue. Traditional Intrusion Detection Systems (IDSs) cannot be used in typical IoT-based network due to various constraints in terms of battery life, memory capacity and computational capability. In order to address these issues, various IDSs have been proposed in literature. However, most of the IDSs face problem of high false alarm rate and low accuracy in anomaly detection process. In this paper [2], we have proposed a anomaly-based intrusion detection system by decentralizing the existing cloud based security architecture to local fog nodes. In order to evaluate the effectiveness of the proposed model various machine learning algorithms such as

Random Forest, k-Nearest Neighbor and Decision Tree are used. Performance of our proposed model is tested using actual IoT-based dataset. The evaluation of the underlying approach outperforms in high detection accuracy and low false alarm rate using Random Forest algorithm.

The recent emergence of Internet-of-Things (IoT) [2, 10, 15] technologies in mission-critical applications in the maritime industry has led to the introduction of the Internet-of-Ships (IoS) paradigm. IoS is a novel application domain of IoT that refers to the network of smart interconnected maritime objects, which can be any physical device or infrastructure associated with a ship, a port, or the transportation itself, with the goal of significantly boosting the shipping industry toward improved safety, efficiency, and environmental sustainability. In this article [3], we provide a comprehensive survey of the IoS paradigm, its architecture, its key elements, and its main characteristics. Furthermore, we review the state of the art for its emerging applications, including safety enhancements, route planning and optimization, collaborative decision making, automatic fault detection and preemptive maintenance, cargo tracking, environmental monitoring, energy-efficient operations, and automatic berthing. Finally, the presented open challenges and future opportunities for research in the areas of satellite communications, security, privacy, maritime data collection, data management, and analytics, provide a road map toward optimized maritime operations and autonomous shipping.

This paper [4] addresses these challenges by proposing a new threat intelligence scheme that models the dynamic interactions of industry 4.0 components including physical and network systems. The scheme consists of two components: a smart management module and a threat intelligence module. The smart data management module handles heterogeneous data sources, one of the foundational requirements for interacting with an Industry 4.0 system. This includes data to and from sensors, actuators, in addition to other forms of network traffic. The proposed threat intelligence technique is designed based on beta mixture-hidden Markov models (MHMMs) for discovering anomalous activities against both physical and network systems. The scheme is evaluated on two well-known datasets: the CPS dataset of sensors and actuators and the UNSW-NB15 dataset of network traffic [4], [21], [22], [26], [27]. The results reveal that the proposed technique outperforms five peer mechanisms, suggesting its effectiveness as a viable deployment methodology in real-Industry 4.0 systems.

With the development of Internet of Vehicles (IoV), the integration of Internet of Things (IoT) and manual vehicles becomes inevitable in Intelligent Transportation Systems (ITS). In ITS, the IoVs communicate wirelessly with other IoVs, Road Side Unit (RSU) and Cloud Server using an open channel Internet. The openness of above participating entities and their communication technologies brings challenges such as security vulnerabilities, data privacy, transparency, verifiability, scalability, and data integrity among participating entities. To address these challenges, [7] we present a Privacy-Preserving based Secured Framework for Internet of Vehicles (P2SF-IoV) [7]. P2SF-IoV integrates blockchain and deep learning technique to overcome aforementioned challenges, and works on two modules. First, a blockchain module is developed to securely transmit the data between IoV-RSU-Cloud. Second, a deep learning module is designed that uses the data from blockchain module to detect intrusion and its performance is assessed using two network datasets IoT-Botnet and ToN-IoT. In contrast with other peer privacy-preserving intrusion detection strategies, the P2SF-IoV approach is compared, and the experimental results reveal that in both blockchain and non-blockchain based solutions, the proposed P2SF-IoV framework outperforms

III. METHODOLOGY

i) Proposed Work:

