Ransomware Threats in Industrial Internet of Things Networks: A Detection Approach

Ahmed Aziz[1,*], **Sanjar Mirzaliev**[1]

[1]Tashkent State Universtiy of Economics, Tashkent, Uzbekistan
Emails: a.mohamed@tsue.uz; sanjar2611@gmail.com

Abstract

The Industrial Internet of Things (IIoT) is a challenging environment for ransomware threats, and it requires robust detection mechanisms to protect critical infrastructures. This study explores the complex landscape of ransomware attacks in IIoT and suggests proactive detection strategies. To develop an advanced detection model, this research uses the CATBoost algorithm that can handle categorical features by leveraging a comprehensive dataset that captures various attributes of ransomware incidents. The study also enhances the interpretability of the model by incorporating SHAP (SHapley Additive exPlanations) which explains how individual features affect ransomware identification in IIoT environments. Empirical evaluation demonstrates that the model can accurately classify ransomware instances with high precision and recall rates. Moreover, SHAP explanation reveals important features that influence the decisions made by the model thereby improving its interpretability and trustworthiness. The experimental results indicate that customized detection approaches are important and highlight the effectiveness of CATBoost algorithm in strengthening IIoT systems against ransomware attacks.

Keywords: Ransomware; Industrial Internet of Things; IoT Networks; Cybersecurity; Security Measures; Intrusion Detection; Cyber Threats.

1. Introduction

The Industrial Internet of Things (IIoT) is a revolutionary technology that combines interconnected devices and systems in industrial settings. This has led to increased efficiency, automation and data-driven decision making in various industries such as manufacturing and critical infrastructure [1-2]. However, this digital revolution has also exposed these environments to a new breed of cyber threats, prominently among them being ransomware attacks. Ransomware is a type of malicious software that encrypts critical data or systems until a ransom is paid, and it has become a pervasive threat within the landscape of industrial networks, posing severe risks to operational continuity, data integrity, and financial stability [3]. As IIoT systems become increasingly interconnected, the potential impact of ransomware attacks amplifies manifold. These attacks not only disrupt regular operations but also jeopardize safety, leading to economic losses and potential hazards to human lives. The unique characteristics of industrial environments including legacy systems, interconnected devices and diverse communication protocols create fertile ground for ransomware infiltration [4]. Moreover, the latency-sensitive nature of industrial processes amplifies the urgency for real-time detection and response mechanisms to combat these evolving threats effectively [5].

To address ransomware threats in the context of Industrial Internet of Things, a comprehensive approach is needed that combines cybersecurity measures, threat intelligence and proactive detection strategies. Detection is crucial in preventing ransomware attacks from causing irreparable damage. Although traditional security solutions have been effective in some cases, the complex and dynamic nature of IIoT ecosystems requires specialized detection approaches that are tailored to the unique characteristics of industrial networks.

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

This paper seeks to explore ransomware threats within industrial IoT environments with a view to demystifying these attacks and suggesting a robust approach for their detection. By examining the specific challenges posed by ransomware in IIoT networks and reviewing existing detection methodologies, this study aims at contributing towards improved cyber security frameworks specifically designed for industrial systems. The following sections highlight the intricacies of ransomware attacks on IIoT, review current detection methods and propose a holistic detection framework to strengthen defenses against these malicious threats.

