Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 11
November 2024

Hybrid Bi-LSTM-Squeeze Model for Attack Detection and Mitigation in Industrial IoT

[1]Dr. Bibhuti Bhusana Behera, [2*]Sushree Subhasmita Mohanty, [3]Sunita Sahu
[1]Associate Professor, Department of CSE, GIET, Ghangapatna, Bhubaneswar, India
[2]Reseach Scholar, BPUT
mohantysubhasmita1129 @ gmail.com
[3]Asst. Professor, BEC,Bhubaneswar
bibhutibbehera@gietbbsr.edu.in

Abstract
The IIoT has revolutionized industrial operations by enabling seamless connectivity, data-driven decision-making, and enhanced efficiency. However, the pervasive integration of IIoT systems also introduces unprecedented cybersecurity risks, necessitating robust intrusion detection and mitigation mechanisms to safeguard critical infrastructure. Conventional approaches to IIoT security frequently fall short in addressing the dynamic and complex nature of cyber threats, prompting a paradigm shift towards advanced ML techniques, particularly deep learning, for threat detection and mitigation. This paper introduces a novel hybrid detection model aimed at enhancing IIoT security through improved attack detection capabilities. This proposed methodology addresses key concerns such as detection accuracy, efficiency, privacy, and time consumption. Here, propose a comprehensive framework comprising pre-processing, feature extraction, feature selection, attack detection, and attack mitigation. Notably, we employ Improved SMOTE for class imbalance resolution and min-max normalization for data normalization. Feature extraction encompasses info gain, raw, correntropy, and statistical features, while Improved SVM-RFE aids in feature selection. The fundamental component of this strategy is a hybrid model that combines Bi-LSTM and Improved LinkNet for effective attack detection, followed by the utilization of Improved Entropy-based mitigation to eliminate identified threats.

Keywords- Industrial IoT, attack detection, Improved Bi-LSTM, SqueezeNet, attack mitigation, Improved SMOTE, entropy-based mitigation

Introduction

The IIoT has emerged as a transformative force in the realm of industrial automation and data management, revolutionizing traditional manufacturing processes and operational methodologies [9] [10]. At its core, IIoT harnesses the power of interconnected devices, sensors, and machines, leveraging internet connectivity to optimize production, enhance decision-making, and minimize human intervention [13] [14]. By facilitating real-time data collection and analysis, IIoT networks empower industries to streamline operations, improve quality control, optimize asset tracking, and enable predictive maintenance strategies [26].

However, the proliferation of interconnected devices and the ubiquitous nature of IIoT systems have ushered in a new era of cybersecurity challenges [15]. The extensive connectivity that underpins IIoT architectures exposes industrial operations to a myriad of cyber threats, ranging from integrity-compromising attacks to availability disruptions and confidentiality breaches. Integrity-compromising attacks, such as sensor data tampering or control system manipulation, pose a direct threat to the reliability and trustworthiness of industrial processes [12]. Availability attacks, including DDoS [20] [44] assaults and wireless interference, seek to disrupt system accessibility, potentially causing operational downtime and financial losses [17]. Confidentiality breaches involve unauthorized access to sensitive data, while authentication attacks exploit weaknesses in authentication mechanisms, undermining the overall security posture of IIoT infrastructures [21] [45].

In response to these evolving threats, researchers and industry practitioners alike have increasingly turned to advanced ML [25] [46] techniques for intrusion detection and anomaly recognition in IIoT networks. DL, a subset of ML, has gained prominence for its ability to automatically extract intricate patterns and features from raw data, making it particularly well-suited for complex and

dynamic environments like IIoT. Deep learning algorithms [11] [16], such as CNNs and RNNs [19], offer the promise of automated threat detection, capable of analyzing vast streams of sensor data and identifying anomalous patterns indicative of potential attacks [18] [22] [23]. However, the efficacy of DL-based intrusion detection models hinges on the quality and representativeness of training data. Unfortunately, the scarcity and imbalance inherent in IIoT datasets often lead to biased predictions and suboptimal performance [24] [42].

Contribution:

- Introducing an Improved SMOTE for addressing class imbalance in IIoT datasets during the preprocessing stage.
- Contributing an Improved SVM-RFE for feature selection to identify a subset of discriminative features.
- Proposing a novel hybrid detection model, which combines Bi-LSTM and SqueezeNet architectures.
- Suggesting an Improved Entropy-based mitigation strategies to neutralize detected threats in IIoT environments.

Literature Riview

In 2024, F. S. Melícias et al., [1] assessed data augmentation techniques for improving intrusion detection models utilizing IIoT traffic data, such as variations of GPT and SMOTE. To evaluate performance differences, five intrusion detection methods were tested using original and supplemented datasets.