The proposed system is DLTIF (Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework) and is designed for IoT-enabled Maritime Transportation Systems (MTS) in the maritime industry. DLTIF consists of three schemes: a deep feature extractor (DFE), CTI-driven detection (CTIDD), and CTI-attack type identification (CTIATI). The DFE scheme automatically extracts hidden patterns from the IoT-

enabled MTS network, which is then used by the CTIDD scheme for threat detection. The CTIATI scheme is designed to identify the exact threat types and provide early warning to security analysts, enabling them to adopt defensive strategies. And also added, CNN and ensemble methods, specifically CNN+LSTM [26, 33] and Stacking Classifier, are integrated to enhance accuracy and robustness. In which Stacking Classifier achieved 99% accuracy, showcasing the efficacy of ensemble approaches. Furthermore, a Flask-based front-end interface is created to facilitate user testing, incorporating built-in authentication for enhanced security and access control. These models broadens the project's capabilities by integrating advanced modeling techniques and providing a user-friendly interface for practical implementation.

ii) System Architecture:

The proposed DLTIF framework uses DL approach to automate the extraction of threat pattern, and with the help of these meaningful patterns the abnormal behaviours are detected and finally, their types in IoT-enabled MTS [31] network is identified. The proposed DLTIF framework is shown in Fig 1. The network sniffing tool such as wireshark can gather raw packets at various choke points (such as mobile base stations) and can log them into a distributed database such as MySQL cluster database to enable real-time network monitoring [32]. As a result, the collected traffic is transformed into observations by network monitoring systems. Each observation represents useful information about the network connection statistics and features, which can assist in the detection of attacks. However, humans are normally taking control of integrating these points to form a pattern, which means that many hidden patterns are neglected. As a result, in the proposed DLTIF framework, we first introduce a data pre-processing scheme to map nominal features to numeric and then features are normalized to same scale. Second, a DFE scheme is added that explores knowledge about network activities and anticipated attacks. Since, the IoT-enabled MTS network is mixed of normal, and abnormal events, monitoring such large MTS [31] data to extract benign and attack patterns is extremely challenging. As a result, the proposed DFE scheme automatically incorporates network data and produces a unique representation in this sense that includes more relevant and functional network patterns. The DFE scheme is constructed on a generative DL architecture, which allows it to learn unknown and unidentified patterns without knowing any groups (such as normal or abnormal). It can also extract general trends from a variety of data types, which is very useful for analyzing uncertain, and varied MTS [31] data and emerging threats. The DFE scheme's data is feed into the CTIDD scheme, which determines whether certain patterns are related to threats. As a result, this approach lowers the dependency on passive attack detection methods that rely on conventional intrusion detection modeling (such as rules or signatures). Finally, to identify the exact attack type DFE extracted features are used by CTIATI scheme. Thus, based on exact threat types, the security analyst can take proper necessary prevention steps and analyst are relieved from heavy investigation work and ensuring that the industry are properly secured against threats [32].

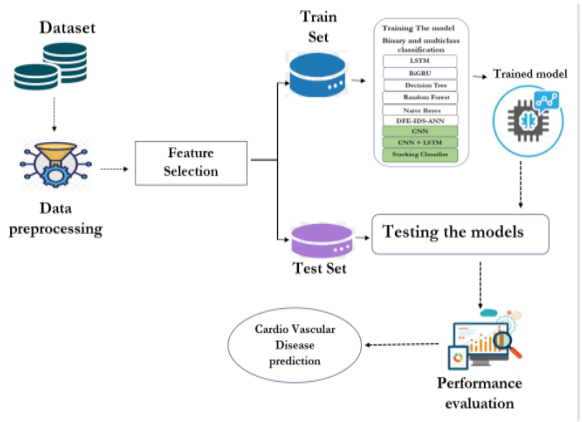
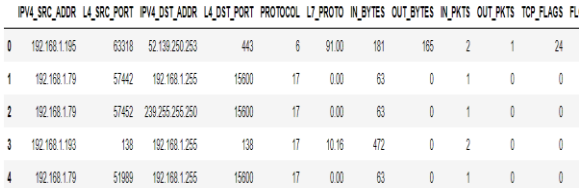