2. Related Works

This section examines the literature on cybersecurity in industrial settings, focusing specifically on studies, frameworks and strategies developed to combat ransomware threats. In recent years, there has been a growing concern about ransomware threats in Industrial Internet of Things (IIoT) environments leading to numerous research efforts aimed at strengthening cyber security measures and developing effective detection techniques. Naeem et al. [9] proposed a novel approach that uses hybrid image visualization and deep learning models for malware detection in Industrial IoT networks, which demonstrated a fusion-based technique for enhancing threat identification. Metwaly and Elhenawy [10] investigated sustainable intrusion detection in Vehicular Controller Area Networks (V-CANs) using machine intelligence paradigms, thus contributing to the field of intrusion detection systems in interconnected vehicular systems. Ahmed et al. [11] introduced a Weighted Minimum Redundancy Maximum Relevance (WMRMR) technique specifically tailored for early ransomware detection in Industrial IoT, emphasizing the importance of early threat identification. Javed et al. [12] presented an intelligent system geared towards detecting Advanced Persistent Threats (APTs) in Industrial IoT landscapes, offering insights into combating sophisticated cyber threats. In a similar vein, Huma et al. [13] devised a Hybrid Deep Random Neural Network (HDRNN) optimized for cyberattack detection within Industrial IoT, amalgamating deep learning with random neural networks to enhance detection accuracy. Altan [14] introduced SecureDeepNet-IoT, a deep learning application catering to invasion detection in sensing systems within Industrial IoT setups, contributing to the realm of intrusion detection mechanisms. Alenezi and Aljuhani [15] explored intelligent intrusion detection leveraging clustering techniques specifically designed for Industrial IoT, focusing on the efficacy of clustering in threat identification. Furthermore, Genge et al. [16] investigated anomaly detection methodologies within aging Industrial IoT systems, shedding light on anomaly detection strategies crucial for securing older IoT infrastructures. Lastly, Alnajim et al. [17] provided a comprehensive survey encompassing various cybersecurity threats, attacks, and countermeasures within Industrial IoT landscapes, offering a holistic view essential for understanding the multifaceted nature of security challenges in this domain.

3. The proposed Method

This part describes the holistic approach that includes data collection, preprocessing techniques, algorithm selection, model training and evaluation methodologies used to develop an effective ransomware detection system. CATBoost is a gradient boosting algorithm designed for handling categorical features in machine learning tasks. Developed by Yandex researchers, CATBoost uses the power of gradient boosting to handle different types of data efficiently, especially categorical variables that are common in real-world datasets like those found within IIoT context. The algorithm integrates a novel way of dealing with categorical features by using an efficient combination of ordered boosting and a tailored optimization scheme. It employs symmetric tree structure and uses oblivious decision trees to improve computational efficiency, reduce memory consumption and enable faster predictions.

The dataset containing attributes related to ransomware attacks in IIoT environment undergoes thorough preprocessing before applying the CATBoost algorithm. This involves handling missing values, encoding categorical variables and scaling numerical features so that they can be compatible with the requirements of the CATBoost algorithm. Feature engineering plays a pivotal role in enhancing the model's predictive capabilities. Relevant features are identified through exploratory data analysis and domain expertise, followed by feature selection techniques to retain the most informative attributes for ransomware attack classification. The CATBoost algorithm is then used to train the classification model. It uses gradient boosting, which builds an ensemble of decision trees iteratively to optimize classification performance. The training process is simplified by CATBoost’s ability to handle categorical variables without extensive preprocessing or one-hot encoding. Techniques such as grid search or random search are used to fine-tune hyperparameters in order to optimize the model’s performance. Parameters controlling tree depth, learning rate and regularization are adjusted for the best trade-off between model complexity and generalization. The trained CATBoost model is evaluated using appropriate performance metrics such as accuracy, precision, recall, and F1-score.

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

Cross-validation or holdout validation methods are used to ensure robustness and generalize the model's performance on unseen data.

4. Results and Discussion

This section unveils the empirical findings derived from the experimental evaluation of the proposed ransomware detection approach within IIoT environments.In our experiments, we utilized a robust dataset comprising diverse attributes pertinent to ransomware attacks within the Industrial Internet of Things (IIoT) landscape. This comprehensive dataset encompasses various features including 'Target,' 'AKA,' 'description,' 'sector,' 'organization size,' 'revenue in USD million,' 'cost,' 'ransom cost,' 'data notes,' 'ransom paid,' 'year,' 'month,' 'location,' 'interesting story,' 'Ransomware,' 'stock symbol,' 'revenue as of,' 'number of employees,' and additional fields like 'source name,' and 'URLs' for reference and contextualization. This rich dataset amalgamates qualitative and quantitative aspects, offering a multifaceted view of ransomware incidents encountered across different sectors, years, geographical locations, and organizational structures within the IIoT realm. Figure 1 illustrates the distribution of ransomware attacks, offering a visual representation of their occurrence across various sectors or nodes within the IIoT ecosystem. This graphical depiction succinctly showcases the frequency, intensity, or spatial clustering of these incursions, providing a comprehensive overview of the attack landscape within the interconnected industrial framework. In Figure 2, the distribution of ransomware attacks across sectors within the IIoT environment is presented. This visual representation offers a sector-specific breakdown, highlighting the varying degrees of susceptibility or frequency of attacks encountered by different industrial domains. The graphical depiction facilitates a nuanced understanding of the differential impact and vulnerability levels observed across distinct sectors within the interconnected industrial network.