In 2024, P. Verma et al., [2] addressed cybersecurity data imbalance issues by introducing a novel oversampling method based on gametic heredity, with a focus on IIoT systems.

In 2024, Ferrag et al., [3] presented SecurityBERT, a novel architecture for cyber threat detection in Internet of Things networks that made use of the BERT concept. SecurityBERT was able to represent network traffic data more efficiently than conventional ML and DL techniques such as CNNs or RNNs because it incorporated the PPFLE technique during training.

In 2024, X. Jin et al., [4] provided a blockchain-federated learning distributed anomaly detection solution for IIoT devices. The side-chain logged the hash values of the global and local models, which were updated by participating nodes, while the main-chain stored the global model. With the use of smart contracts and main-side blockchain, access to the global model was controlled.

Problem statement

The literature review highlights significant strides in IIoT cybersecurity, yet challenges persist across existing methodologies, which is illustrates in Table I. Data augmentation [1] and oversampling methods [2] show potential but may compromise accuracy and suffer from overgeneralization. Although ensemble learning [8] and deep neural networks [1] offer impressive accuracy, their computational demands limit deployment on resource-constrained IIoT devices. Additionally, collaborative defense mechanisms, although effective in countering DDoS attacks, face challenges in ensuring secure data sharing and minimizing response delays. Therefore, there is an crucial need for a comprehensive intrusion detection and cybersecurity solution tailored specifically for IIoT environments, mitigating the limitations of existing approaches while using their strengths. The suggested work aims to address this gap by introducing a novel hybrid detection model.

Proposed model:

The proposed methodology tackles the pressing issue of attack detection and mitigation in IIoT environments. It begins with data preprocessing to address class imbalance and ensure feature uniformity. Feature extraction and selection techniques are then applied to improve the discriminative power of the model. This is followed by the implementation of a hybrid detection model and improved entropy-based mitigation strategies for bolstering IIoT system resilience.

- The initial step in the proposed work involves preprocessing the input data to address inherent challenges in IIoT datasets, particularly class imbalance. Improved SMOTE is utilized to handle class imbalance, while min-max normalization is applied for feature scaling, ensuring unbiased analysis and equitable feature contribution.
- Following preprocessing, the approach encompasses the extraction of diverse feature

types—info gain, raw, correntropy, and statistical—to comprehensively represent data characteristics, thereby enhancing model robustness and discriminative power.

- Subsequently, using Improved SVM-RFE, a parsimonious set of discriminative features is identified, enhancing computational efficiency and interpretability of subsequent analysis.
- For attack detection, a hybrid model is proposed, combining Improved LinkNet and SqueezeNet architectures. This hybrid approach achieves a balance between accuracy and efficiency, enabling real-time detection of cyber-attacks by leveraging feature-rich data for superior performance.
- Finally, through Improved Entropy-based Mitigation, IIoT system resilience against adversarial activities is bolstered, thereby enhancing security and ensuring dependable operational integrity. The suggested model for attack detection and mitigation is shown in Figure 1.

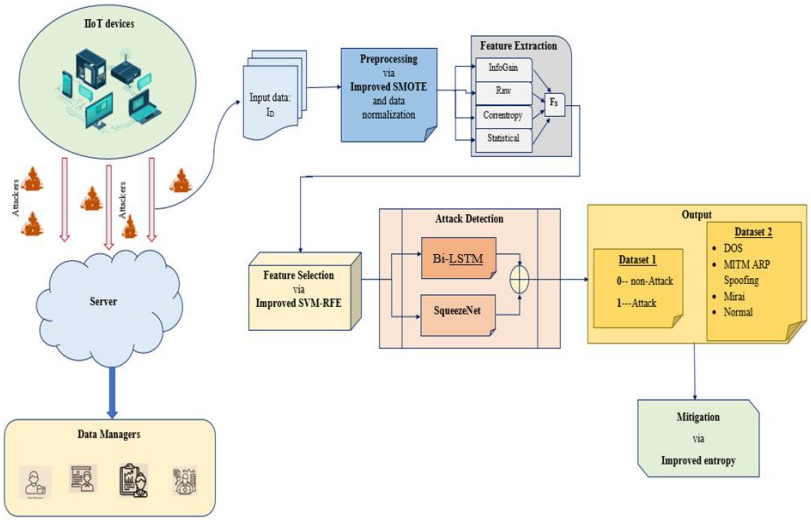

Figure 1: Proposed model for attack detection

Dataset Description

The raw data collection produced a dataset totaling 627 MB, where normal traffic accounts for 93.93% and abnormal traffic, indicative of attacks, makes up 6.07%. This dataset includes 25 networking features, utilized for both data classification and training/testing ML algorithms. Post data collection, the dataset underwent cleaning, classification, and labeling processes.