Fig 1 Proposed architecture

iii) Dataset collection:

In this project used the NF ToN-IoT dataset and exploring its structure. We will examine the data to understand its features, data types, and potential challenges. This exploration helps in gaining insights into the dataset before further processing. It indicates that the proposed DFE-CTIATI scheme has obtained outstanding results and has achieved the values between 87-100% for PR, DR, and F1 score on both IoT-based datasets using ToN-IoT dataset [38, 39]. Moreover, DFE-CTIATI scheme has reduced FAR close to 0% for all attack and normal vectors.



	IPV4_SRC_ADDR	L4_SRC_PORT	IPV4_DST_ADDR	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_BYTES	OUT_BYTES	IN_PKTS	OUT_PKTS	TCP_FLAGS	FL
0	192.168.1.195	63318	52.139.250.253	443	6	91.00	181	165	2	1	24	
1	192.168.1.79	57442	192.168.1.255	15600	17	0.00	63	0	1	0	0	
2	192.168.1.79	57452	239.255.255.250	15600	17	0.00	63	0	1	0	0	
3	192.168.1.193	138	192.168.1.255	138	17	10.16	472	0	2	0	0	
4	192.168.1.79	51989	192.168.1.255	15600	17	0.00	63	0	1	0	0	

Fig 2 NF ToN-IoT Dataset

iv) Data Processing:

Data processing involves transforming raw data into valuable information for businesses. Generally, data scientists process data, which includes collecting, organizing, cleaning, verifying, analyzing, and converting it into readable formats such as graphs or documents. Data processing can be done using three methods i.e., manual, mechanical, and electronic. The aim is to increase the value of information and facilitate decision-making. This enables businesses to improve their operations and make timely strategic decisions. Automated data processing solutions, such as computer software programming, play a significant role in this. It can help turn large amounts of data, including big data, into meaningful insights for quality management and decision-making.

v) Feature selection:

Feature selection is the process of isolating the most consistent, non-redundant, and relevant features to use in model construction. Methodically reducing the size of datasets is important as the size and variety of datasets continue to grow. The main goal of feature selection is to improve the performance of a predictive model and reduce the computational cost of modeling.

Feature selection [10], one of the main components of feature engineering, is the process of selecting the most important features to input in machine learning algorithms. Feature selection techniques are employed to reduce the number of input variables by eliminating redundant or irrelevant features and narrowing down the set of features to those most relevant to the machine learning model. The main benefits of performing feature selection in advance, rather than letting the machine learning model figure out which features are most important.

vi) Algorithms:

Long Short-Term Memory (LSTM) – Variational Autoencoder (VAE):

Long Short-Term Memory (LSTM): Long Short-Term Memory (LSTM) is a type of recurrent neural network (RNN) architecture designed to address the vanishing gradient problem in traditional RNNs. LSTMs are capable of learning and capturing long-term dependencies in sequential data, making them suitable for tasks involving time series or sequential patterns [33].

Variational Autoencoder (VAE): Variational Autoencoder (VAE) is a type of generative model that learns a probabilistic mapping between input data and a latent space. It is often used for dimensionality reduction, generating new data points, and representing complex data distributions in an unsupervised manner. In this combination, LSTM and VAE are likely used together in an integrated manner. LSTMs capture sequential dependencies in data, crucial for understanding temporal aspects, while VAEs provide a generative framework for learning and representing the underlying distribution of the data in a probabilistic manner.

LSTMs [33] capture time-series patterns and dependencies, essential for intrusion detection in scenarios where the order of events matters. VAEs can model the latent space of normal behavior, allowing for the identification of anomalies and deviations from the learned distribution.