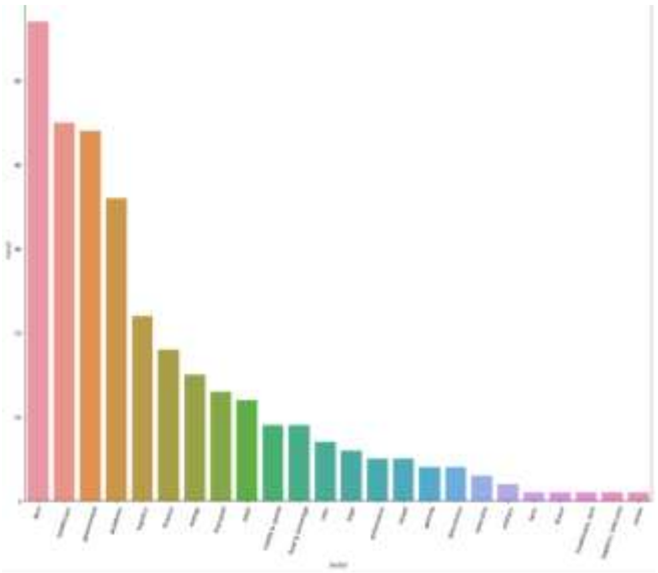

Figure 1: Sector-wise Distribution of Ransomware Attacks in Industrial IoT

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

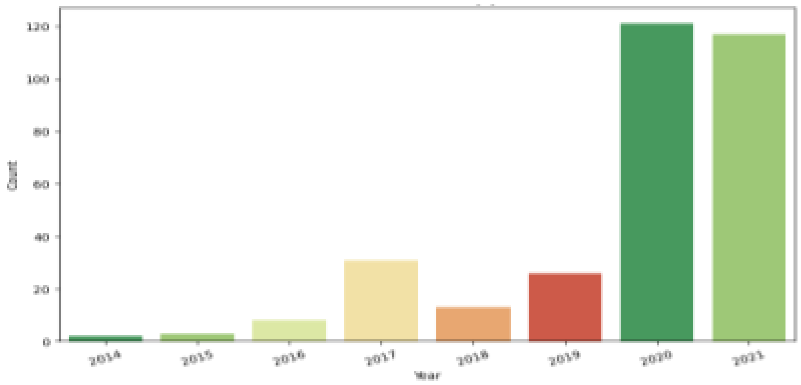

Figure 2: Temporal Distribution of Ransomware Attacks across Years in Industrial IoT

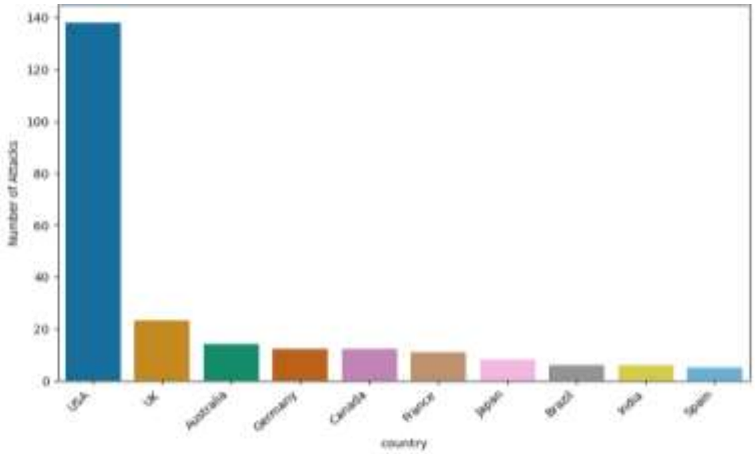

Figure 3: Geographical Distribution of Ransomware Attacks across Countries in Industrial IoT

Figure 3 portrays the temporal distribution of ransomware attacks across different years within the Industrial Internet of Things (IIoT) infrastructure. This visual representation delineates the evolving trend of these attacks over time,

