Enhancing Security of Industrial Internet of Things Against Botnet Attacks through Hybrid Deep Learning Methodology

1st Snehesh Theophine Jose
Dept. Computer Science And Engineering
Mangalam College Of Engineering
Ettumanoor, Kottayam
sneheshtheophine321@gmail.com

2nd Mr. Eldhose K Paul
Dept. Computer Science And Engineering
Mangalam College Of Engineering
Ettumanoor, Kottayam
eldhose.paul@mangalam.in

***Abstract*—The Industrial Internet of Things (IIoT) has transformed the manufacturing industry by enabling intelligent interconnected devices and driving digital innovation. However, the distributed nature of IIoT, Industrial 5G, IoT sensing devices, IT/OT convergence, Edge Computing, and Time Sensitive Networking also make it a prime target for cyber-attacks. Multivariant and persistent bot attacks are particularly devastating for IIoT systems, and detecting them is both complex and critical. To address this challenge, I propose a hybrid intelligent mechanism that leverages Deep Learning (DL) to protect IIoT infrastructure from sophisticated botnet attacks. The proposed solution has been rigorously evaluated using the latest datasets, performance metrics, and DL benchmark algorithms, achieving a detection rate of 99.94 and an impressive speed efficiency of 0.066(ms). The results demonstrate the effectiveness of our approach in accurately identifying and mitigating multi-variant bot attacks, providing much-needed security for IIoT systems. To ensure the security of heterogeneous IIoT devices and generated traffic, existing solutions for identifying cyber threats and attacks predominantly rely on pre-defined signature vectors for pattern matching, also known as signature-based detection.**

***Index Terms*—IIoT botnet detection, deep learning (DL), Internet-of-thing (IoT), network security.**

I. Introduction

The Industrial Internet of Things (IIoT) is rapidly growing and becoming integral to our daily lives. It is revolutionizing various industries, generating massive amounts of data for analytics and decision-making. By 2025, it is estimated that around 75 billion IoT devices will be connected. However, the heterogeneity of devices and data transmission, along with resource constraints, make IIoT vulnerable to cyber threats. Attacks like phishing, DoS, MITM, and Botnet can compromise the entire system, with Botnets being particularly dangerous. Current solutions rely on signature-based detection, which is insufficient for dynamic IoT infrastructure and zero-day threats. A hybrid DL-driven intelligent threat detection mechanism is proposed to address these challenges, combining deep learning algorithms with signature-based detection for real-time detection of unseen threats. This approach aims to provide a comprehensive solution to the security concerns of IIoT systems.

II. Related Work

A. Reinforcement learning in blockchain-enabled IIoT networks

Reinforcement learning (RL) techniques have shown great potential in addressing some of the major issues faced by blockchain-enabled IIoT networks, such as block time minimization and transaction throughput enhancement. However, there are several challenges and open research questions that need to be addressed, such as the energy-constrained nature of IIoT devices, scalability paradox, and anonymous data sharing. Additionally, there is a need for further research to explore the applicability of Reinforcement learning techniques in blockchain-enabled IIoT networks, and to develop novel solutions that can improve the performance, security, and efficiency of these networks. Overall, the insights and results provided in this work could pave the way for the rapid adoption of blockchain technology in IIoT networks, but moreresearch is needed to fully realize its potential.

[1].

B. A secure industrial internet of things (iiot) framework for resource management in smart manufacturing

The SoftMax-DNN algorithm is used to optimize resource scheduling and to make efficient use of available resources in the IIoT framework. Improved RSA techniques are applied to ensure secure transmission of data between devices. The algorithm aims to reduce process delays and improve the use of resources to achieve optimal planning goals. The proposed algorithm achieves the lowest latency, the lowest energy consumption, and the highest network lifetime. Overall, this work presents an efficient and secure approach for IIoT resource scheduling and data transmission. [2].

C. An ensemble deep learning-based cyber-attack detection in industrial control system

The proposed attack detection model utilizes a deep learning approach with a combination of DNN and DT classifiers to detect cyber-attacks. The model also includes a deep representationlearning component, which constructs new balanced representations from raw imbalanced datasets. Multiple unsupervised SAEs are used to learn new representations from unlabeled data, and the new representations are then passed through a DNN and a DT classifier to identify cyberattacks. The performance of the proposed model is validated using two different ICS datasets obtained from real critical infrastructure facilities. Overall, the proposed approach shows promising results in detecting cyber-attacks in ICS environments. [3].

D. The industrial internet of things (IIoT): An analysis framework.

Developing an analysis framework for IIoT is crucial in identifying and characterizing IIoT devices for studying system architectures and analyzing security threats and vulnerabilities. The proposed framework aims to improve existing definitions of IIoT and provide a basis for analyzing the deployment of IoT technologies in industrial settings. Currently, there is a lack of consistent approaches to assess the safety and security risks associated with IIoT deployment. Therefore, the proposed framework can aid in identifying potential risks and vulnerabilities in IIoT systems, ultimately improving the safety and security of industrial settings. [4].