Bidirectional Gated Recurrent Unit (BiGRU): Bidirectional Gated Recurrent Unit (BiGRU): BiGRU is a variant of the Gated Recurrent Unit (GRU), which is a type of recurrent neural network. The bidirectional aspect allows the model to consider information from both past and future time steps when making predictions. BiGRU is chosen for its ability to capture dependencies in both forward and backward directions, enhancing the model's understanding of sequential patterns in the data. This is advantageous for tasks like intrusion detection, where comprehensive context is crucial.

Decision Tree: Decision Tree: A decision tree is a tree-like model where each node represents a decision based on the value of a particular feature. It recursively splits the data into subsets, making decisions at each node until a stopping criterion is met. Decision trees are used for their simplicity and interpretability. They can handle both categorical and numerical data, making them suitable for datasets with a mix of data types. Decision trees are often employed in intrusion detection for their ability to reveal decision paths that lead to potential security threats.

Random Forest: Random Forest: Random Forest is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes (classification) or the mean prediction (regression) of the individual trees. Random Forest is utilized for its ability to improve predictive accuracy and control overfitting. By combining the predictions of multiple decision trees, it provides a robust and generalizable model. In intrusion detection, Random Forest can capture complex relationships in the data and enhance the overall performance.

Naive Bayes: Naive Bayes: Naive Bayes is a probabilistic classification algorithm based on Bayes' theorem with the assumption of independence between features. Despite its "naive" assumption, it often performs well, especially in text classification and spam filtering. Naive Bayes is chosen for its simplicity, efficiency, and ability to handle high-dimensional data. It is particularly effective for text-based data and is employed in intrusion detection for its speed and suitability for datasets with many features.

DFE (Distributed Feature Extraction) based IDS (Intrusion Detection System) and ANN (Artificial Neural Network): Distributed Feature Extraction (DFE) is an approach to extracting relevant features from data that is distributed across multiple sources or components. It involves collecting and aggregating features from different parts of a system or network. Artificial Neural Network (ANN) is a computational model inspired by the structure and functioning of the human brain. It consists of interconnected nodes (neurons) organized into layers, including an input layer, hidden layers, and an output layer. ANNs are capable of learning complex relationships in data through training on labeled examples. This combination involves using a Distributed Feature Extraction (DFE) approach within an Intrusion Detection System (IDS), coupled with the use of an Artificial Neural Network (ANN). DFE extracts relevant features from distributed sources, and ANN models the complex relationships in these features for effective intrusion detection.

DFE efficiently handles data distributed across the network, relevant for scenarios like IoT-enabled Maritime Transportation Systems where data may be spread across various components. ANN, with its ability to learn complex patterns, processes the extracted features to model relationships indicative of normal and anomalous behavior.

IV. EXPERIMENTAL RESULTS

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

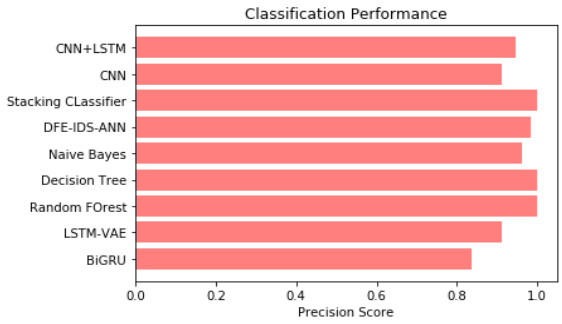


Fig 3 Precision comparison graph

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a

model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN}$$

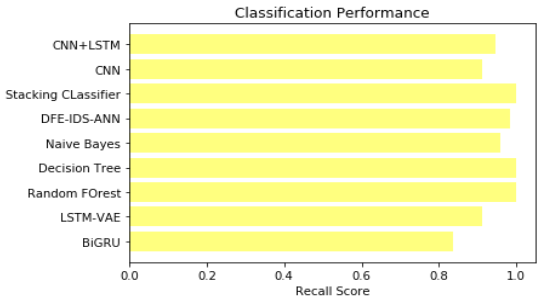


Fig 4 Recall comparison graph

Accuracy: Accuracy is the proportion of correct predictions in a classification task, measuring the overall correctness of a model's predictions.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