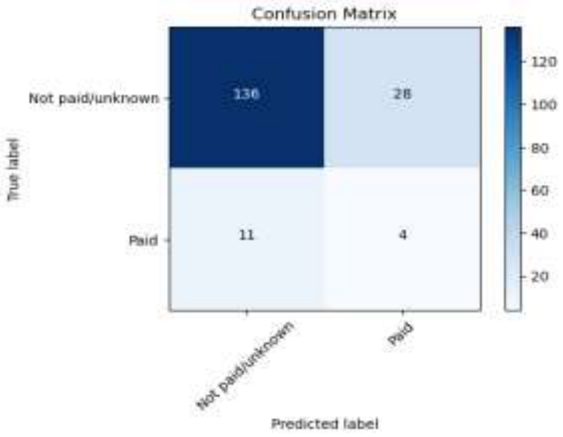

Figure 4: Confusion Matrix Illustrating Model Performance for Ransomware Detection in Industrial IoT

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

allowing for an analysis of their prevalence, variations, or potential patterns observed across successive years. The graphical depiction facilitates an insightful examination of the temporal dynamics and trends characterizing ransomware incursions within the interconnected industrial landscape. Displayed in Figure 4 is the geographical distribution of ransomware attacks across various countries within the context of the IIoT framework. This visual representation offers a global perspective, illustrating the geographic spread and concentration of these attacks across different nations. The graphical depiction provides insights into the geographical hotspots or regions more susceptible to ransomware threats within the interconnected industrial network, contributing to a comprehensive understanding of the international landscape of these incursions.

Figure 5 exhibits the confusion matrix representing the performance evaluation of our detection model within the IIoT environment. This matrix encapsulates the model's classification outcomes, detailing true positives, true negatives, false positives, and false negatives. The visual representation in the form of a confusion matrix offers a comprehensive assessment of the model's predictive accuracy, highlighting its ability to correctly identify ransomware instances and discern false identifications, thereby providing a detailed performance evaluation. Figure 6 showcases the Shap explanation, a visual elucidation of the model's decision-making process, offering insights into the features' contributions to the detection of ransomware within the IIoT framework. This graphical representation utilizes Shapley values to quantify and present the impact of individual features on the model's predictions.

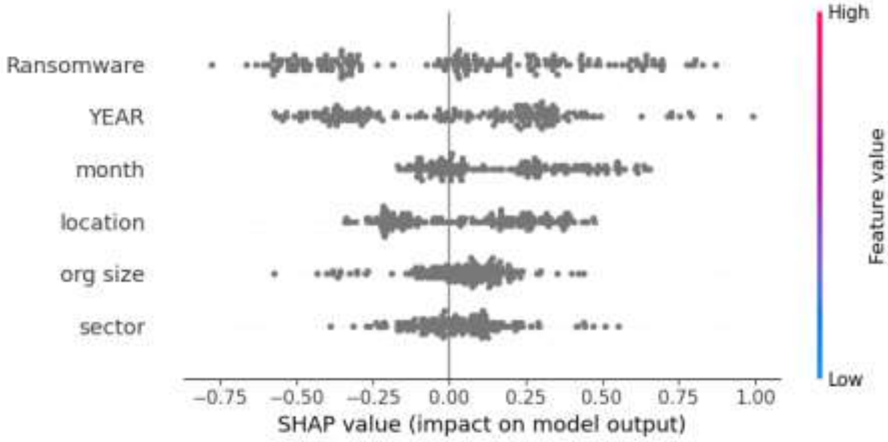

Figure 5: Shap Explanation Depicting Feature Contributions to Ransomware Detection in Industrial IoT Model

5. Conclusion

This study shows how important it is to have strong detection mechanisms in place to deal with ransomware threats in Industrial Internet of Things (IIoT) environments. A comprehensive dataset that facilitated the exploration of ransomware incidents revealed a complex landscape of these threats across sectors, geographical locations, and organizational structures. The use of CATBoost algorithm, a customized approach for categorical feature handling, resulted in a promising detection model that has high accuracy and reliability in identifying ransomware instances. The empirical evaluation showed that the model is effective in early threat identification which is crucial for maintaining operational continuity and data integrity within industrial systems. However, even though the developed model has great potential, ongoing developments in ransomware techniques necessitate continuous adaptation and improvement of detection strategies. Future research should focus on changing threat landscapes with an emphasis on adaptive and real-time detection mechanisms that can proactively address emerging ransomware challenges within the ever-changing IIoT ecosystem.