Result Analysis:

In assessing the negative metric evaluation of Improved Bi-LSTM+SqueezeNet model against conventional methods for attack detection and mitigation within IIoT, using dataset as depicted in Figure 2. In this comparative study, the Improved Bi-LSTM +SqueezeNet model is systematically contrasted with established methods such as SqueezeNet, EfficientNet, SA-DCNN [5], ResNet, DenseNet, Bi-LSTM, and CNN. The primary goal is to achieve minimized negative measure ratings, critical for effectual recognition and mitigation of threats in IIoT environments. Notably, the Improved Bi-LSTM+SqueezeNet strategy consistently achieves lower negative metric values compared to traditional schemes. This underscores its potential to enhance security measures by reducing false positives and ensuring accurate detection of malicious activities. The FPR evaluation for Dataset provides significant understanding of the performance of Improved Bi-LSTM + Squeeze Net and conventional models. At 60% training data, SqueezeNet demonstrates an FPR of 0.298, indicating its ability to maintain a relatively low rate of falsely identifying normal instances as attacks. Increasing the training data to 70% and 80%, most models maintain consistent FPR values with slight variations.

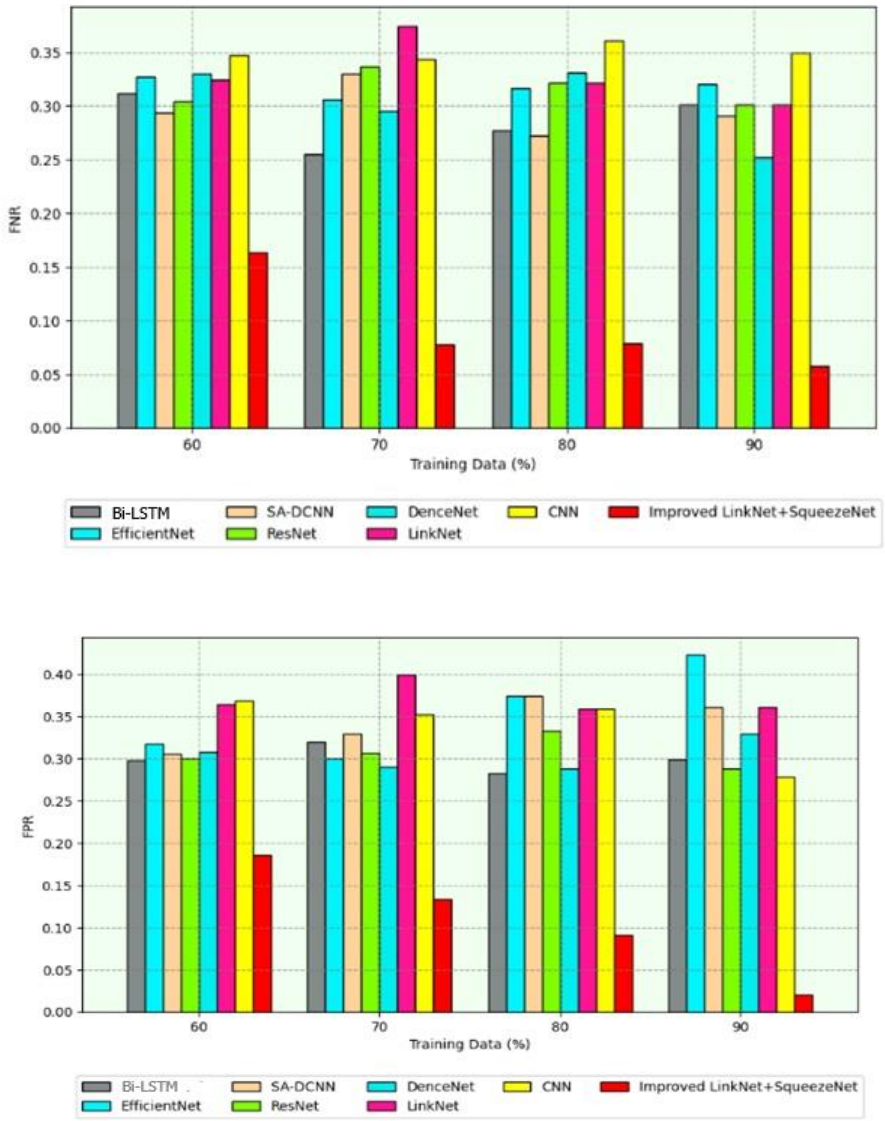

Figure 2: Negative metric analysis comparing the Improved Bi-LSTM+SqueezeNet model with conventional methods using dataset