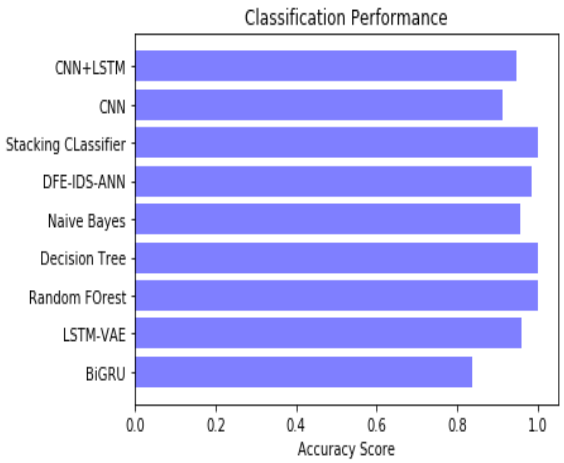


Fig 5 Accuracy graph

F1 Score: The F1 Score is the harmonic mean of precision and recall, offering a balanced measure that considers both false positives and false negatives, making it suitable for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

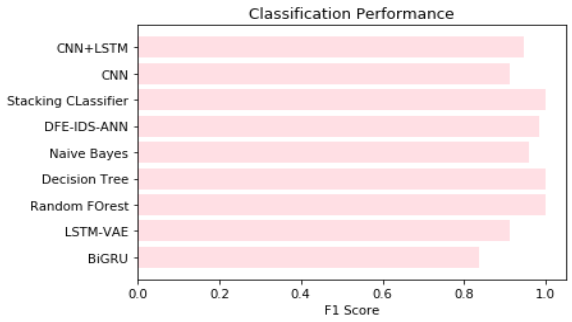


Fig 6 F1Score

ML Model	Accuracy	Precision	Recall	F1_score
BiGRU	0.836	0.836	0.836	0.836
LSTM-VAE	0.961	0.913	0.913	0.913
Random Forest	0.999	0.999	0.999	0.999
Decision Tree	0.999	0.999	0.999	0.999
Naive Bayes	0.957	0.961	0.957	0.958
DFE-IDS-ANN	0.985	0.985	0.985	0.985
Extension Stacking Classifier	1.000	0.999	0.999	0.999
Extension CNN	0.913	0.913	0.913	0.913
Extension CNN+LSTM	0.946	0.946	0.946	0.946

Fig 7 Performance Evaluation

V. CONCLUSION

The project strategically combines algorithms like LSTM-VAE and DFE-ANN for robust intrusion detection, leveraging LSTM [33] for temporal dependencies and DFE-ANN for efficient feature extraction in IoT-enabled Maritime Transportation Systems. Comprehensive metrics, including accuracy, precision, recall, and F1-score, provide a thorough assessment of model performance, ensuring a balanced understanding of binary and multi-class classification scenarios. Tailored for Maritime Transportation Systems, the project addresses the unique challenges posed by the dynamic and distributed nature of threats, enhancing security in both physical and cyber domains. The other algorithm, particularly the Stacking Classifier, demonstrates exceptional performance with a 99% accuracy rate. This accuracy was verified through rigorous testing, including the simulation of various threat scenarios with input feature values in the front-end interface. Beyond model efficacy, the project prioritizes user interaction, employing a Flask

framework with SQLite for signup and signin. This user-friendly interface enhances accessibility, making the intrusion detection system practical and user-driven.

