10.48047/jocaaa.2024.32.02.35

DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modelling & Detection Methodology For IoT-Enable Marine Transportation Systems

Dr. V. ANANTHAKRISHNA[1], A . S H I V A N I [2] , SALONI TIWARI[3], B. PRIYANKA[4]
[1]Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India
Email: Krishnaananthav@gmail.com,
[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT

The maritime industry has recently seen a boom in Internet of Things (IoT) technologies, which are effectively digitalizing MTS. The smart maritime items in IoT-enabled MTS communicate wirelessly with port or ship infrastructure through an open channel of the Internet. Cyber criminals have opportunities as a result of the interoperability and integration of diverse technologies in IoT-enabled MTS, in addition to the industries that use it. Using artificial intelligence models to understand cyber-attacks, Cyber Threat Intelligence (CTI) is a powerful security technique that can effectively secure the data of IoT-enabled MTS. unsurprisingly, the majority of CTI-based solutions now in use manual analysis to extract relevant threat information, have a high false alarm rate, and have poor detection rates. Therefore, to tackle aforementioned challenges, an automated framework called DLTIF is developed for modeling cyber threat intelligence and identifying threat types. The proposed DLTIF is based on three schemes such as a deep feature extractor (DFE), CTI-driven detection (CTIDD) and CTI-attack type identification (CTIATI). The DFE scheme automatically extracts the hidden patterns of IoT-enabled MTS network and its output is used by CTIDD scheme for threat detection. The CTIATI scheme is designed to identify the exact threat types and to assist security analysts in giving early warning and adopt defensive strategies. The proposed framework has obtained high accuracy, and outperforms some traditional and recent state-of-the-art approaches.

Keywords: Maritime Transportation System (MTS), Internet of Things (IoT), Cyber Threat Intelligence (CTI), Artificial Intelligence (AI), Cybersecurity, DLTIF (Deep Learning Threat Intelligence Framework), Threat Detection, Interoperability, Cyber-attacks, Data Security..

10.48047/jocaaa.2024.32.02.35

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. 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. 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. Moreover, since their strategies are based on routine heuristic and static attack signatures and therefore are unable to identify recent threats in the network.

As there is no security mechanism available for defending the diverse, and dynamic systems and processes. IoT-enabled MTS network is vulnerable to a new category of threats that take advantage of embedded devices, attack surfaces and network protocols. Thus, it requires intelligent security solutions that can detect new cyber threats automatically. This integration gives immense flexibility and versatility in the management of inter-maritime processes intelligently, resulting in improved productivity and resource utilization. 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. 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.

In recent years, the field of Software Engineering has witnessed a profound transformation, propelled by cutting-edge research and technological advancements. This evolution is epitomized by a surge in innovative frameworks and solutions designed to address the burgeoning challenges in diverse domains. The work of James F. Peters and Witold Pedrycz in "Software Engineering, an Engineering approach" [1] stands as a testament to the

10.48047/jocaaa.2024.32.02.35

ongoing quest for robust engineering methodologies. This introduction delves into the intersection of software engineering, privacy preservation, and security, highlighting seminal contributions from contemporary research. Kumar et al.'s groundbreaking work introduces "SP2F," a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles [2]. Further expanding into the realm of Internet of Things (IoT) security, Kumar, Tripathi, and Gupta present "P2IDF," a privacy-preserving intrusion detection framework for Software Defined IoT-Fog [3]. As the landscape of cybersecurity evolves, novel approaches such as the PCA-firefly based XGBoost model for intrusion detection [4] and anomaly-based intrusion detection using variational autoencoder [5] showcase the integration of advanced techniques. Additionally, the convergence of Artificial Intelligence and Internet of Things is explored in the work of Sharma et al., focusing on optimal and privacy-aware resource management through osmotic computing in AIoT [6]. Beyond cybersecurity, the exploration extends to maritime domains with Aslam, Michaelides, and Herodotou's survey on the "Internet of Ships" [7]. Furthermore, Kagita et al. offer a comprehensive review on cybercrimes in the Internet of Things [8], shedding light on the challenges and vulnerabilities in this interconnected landscape. Collectively, these works underscore the dynamic and interdisciplinary nature of contemporary software engineering, emphasizing the pivotal role it plays in shaping the future of technology, security, and privacy.