Table I: Ablation study on Improved LinkNet+SqueezeNet , Model with Conventional LinkNet, Model without Imbalance Processing and Model without Feature Selection for Dataset

Metrics	Model without Imbalance Processing	Improved Bi- LSTM + SqueezeNet	Model without Feature Selection	Model with Conventional Bi-LSTM
Accuracy	0.691	0.960	0.697	0.717
F-Measure	0.682	0.960	0.686	0.719
FPR	0.297	0.021	0.282	0.306
Sensitivity	0.678	0.942	0.675	0.740
FNR	0.322	0.058	0.325	0.260
MCC	0.381	0.921	0.393	0.434
Specificity	0.703	0.979	0.718	0.694
NPV	0.695	0.941	0.697	0.736
Precision	0.687	0.980	0.696	0.699

The model with conventional LinkNet achieves a precision of 0.699, indicating improved performance in correctly identifying true positives compared to previous models but not yet optimal. In contrast, the Improved LinkNet+SqueezeNet model achieves a significantly higher precision of 0.980, demonstrating its superior ability to accurately identify true positive attack instances while minimizing false positives.

Conclusion

Thus, the proposed hybrid detection model presented a significant advancement in addressing the intricate cybersecurity challenges faced by IIoT environments. Through the integration of Improved LinkNet-Squeeze architecture, Improved SMOTE preprocessing, and Improved Entropy-based mitigation, the model aimed to enhance the accuracy, efficiency, and resilience of intrusion detection systems. By leveraging the strengths of various techniques while mitigating their respective limitations, the model offered a holistic approach to IIoT security.

References

[1] F. S. Melícias, T. F. R. Ribeiro, C. Rabadão, L. Santos and R. L. D. C. Costa, "GPT and Interpolation-Based Data Augmentation for Multiclass Intrusion Detection in IIoT", IEEE Access, vol. 12, pp. 17945-17965, 2024, doi: 10.1109/ACCESS.2024.3360879

[2] P. Verma, J. G. Breslin, D. O'Shea, N. Mehta, N. Bharot and A. Vidyarthi, "Leveraging Gametic Heredity in Oversampling Techniques to Handle Class Imbalance for Efficient Cyberthreat Detection in IIoT", IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1940-1951, Feb. 2024, doi: 10.1109/TCE.2023.3319439

[3] Ferrag, Mohamed Amine, Mthandazo Ndhlovu, Norbert Tihanyi, Lucas C. Cordeiro, Merouane Debbah, Thierry Lestable and Narinderjit Singh Thandi, "Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices", IEEE Access, vol. 12, pp. 23733-23750, 2024, doi: 10.1109/ACCESS.2024.3363469

[4] X. Jin, C. Ma, S. Luo, P. Zeng and Y. Wei, "Distributed IIoT anomaly detection scheme based on blockchain and federated learning", Journal of Communications and Networks, vol. 26, no. 2, pp. 252-262, April 2024, doi: 10.23919/JCN.2024.000016

[5] M. S. Alshehri, O. Saidani, F. S. Alrayes, S. F. Abbasi and J. Ahmad, "A Self-Attention-Based Deep Convolutional Neural Networks for IIoT Networks Intrusion Detection", IEEE Access, vol. 12, pp. 45762-45772, 2024, doi: 10.1109/ACCESS.2024.3380816

[6] Okfie, Mayar Ibrahim Hasan, and Shailendra Mishra, "Anomaly Detection in IIoT Transactions using Machine Learning: A Lightweight Blockchain-based Approach", Engineering, Technology & Applied Science Research 14, no. 3 (2024), pp: 14645-14653

[7] S. Ullah, W. Boulila, A. Koubâa and J. Ahmad, "MAGRU-IDS: A Multi-Head Attention-Based Gated Recurrent Unit for Intrusion Detection in IIoT Networks", IEEE Access, vol. 11, pp. 114590-114601, 2023, doi: 10.1109/ACCESS.2023.3324657

[8] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security", Big Data Mining and Analytics, vol. 6, no. 3, pp. 273-287, September 2023, doi: 10.26599/BDMA.2022.9020032

[9] M. M. Shtayat, M. K. Hasan, R. Sulaiman, S. Islam and A. U. R. Khan, "An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things," in IEEE Access, vol. 11, pp. 115047-115061, 2023, doi: 10.1109/ACCESS.2023.3323573

[10] O. M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement and C. D'amours, "Secure Industrial IoT Systems via RF Fingerprinting Under Impaired Channels With Interference and Noise", IEEE Access, vol. 11, pp. 26289-26307, 2023, doi: 10.1109/ACCESS.2023.3257266

[11] Bibhuti Bhusana Behera, Binod Kumar Pattanayak and Rajani Kanta Mohanty, "Deep Ensemble Model for Detecting Attacks in Industrial IoT", International Journal of

Information Security and Privacy (IJISP), vol.16, pp.1-29, 2022.