VII. FUTURE SCOPE

In future, we will evaluate the proposed framework with different IoT-based datasets to verify the effectiveness of proposed DLTIF framework. Since the proposed DLTIF framework uses a DL based deep feature extractor (DFE) scheme, the computational complexity is higher than the traditional threat identification methods (i.e., RF, DT, NB) [19], [22]–[24], [13], [25]. However, during the training process of the framework, the availability of specialized hardware, such as TPUs, GPUs, and software, such as automated differentiation packages, can overcome these computational complexity. Furthermore, since the deep models weights have already been learned during the training process, the testing phase difficulty decreases.

REFERENCES

[1] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities," IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2489–2520, 4th Quart., 2020.

[2] P. Kumar, G. P. Gupta, and R. Tripathi, "Design of anomaly-based intrusion detection system using fog computing for IoT network," Autom. Control Comput. Sci., vol. 55, no. 2, pp. 137–147, Mar. 2021.

[3] S. Aslam, M. P. Michaelides, and H. Herodotou, "Internet of ships: A survey on architectures, emerging applications, and challenges," IEEE Internet Things J., vol. 7, no. 10, pp. 9714–9727, Oct. 2020.

[4] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," IEEE Access, vol. 6, pp. 32910–32924, 2018.

[5] T. Xia, M. M. Wang, J. Zhang, and L. Wang, "Maritime Internet of Things: Challenges and solutions," IEEE Wireless Commun., vol. 27, no. 2, pp. 188–196, Apr. 2020.

[6] M. Sadiq et al., "Future greener seaports: A review of new infrastructure, challenges, and energy efficiency measures," IEEE Access, vol. 9, pp. 75568–75587, 2021.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, and N. Kumar, "P2SFIoV: A privacy-preservation-based secured framework for Internet of vehicles," IEEE Trans. Intell. Transp. Syst., early access, Aug. 11, 2021, doi: 10.1109/TITS.2021.3102581.

[8] S. U. Rehman et al., "DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," Future Gener. Comput. Syst., vol. 118, pp. 453–466, May 2021.

[9] T. Qiu, Z. Zhao, T. Zhang, C. Chen, and C. L. P. Chen, "Underwater Internet of Things in smart ocean: System architecture and open issues," IEEE Trans. Ind. Informat., vol. 16, no. 7, pp. 4297–4307, Jul. 2020.

[10] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," Comput. Secur., vol. 94, Jul. 2020, Art. no. 101863.

[11] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," Future Gener. Comput. Syst., vol. 111, pp. 763–779, Oct. 2020.

[12] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, and S. Singh, "A review on cyber crimes on the Internet of Things," 2020, arXiv:2009.05708. [Online]. Available: http://arxiv.org/abs/2009.05708

[13] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A trustworthy privacypreserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," J. Syst. Archit., vol. 115, May 2021, Art. no. 101954.

[14] T. Yang, J. Chen, and N. Zhang, "AI-empowered maritime Internet of Things: A parallel-network-driven approach," IEEE Netw., vol. 34, no. 5, pp. 54–59, Sep. 2020.

[15] V. Sharma, T. G. Tan, S. Singh, and P. K. Sharma, "Optimal and privacy-aware resource management in AIoT using osmotic computing," IEEE Trans. Ind. Informat., early access, Aug. 6, 2021, doi: 10.1109/TII.2021.3102471.

[16] P. Kumar, G. P. Gupta, and R. Tripathi, "Toward design of an intelligent cyber attack detection system using hybrid feature reduced