RELATED WORK

“Design of Anomaly-Based Intrusion Detection System Using Fog Computing for IoT Network”

With increase in the demand for Internet of Things (IoT)-based services, 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,

10.48047/jocaaa.2024.32.02.35

most of the IDSs face problem of high false alarm rate and low accuracy in anomaly detection process. In this paper, we have proposed an 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 methodology involves decentralizing intrusion detection by migrating from cloud-based security to local fog nodes in an IoT network. Various machine learning algorithms (Random Forest, K-Nearest Neighbor, and Decision Tree) are employed for anomaly detection using real IoT data. The system's performance is evaluated for accuracy and false alarm rates. Our system shifts intrusion detection from cloud to local fog nodes in IoT networks. It leverages machine learning algorithms, including Random Forest, for enhanced anomaly detection. This model is evaluated using real IoT data, demonstrating superior accuracy and reduced false alarm rates. Decentralizing intrusion detection to local fog nodes in IoT networks offers a promising solution to address resource constraints. The utilization of machine learning algorithms, particularly Random Forest, results in higher detection accuracy and lower false alarm rates, enhancing IoT network security.

“Future Greener Seaports: A Review of New Infrastructure, Challenges, and Energy Efficiency Measures”

Recently, the application of renewable energy sources (RESs) for power distribution systems is growing immensely. This advancement brings several advantages, such as energy sustainability and reliability, easier maintenance, cost-effective energy sources, and ecofriendly. The application of RESs in maritime systems such as port microgrids massively improves energy efficiency and reduces the utilization of fossil fuels, which is a serious threat to the environment. Accordingly, ports are receiving several initiatives to improve their energy efficiency by deploying different types of RESs based on the power electronic converters. This paper

10.48047/jocaaa.2024.32.02.35

conducts a systematic review to provide cutting-edge state-of-the-art on the modern electrification and infrastructure of seaports taking into account some challenges such as the environmental aspects, energy efficiency enhancement, renewable energy integration, and legislative and regulatory requirements. Moreover, the technological methods, including electrifications, digitalization, onshore power supply applications, and energy storage systems of ports, are addressed. Furthermore, details of some operational strategies such as energy-aware operations and peak-shaving are delivered. Besides, the infrastructure scheme to enhance the energy efficiency of modern ports, including port microgrids and seaport smart microgrids are delivered. Finally, the applications of nascent technologies in seaports are presented. This review conducts a systematic analysis of modern seaport electrification and infrastructure developments, considering factors like environmental concerns, energy efficiency, renewable energy integration, and regulatory requirements. It also explores technological solutions such as electrification, digitalization, onshore power supply, and energy storage. The study analyzes operational strategies, including energy-aware operations and peak-shaving, and discusses infrastructure improvements, including port microgrids and smart microgrids. The proposed system involves the comprehensive integration of renewable energy sources and modern infrastructure solutions in seaports. It emphasizes environmental sustainability, energy efficiency, and adherence to regulatory requirements. It incorporates electrification, digitalization, onshore power supply, and energy storage to create resilient and ecofriendly port systems. Modern seaports are adopting renewable energy integration, digitalization, and innovative infrastructure to enhance energy efficiency and reduce environmental impacts. 6 DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Detection Methodology for IoT-Enable Marine Transportation Systems While challenges exist, such as initial costs and regulatory hurdles, the adoption of these technologies and operational strategies is crucial for greener, more sustainable port operations, contributing to a cleaner and more reliable maritime industry.