[12] Bibhuti Bhushan Behera, Rajani Kanta Mohanty, Binod Kumar Pattanayak., “Attack Detection and Mitigation in Industrial IoT: An Optimized Ensemble Approach”, Specialusis Ugdymas, vol.1, pp.879-905, 2022.

[13] Bibhuti Bhusana Behera, Rajani Kanta Mohanty, Binod Kumar Pattanayak “Ensemble Model for Detecting Attacks in Industrial Internet of Things (IIoT)”, NeuroQuantology, vol.20, p.1399, 2022.

[14] Bibhuti Bhusana Behera, Rajani Kanta Mohanty, Binod Kumar Pattanayak, “A Deep Fusion Model For Automated Industrial Iot Cyber Attack Detection And Mitigation”, International Journal of Electrical and Electronics Research (IJEER), vol.10, pp.604-613, 2022.

[15] Bibhuti Bhusana Behera, Rajani Kanta Mohanty, Binod Kumar Pattanayak, “A SYNTHESIZED ARCHITECTURE AND FUTURE RESEARCH DIRECTIONS FOR INDUSTRIAL IOT IN THE MINING INDUSTRY”, Journal of East China University of Science and Technology, vol.65, pp.511-528, 2022

[16] Sahar Soliman, Wed Oudah and Ahamed Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things", Alexandria Engineering Journal, Volume 81, 15 October 2023, Pages 371-383, doi : 10.1016/j.aej.2023.09.023

[17] Francesco Vitale, Fabrizio De Vita, Nicola Mazzocca and Dario Bruneo, "A Process Mining-based unsupervised Anomaly Detection technique for the Industrial Internet of Things", Internet of Things, Volume 24, December 2023, 100993, doi : 10.1016/j.iot.2023.100993

[18] Shiming Li, Jingxuan Wang, Yuhe Wang, Guohui Zhou and Yan Zhao, "EIFDAA: Evaluation of an IDS with function-discarding adversarial attacks in the IIoT", Heliyon, Volume 9, Issue 2, February 2023, e13520, doi : 0.1016/j.heliyon.2023.e13520

[19] Subir Halder and Thomas Newe, "Radio fingerprinting for anomaly detection using federated learning in LoRa-enabled Industrial Internet of Things", Future Generation Computer Systems, Volume 143, June 2023, Pages 322-336, doi : 10.1016/j.future.2023.01.021

[20] Renfang Wang, Hong Qiu, Xu Cheng and Xiufeng Liu, "Anomaly detection with a container-based stream processing framework for Industrial Internet of Things", Journal of Industrial Information Integration, Volume 35, October 2023, 100507, doi : 10.1016/j.jii.2023.100507

[21] Abbas Yazdinejad, Mostafa Kazemi, Reza M. Parizi, Ali Dehghantanha and Hadis Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things", Digital Communications and Networks, Volume 9, Issue 1, February 2023, Pages 101-110, doi : 10.1016/j.dcan.2022.09.008

[22] Alanazi, Rehab and Ahamed Aljuhani, "Anomaly Detection for Industrial Internet of Things Cyberattacks", Computer Systems Science & Engineering 44, no. 3 (2023)

[23] S. M. Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms", IEEE Access, vol. 9, pp. 113199-113212, 2021, doi: 10.1109/ACCESS.2021.3104113

[24] Huma, Zil E, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani and Fatmah Baothman, "A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things", IEEE Access, vol. 9, pp. 55595-55605, 2021, doi: 10.1109/ACCESS.2021.3071766

[25] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino and S. E. Quincozes, "Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks Within Industrial Internet of Things", IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4569-4578, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028652

[26] R. Taheri, M. Shojafar, M. Alazab and R. Tafazolli, "Fed-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT", IEEE Transactions on Industrial Informatics, vol. 17, no. 12, pp. 8442-8452, Dec. 2021, doi: 10.1109/TII.2020.3043458

[27] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty and M. Ryan, "Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment", IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7704-7715, Nov. 2021, doi: 10.1109/TII.2020.3025755

[28] S. Latif, Z. Zou, Z. Idrees and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network", IEEE Access, vol. 8, pp. 89337-89350, 2020, doi: 10.1109/ACCESS.2020.2994079.