approach for IoT networks," Arabian J. Sci. Eng., vol. 46, no. 4, pp. 3749–3778, Apr. 2021.
[17] M. Al-Hawawreh, N. Moustafa, S. Garg, and M. S. Hossain, "Deep learning-enabled threat intelligence scheme in the Internet of Things networks," IEEE Trans. Netw. Sci. Eng., early access, Oct. 20, 2020, doi: 10.1109/TNSE.2020.3032415.
[18] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," IEEE Trans. Intell. Transp. Syst., early access, Aug. 3, 2021, doi: 10.1109/TITS.2021.3098636.
[19] I. Deliu, C. Leichter, and K. Franke, "Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent Dirichlet allocation," in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2018, pp. 5008–5013.
[20] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: A cyber threat intelligence perspective," in The Palgrave Handbook of International Cybercrime and Cyberdeviance. Cham, Switzerland: Springer, 2020, pp. 135–154.
[21] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2017, pp. 3648–3656.
[22] Y. Zhou and P. Wang, "An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence," Comput. Secur., vol. 82, pp. 261–269, May 2019.
[23] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem, and A. Tahir, "A supervised machine learning based approach for automatically extracting highlevel threat intelligence from unstructured sources," in Proc. Int. Conf. Frontiers Inf. Technol. (FIT), Dec. 2018, pp. 129–134.
[24] U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories," Future Gener. Comput. Syst., vol. 95, pp. 467–487, Jun. 2019.
[25] P. Kumar et al., "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2326–2341, Jul. 2021.
[26] M. Ebrahimi, J. F. Nunamaker, and H. Chen, "Semi-supervised cyber threat identification in dark net markets: A transductive and deep learning approach," J. Manage. Inf. Syst., vol. 37, no. 3, pp. 694–722, Jul. 2020.
[27] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, "Exploring the dark web for cyber threat intelligence using machine leaning," in Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), Jul. 2019, pp. 200–202.
[28] A. Piplai, S. Mittal, M. Abdelsalam, M. Gupta, A. Joshi, and T. Finin, "Knowledge enrichment by fusing representations for malware threat intelligence and behavior," in Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), Nov. 2020, pp. 1–6.
[29] G. Husari, X. Niu, B. Chu, and E. Al-Shaer, "Using entropy and mutual information to extract threat actions from cyber threat intelligence," in Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI), Nov. 2018, pp. 1–6.
[30] Q. Li et al., "A highly efficient vehicle taillight detection approach based on deep learning," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4716–4726, Jul. 2021.
[31] Y. Gao, X. Li, H. Peng, B. Fang, and P. Yu, "HinCTI: A cyber threat intelligence modeling and identification system based on heterogeneous information network," IEEE Trans. Knowl. Data Eng., early access, Apr. 20, 2020, doi: 10.1109/TKDE.2020.2987019.
[32] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fogcloud architecture-driven cyber-attack detection framework for IoMT networks," Comput. Commun., vol. 166, pp. 110–124, Jan. 2021.
[33] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, T. R. Gadekallu, and G. Srivastava, "SP2F: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles," Comput. Netw., vol. 187, Mar. 2021, Art. no. 107819.
[34] S. Zavrak and M. Iskefiyeli, "Anomaly-based intrusion detection from network flow features using variational autoencoder," IEEE Access, vol. 8, pp. 108346–108358, 2020.
[35] Y. Deng, L. Wang, H. Jia, X. Tong, and F. Li, "A sequence-tosequence deep learning architecture

based on bidirectional GRU for type recognition and time location of combined power quality disturbance," IEEE Trans. Ind. Informat., vol. 15, no. 8, pp. 4481–4493, Aug. 2019.
[36] S. Bhattacharya et al., "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," Electronics, vol. 9, no. 2, p. 219, Jan. 2020.
[37] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using Fog computing to protect the Internet of Things networks," J. Ambient Intell. Humanized Comput., vol. 12, pp. 9555–9572, Nov. 2020.
[38] N. Moustafa. (2019). Ton IoT Datasets. Accessed: Feb. 10, 2020. [Online]. Available: http://dx.doi.org/10.21227/fesz-dm97
[39] P. Kumar, R. Tripathi, and G. P. Gupta, "P2IDF: A privacy-preserving based intrusion detection framework for software defined Internet of Things-fog (SDIoT-Fog)," in Proc. Int. Conf. Distrib. Comput. Netw. New York, NY, USA: Association for Computing Machinery, 2021, pp. 37–42, doi: 10.1145/3427477.3429989.