“P2SF-IoV: A Privacy-Preservation-Based Secured Framework for Internet of Vehicles”

10.48047/jocaaa.2024.32.02.35

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, we present a Privacy-Preserving based Secured Framework for Internet of Vehicles (P2SF-IoV). P2SF-IoV integrates blockchain and deep learning technique to overcome aforementioned challenges, and works on two modules. The methodology involves the development of a Privacy-Preserving Secured Framework for Internet of Vehicles (P2SF-IoV). It combines blockchain and deep learning techniques in two modules. The first module employs blockchain for secure data transmission among IoV, RSU, and Cloud. The second module uses data from the blockchain to detect intrusions, evaluated with IoT-Botnet and ToN-IoT datasets. P2SF-IoV integrates blockchain and deep learning to enhance security and privacy in Internet of Vehicles (IoV). It ensures secure data exchange between IoVs, RSUs, and the Cloud while utilizing deep learning for intrusion detection. The system excels in comparison to other privacy-preserving intrusion detection methods, both with and without blockchain. The P2SF-IoV framework successfully addresses security and privacy challenges in Internet of Vehicles through the fusion of blockchain and deep learning technologies. Experimental results demonstrate its superiority compared to alternative solutions, highlighting its effectiveness in securing IoV communication and intrusion detection, contributing to safer and more reliable Intelligent Transportation Systems.

“DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)”

Distributed Denial of Service (DDoS) attacks can put the communication networks in instability by throwing malicious traffic and requests in bulk over the network. Computer networks form a complex chain of nodes resulting in a

10.48047/jocaaa.2024.32.02.35

formation of vigorous structure. Thus, in this scenario, it becomes a challenging task to provide an efficient and secure environment for the user. Numerous approaches have been adopted in the past to detect and prevent DDoS attacks but lack in providing efficient and reliable attack detection. As a result, there is still notable room for improvement in providing security against DDoS attacks. In this paper, a novel high-efficient approach is proposed named DIDDOS to protect against real-world new type DDoS attacks using Gated Recurrent Unit (GRU) a type of Recurrent Neural Network (RNN). Different classification algorithms such as Gated Recurrent Units (GRU), Recurrent Neural Networks (RNN), Naive Bayes (NB), and Sequential Minimal Optimization (SMO) are utilized to detect and identify DDoS attacks. The study employs the DIDDOS approach for DDoS attack detection, using Gated Recurrent Units (GRU) and other classifiers. Real-world DDoS attack data is collected and preprocessed. Various classification algorithms are utilized, and performance metrics like accuracy, recall, f1-score, and precision are assessed to measure classifier efficiency. DIDDOS is a novel approach for effective DDoS attack detection, employing GRU, a type of Recurrent Neural Network. It also explores other classifiers such as RNN, Naive Bayes, and SMO. The system aims to provide high-efficiency protection against emerging DDoS attacks, achieving impressive accuracy in classification. The DIDDOS approach, leveraging GRU and other classifiers, demonstrates exceptional accuracy in DDoS attack classification. It addresses the pressing need for reliable and efficient DDoS attack detection, offering promising results in safeguarding communication networks against both reflection and exploitation DDoS attacks, contributing to enhanced network security.

"TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning"

The methodology involves developing the TP2SF framework for smart cities, consisting of three modules: a trustworthiness module with an address-based blockchain reputation system, a two-level privacy module using blockchain-based ePoW and PCA, and an intrusion detection module deploying XGBoost. Additionally, a Fog-Cloud infrastructure, CloudBlock and FogBlock, is introduced to

10.48047/jocaaa.2024.32.02.35

enable the deployment of TP2SF. Evaluation is performed on IoT datasets, ToNIoT and BoT-IoT, for comparison. TP2SF is a comprehensive framework designed for smart cities, addressing security, privacy, trust, scalability, and centralization challenges. It integrates blockchain reputation, privacy-preserving techniques, and intrusion detection. Furthermore, it utilizes a Fog-Cloud architecture with CloudBlock and FogBlock for effective deployment, offering superior performance in both blockchain and non-blockchain IoT systems. Implementation complexity due to the integration of various modules and technologies. Scalability challenges when applied to large and complex smart city networks. TP2SF provides a robust solution for secure and trustworthy smart cities, overcoming key IoT challenges. Its evaluation on real-world datasets demonstrates its superiority compared to existing techniques, highlighting its potential for enhancing the security and privacy of IoT-driven smart cities.

