Adopting Machine Learning Techniques for Predictive Maintenance in the Industrial Internet of Things (Iot)

Dr Guguloth Lachiram[1], Dr Vadithya Redya[2], Dr.Somepalli Uma Maheswararao[3], Mr Azmeera Ramesh[4], Mr S L Hemanth Chandra[5], Mrs P.Swetha Nagasri[6]

[1]Department of Computer Science & Engineering, Narsimhareddy Engineering College, Maisamma Guda, Hyderabad, TS, E-Mail: rams.5812@gmail.com, ORCID ID: 0009-0006-9289-3580
[2]Department of Computer Science & Engineering, MLRITM, Nehru Outer Ring Road, Domara PochamPally, Hyderabad, TS.
[3]Department of Computer Science & Engineering (Data Science), CMRCET, Medchal, Hyderabad,TS, Email: umaheshphd@gmail.com, ORCID ID: 0000-0002-2000-4047
[4]Department of Computer Science & Engineering(AI&ML) CMRTC, Kondla Koya, Hyderabad,TS.
[5]Department of Computer Science & Engineering, Narsimhareddy Engineering College, Maisamma Guda, Hyderabad, TS.
[6]Department of Computer Science & Engineering, Koneru Lakshmaiah Educational Foundation, Bowrampet, Hyderabad, TS.

Abstract
Maintenance performed before problems occur is essential. Through specialized strategies, the machine learning (ML) approach allows systems to predict and reduce various machine failures. Predictive maintenance (PdM) has become an essential tool to improve the efficiency and reliability of industrial machines to improve maintenance management. By using ML algorithms to proactively detect and correct potential equipment failures, PdM minimizes unplanned downtime, reduces maintenance costs and improves operational efficiency. The Internet of Things (IoT) refers to the network of everyday objects connected via the Internet, global data and real-time responses. Invented by Kevin Ashton in 1999, the IoT has since revolutionized industries with examples including self-driving cars, smart TVs and RFID supply chains. As this technology evolves, it continues to have a significant impact on many industries. Recently, research on deep learning (DL) techniques, including convolutional neural networks (CNN), closed recurrent units (GRU), and long-term memory (LSTM), have focused on anomaly detection. This thesis proposes a new DL-based hybrid strategy to perform critical security assessments before cyber-attacks on IoT-embedded infrastructure. The models integrate techniques such as XGBoost, Autoencoders, CNN, GRU and LSTM to build, train and validate efficiently.

1. Introduction

In the 21st century, the Internet of Things (IoT) has become a fundamental part of daily life, with applications ranging from healthcare and home automation to smart vehicles and industrial manufacturing. Advances in microdevice manufacturing, sub-evaluation, and server connectivity have enabled the development of innovative IoT products and have broadly transformed communications-centric operations.

1.1 AN INTERNET OF THINGS (IIOT)

IoT is widely recognized as a technological breakthrough that can address major societal challenges such as smart cities, traffic monitoring, pollution prevention, and connected healthcare. The Industrial Internet of Things (IIoT) is a subset of the IoT that integrates machine-to-machine (M2M) communications with industrial automation and robotics. As shown in Figure 1, IIoT represents the convergence of IoT technology and the Industry 4.0 paradigm.

IIoT enables real-time collection, sharing, and interpretation of data across distributed systems, enabling faster decision-making. For example, errors in industrial plants can be identified and corrected before catastrophic failures occur. IIoT leverages traditional industrial control systems (ICS) through connected smart devices to save time, resources, and costs by creating intelligent workplace systems.

Laut Chan et al. (2017) integrate IIoT intelligent electronic devices into the entire lifecycle of industrial processes. This enables M2M communications and supports human-machine interaction, making it a central component of modern and future industrial ecosystems.