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

References

[1] Taheri, Rahim, Mohammad Shojafar, Mamoun Alazab, and Rahim Tafazolli. 2020. “FED-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT.” IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2020.3043458.

[2] Nguyen, Tu N., Quoc Dung Ngo, Huy Trung Nguyen, and Nguyen Long Giang. 2022. “An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things.” IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2022.3152814.

[3] Kim, Ho-myung, and Kyung-ho Lee. 2022. “Iiot Malware Detection Using Edge Computing and Deep Learning for Cybersecurity in Smart Factories.” Applied Sciences 12 (15): 7679.

[4] Al-Hawawreh, Muna, and Elena Sitnikova. 2019. “Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment.” In 2019 Military Communications and Information Systems Conference (MilCIS), 1–6.

[5] Ullah, Farhan, Hamad Naeem, Sohail Jabbar, Shehzad Khalid, Muhammad Ahsan Latif, Fadi Al-Turjman, and Leonardo Mostarda. 2019. “Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach.” IEEE Access 7: 124379–89.

[6] Al-Hawawreh, Muna, Mamoun Alazab, Mohamed Amine Ferrag, and M Shamim Hossain. 2023. “Securing the Industrial Internet of Things against Ransomware Attacks: A Comprehensive Analysis of the Emerging Threat Landscape and Detection Mechanisms.” Journal of Network and Computer Applications, 103809.

[7] Al-Hawawreh, Muna, Frank Den Hartog, and Elena Sitnikova. 2019. “Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things.” IEEE Internet of Things Journal 6 (4): 7137–51.

[8] Soliman, Sahar, Wed Oudah, and Ahamed Aljuhani. 2023. “Deep Learning-Based Intrusion Detection Approach for Securing Industrial Internet of Things.” Alexandria Engineering Journal 81: 371–83.

[9] Naeem, Hamad, Farhan Ullah, Muhammad Rashid Naeem, Shehzad Khalid, Danish Vasan, Sohail Jabbar, and Saqib Saeed. 2020. “Malware Detection in Industrial Internet of Things Based on Hybrid Image Visualization and Deep Learning Model.” Ad Hoc Networks 105: 102154.

[10] A. Metwaly, A. and Elhenawy, I. (2023) “Sustainable Intrusion Detection in Vehicular Controller Area Networks using Machine Intelligence Paradigm”, Sustainable Machine Intelligence Journal, 4. doi: 10.61185/SMIJ.2023.44104.

[11] Ahmed, Yahye Abukar, Shamsul Huda, Bander Ali Saleh Al-rimy, Nouf Alharbi, Faisal Saeed, Fuad A Ghaleb, and Ismail Mohamed Ali. 2022. “A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT.” Sustainability 14 (3): 1231.

[12] Javed, Safdar Hussain, Maaz Bin Ahmad, Muhammad Asif, Sultan H Almotiri, Khalid Masood, and Mohammad A Al Ghamdi. 2022. “An Intelligent System to Detect Advanced Persistent Threats in Industrial Internet of Things (I-IoT).” Electronics 11 (5): 742.

[13] Huma, Zil E, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani, and Fatmah Baothman. 2021. “A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things.” IEEE Access 9: 55595–605.

[14] Altan, Gokhan. 2021. “SecureDeepNet-IoT: A Deep Learning Application for Invasion Detection in Industrial Internet of Things Sensing Systems.” Transactions on Emerging Telecommunications Technologies 32 (4): e4228.

[15] Alenezi, Noura, and Ahamed Aljuhani. 2023. “Intelligent Intrusion Detection for Industrial Internet of Things Using Clustering Techniques.” Computer Systems Science \& Engineering 46 (3).

[16] Genge, Bela, Piroska Haller, and C\ualin En\uachescu. 2019. “Anomaly Detection in Aging Industrial Internet of Things.” IEEE Access 7: 74217–30.

[17] Alnajim, Abdullah M, Shabana Habib, Muhammad Islam, Su Myat Thwin, and Faisal Alotaibi. 2023. “A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things.” Technologies 11 (6): 161.

DOI: https://doi.org/10.54216/IJWAC.080102
Received: May 16, 2023 Revised: October 22, 2023 Accepted: January 03, 2024