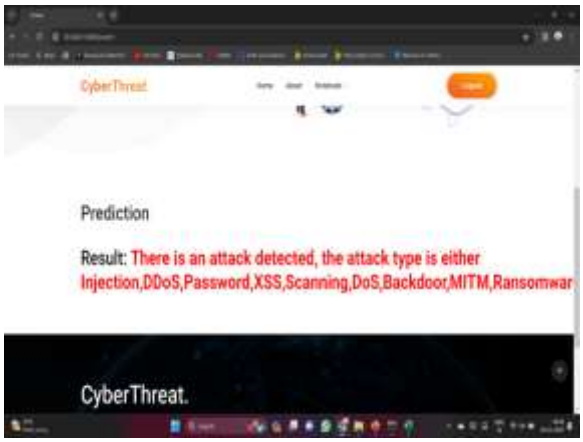
In literature, they have introduced a anomaly-based intrusion detection system by decentralizing the existing cloud based security architecture to local fog nodes. In order to evaluate the effectiveness of their model various machine learning algorithms such as Random Forest, K-Nearest Neighbor and Decision Tree are used. Performance of their model is tested using actual IoT-based dataset. Another research introduced a new TI scheme based on deep learning techniques that can discover cyber threats from SAGS networks. Their scheme contains three modules such as a deep pattern extractor, TI-driven detection and TI-attack type identification technique. The deep pattern extractor module is designed to elicit hidden patterns of IoT networks, and its output used as input to the TI-driven detection. TI-attack type identification is used to identify the attack types of malicious patterns to assist in responding to security incidents. The proposed scheme is evaluated on the two datasets of TON-IoT and N-BAIOT.3.1.1 Disadvantage evaluated on the two datasets of TON-IoT and N-BAIOT.

METHODOLOGY

10.48047/jocaaa.2024.32.02.35

RESULT AND DISCUSSION

In above screen user should click on "Register" it redirects to FORM PAGE. Enter the inputs in the fields and click on "Predict".



In above screen we can see the result as the attack is detected or not. In case there is an attack it will be displayed as "There is an attack detected and its attack type" or else it will be displayed as "There is no attack detected, it is Normal".

CONCLUSION

In this paper, we provided a powerful solution that utilizes deep learning techniques to provide effective cyber threat intelligence modeling and detection for IoT-enabled marine transportation systems. With its data collection, preprocessing, feature extraction, and deep learning model modules, it can accurately identify potential cyber threats in real-time. The system also includes alert generation, visualization, and model update modules to support system administrators in taking necessary actions. Overall, DLTIF enhances the security and protection of IoT-enabled marine transportation systems against cyber threats.

Looking ahead, the future enhancement of the DLTIF (Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework) in IoT-enabled maritime transportation systems involves integrating advanced deep learning algorithms, leveraging cutting-edge neural network architectures for improved predictive capabilities. Real-time data from

10.48047/jocaaa.2024.32.02.35

IoT devices on maritime vessels will be incorporated to enhance threat detection and response. Collaboration with industry experts and maritime authorities, scalability considerations, and continuous research and development efforts will ensure the framework remains agile and effective in addressing the evolving cyber threats within the maritime sector.

REFERENCES

[1]Software Engineering, an Engineering approach- James F. Peters, Witold Pedrycz, John Wiley.

[2]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

[3]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.

[4]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.

[5]S. Zavrak and M. Iskefiyeli, "Anomaly-based intrusion detection from network flow features using variational autoencoder," IEEE Access, vol. 8, pp. 108346–108358, 2020

[6]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

[7]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.

[8]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

10.48047/jocaaa.2024.32.02.35