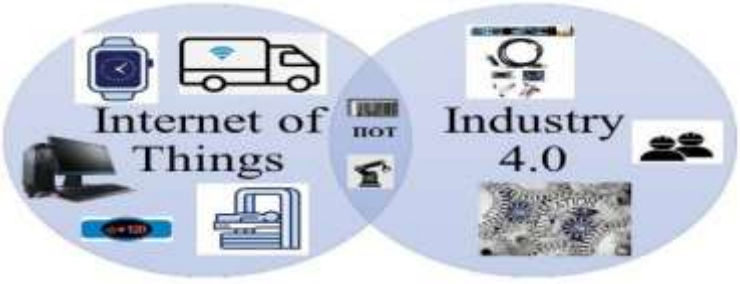

Figure 1. Internet of Things

1.2 INTRUSION DETECTION IN IIOT NETWORKS

In industrial environments where service interruptions can be significant, it is important to protect IIoT systems from cyber threats. Intrusion detection systems (IDS) serve as an important defense mechanism that monitors network traffic for anomalous behavior.

IDS systems are typically categorized by deployment strategy.

 A centralized IDS monitors traffic at the edge of the network. B. Border router. However, this may cause insider threats to be overlooked (Kasinathan et al., 2013).

 Distributed IDS distributes detection tasks across multiple devices and requires lightweight and autonomous optimization due to resource limitations (Wallgren et al., 2013).

 Hybrid IDS combines centralized and distributed strategies to improve detection coverage.

Watchdog nodes configured on IIoT devices monitor neighboring devices and issue alerts when suspicious behavior is detected (Gyamfi & Jurcut, 2022). This collaborative detection strategy helps prevent network breaches in real time.

2. ATTACK VECTORS AGAINST IIOT AND IOT DEVICES

Cyber attacks are intentional efforts to breach the digital infrastructure of organizations or individuals, focusing on unauthorized access, data tampering, and service disruption (Sengupta et al., 2020). Common security attack vectors in IIoT are categorized into four levels

1. Physical Attacks: Involve unauthorized access or alterations to physical devices such as PLCs and RTUs, including techniques like firmware manipulation and hardware backdoors.
2. Network Attacks: Aim to disrupt communication between IIoT devices.
3. Software Attacks: Exploit vulnerabilities within firmware or application logic.
4. Application Layer Attacks*: Target higher-level protocols or APIs, including reconnaissance attacks that map networks and identify vulnerable devices through methods like address scanning and device identification. These categories encapsulate essential threats to IIoT security.

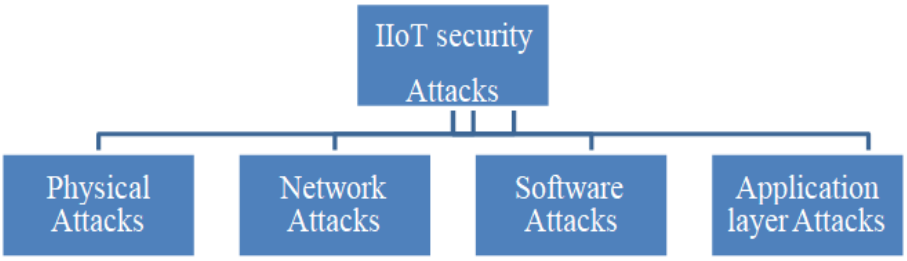

Figure 2. IIoT security attacks associated with various layers Physical Attacks

3. Proposed Intrusion Detection Mechanism

3.1 DATASET PREPARATION

This section presents an intrusion detection approach using machine learning for Industrial Internet of Things (IIoT) environments. The methodology comprises two main phases. The first phase involves dataset preparation, where a relevant dataset with labeled records of both normal and malicious network traffic involving IoT medical devices is crucial for training machine learning (ML) models. The second phase involves evaluating various ML models.

3.2 ML MODEL EVALUATIONS

The K-Nearest Neighbor (KNN) model had the best accuracy, while Decision Trees, Random Forest, SVM, Logistic Regression, and ANN also produced good results. Naïve Bayes performed poorly in comparison.

- **Figure 3** shows False Alarm Rate (FAR): lower values indicate better performance.
- **Figure 4** shows training times: ANN took the longest, while Naïve Bayes and Decision Trees trained faster.