E. Spectral Efficiency Optimization for Next Generation NOMA-Enabled IoT Networks

The proposed resource management scheme is aimed at maximizing the total spectral efficiency (SE) of a multi-carrier IoT network by using power non-orthogonal multiple access (NOMA) multiplexing. The authors used a decoupling technique to divide the main problem into two subproblems and formulated a non-convex optimization problem for both single-tone and multi-tone modes. To obtain efficient solutions, the authors exploited mixed integer programming and difference of convex programming approaches. The proposed scheme can efficiently allocate spectral resources in a multi-carrier IoT network, which is crucial for the seamless connectivity of a massive number of IoT devices in the 6G aera. [5].

III. EXISTING METHODOLOGY

Botnets are very dangerous for computer network security and can cause various types of communication (spam, denial of service, phishing, etc.). This article introduces Bonnet detection method based on network traffic analysis A botnet detection framework has been proposed that consists of two parts: data collection and filtering, botnet search and analysis. The first part is sent in split strategy to capture traffic data on the network, filter the data, and distribute the data. Second,it sends in the middle, collects all the information of the operators and uses the fusion algorithm and feature recog- nition algorithm information to identify the botnets. Detection method works fine and can detect botnets in test environment

IV. PROPOSED METHODOLOGY

The proposed solution aims to detect botnet attacks in the IIoT environment using a hybrid deep learning framework. This framework combines Long Short-Term Memory (LSTM) and Deep Neural Network (DNN) models to achieve accurate and efficient detection. Hybrid models are known for their ability to improve results by leveraging different deep learning classifiers. LSTM is chosen for its effectiveness in learning from longer data sequences, which is crucial in IIoT with its rapid generation of large data volumes. DNN, on the other hand, enhances the algorithm’s speed and efficiency, ultimately boosting its predictive capabilities.

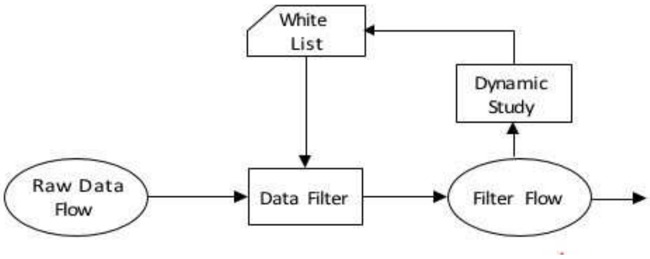

Fig. 1. Dynamic Study Method

Pre-processing of the dataset is a vital step in the proposed DL-based attack detection framework. This step focuses on cleansing, transforming, and preparing the data for accurate classification. Additionally, data visualization and feature engineering techniques are employed to extract valuable insights from the dataset. Once the pre-processing stage is finished, the prepared data is inputted into the LSTM and DNN classifiers to detect various types of IIoT attacks.

The LSTM (Long Short-Term Memory) is a type of recurrent neural network specifically designed to handle longer sequences of data. This characteristic makes it well-suited for processing the significant influx of data generated by IIoT devices. Its ability to capture long-term dependencies in the data is particularly valuable in the context of IIoT.

In contrast, the Deep Neural Network (DNN) is utilized to enhance the algorithm’s predictive capabilities and improve its speed and efficiency. DNNs are known for their ability to learn complex patterns and features from data, making them a valuable component of the hybrid model.

By combining the LSTM and DNN classifiers, the hybrid model harnesses the strengths of both approaches, leading to a more accurate and efficient solution for IIoT attack detection. This integration allows the model to effectively process and analyze the vast amounts of data produced by IIoT devices, resulting in higher accuracy predictions in a shorter amount of time.

Overall, the proposed DL-based attack detection framework seeks to offer a more effective and efficient solution for the detection of sophisticated botnet threats and attacks within the IIoT environment. By leveraging deep learning techniques, such as LSTM and DNN, the framework aims to enhance the accuracy and speed of detection, addressing the unique challenges posed by the dynamic and heterogeneous nature of IIoT systems. The ultimate goal is to provide robust security measures that can effectively safeguard IIoT devices and networks from the ever-evolving landscape of cyber threats.

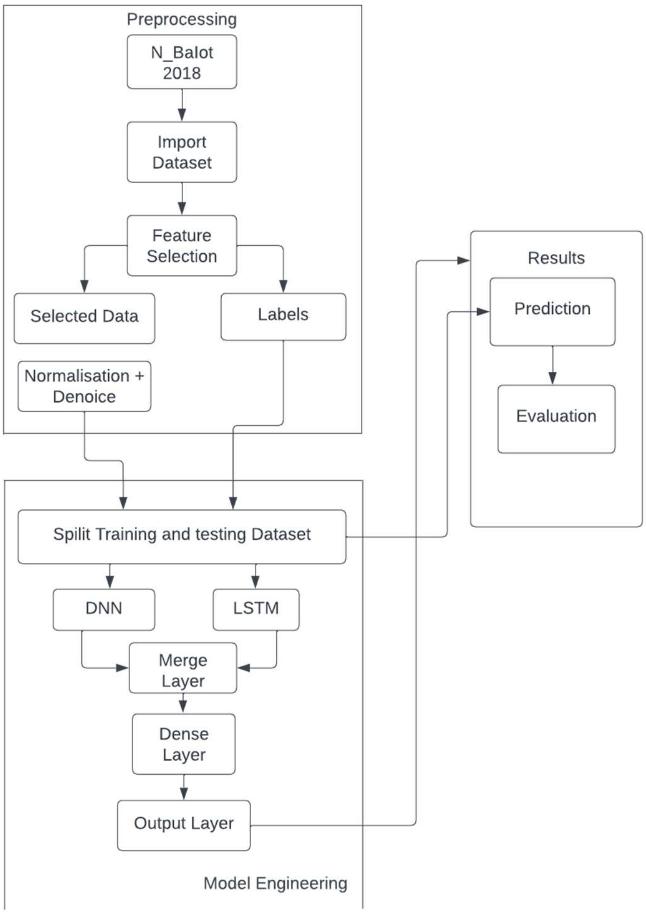

Fig. 2. Proposed Architecture

V. CONCLUSION

The increasing number of IIoT devices has raised concerns about the safety hazards associated with them. Research has shown that Industrial Internet of Things devices are vulnerable to various types of botnet attacks. These attacks have the potential to disrupt the entire IIoT network, emphasizing the need for effective and flexible detection solutions.

To address this issue, I propose a novel hybrid DL algorithm utilizing the DNN-LSTM architecture. This algorithm offers flexibility and adaptability in detecting multiple types of attacks. The proposed system demonstrates a remarkable identification accuracy of 99.94

Looking ahead, the future plan involves utilizing different DL-driven systems for real-time detection of various threats and cyberattacks in IIoT across different countries. The aim is to enhance the security of IIoT systems and mitigate the risks associated with botnet attacks.

VI. FUTURE WORKS

In terms of future research, several avenues have been identified. One such avenue involves creating a second dataset that encompasses all ten attack vectors utilized by botnet malware. This dataset will be instrumental in demonstrating the model's capability to detect the latest evolution of botnets.The modified source code will be employed to generate third- party data, which will then be compared against negative detection based on control name stream and stream.

The next section of the research will delve into the solution for the detection problem. Additionally, other approaches to enhance the effectiveness of botnet operations in IoT willbe explored. By enabling consumers to identify when their devices are infected, the aim is to raise awareness about vulnerabilities and assist users in making informed decisions when it comes to acquiring and using IoT devices.

ACKNOWLEDGMENT

The author expresses gratitude and extends thanks to all the anonymous reviewers for their valuable suggestions and comments. Their input is highly appreciated, as it will contribute to the improvement of this paper.

REFERENCES

[1] K. A. Abuhasel and M. A. Khan, "A secure industrial internet of things (iiot) framework for resource management in smart manufacturing,"IEEE Access, vol. 8, pp. 117354–117364, 2020.

[2] W. U. Khan, T. N. Nguyen, F. Jameel, M. A. Jamshed, H. Pervaiz, M. A. Javed, and R. Jantti, "Learning-based resource allocation for backscatter-aided vehicular networks," IEEE Transactions on Intelligent Transportation Systems, pp. 1–15, 2021.

[3] [3] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learningbased cyber-attack detection in industrial control system," IEEE Access, vol. 8, pp. 83965–83973, 2020.

[4] [4] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," Computers in industry, vol. 101, pp. 1–12, 2018.

[5] [5] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jantti, and Z. Han, "Spectral¨ efficiency optimization for next generation noma-enabled iot networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15284– 15297, 2020.D. C. Yadav and S. Pal, "Prediction of heart disease using feature selection and random forest ensemble method," Int. J. Pharmaceutical Res., vol. 12, no. 4, 2022.

[6] E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, "Towards effective feature selection in machine learning-based botnet detection approaches," in 2014 IEEE Conference on Communications and Network Security. IEEE, 2014, pp. 247–255.

[7] M. Sundermeyer, R. Schluter, and H. Ney, "Lstm neural networks for ¨ language modeling," in Thirteenth annual conference of the international speech communication association, 2012.

[8] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," Information Sciences, vol. 513, pp. 386–396, 2020.