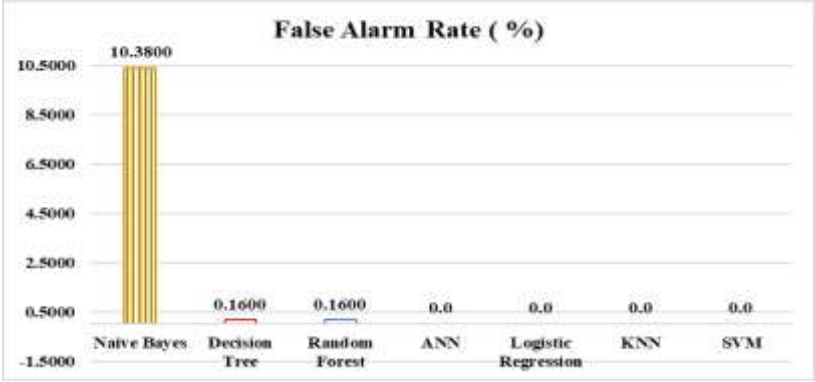

Figure 3. The False Alarm Rate Results

Figures in the text illustrate the False Alarm Rate (FAR) and training times for the models. A lower FAR indicates better performance, with Naïve Bayes having the highest FAR and lowest productivity. ANN took the longest to train, whereas Naïve Bayes and Decision Trees required less time for training.

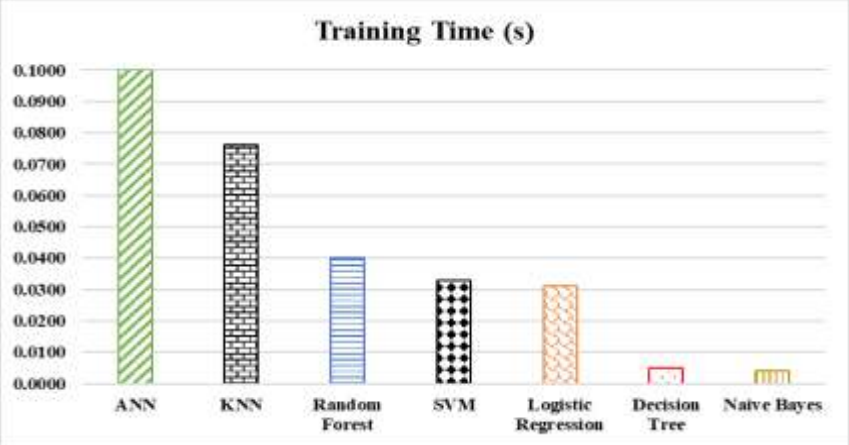

Figure 4. Training time

4. A Secure And Efficient Iiot Anomaly Detection Approach Using A Hybrid Deep Learning Technique

The rise of Internet of Things (IoT) technology has greatly influenced industrial sectors by integrating smart devices for real-time monitoring and improving decision-making processes. The Industrial Internet of Things (IIoT) has led to improvements in predictive maintenance and productivity optimization due to the immense amount of data these devices produce. However, the increased connectivity also introduces security concerns and challenges in anomaly detection, which is vital for spotting and responding to irregular behaviors in IIoT systems. Traditional methods often struggle with the complexity and volume of IIoT data.

4.1 ANOMALY

Anomalies or outliers in data are observations that differ significantly from others, possibly indicating new, unknown processes. Detecting these anomalies is crucial for mitigating risks. Deep learning, a branch of machine learning, has gained popularity for its ability to represent data through layered neural networks, allowing it to handle anomaly detection efficiently. Recent research shows deep learning techniques surpass traditional methods in performance, as they adaptively learn complex data patterns, enhancing anomaly detection in numerous applications. Researchers continuously strive to develop effective models to address anomaly detection challenges in dynamic data environments.

4. 2 CNN AND GRU MODEL

The CNN and GRU model integrates Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs) to enhance performance in anomaly detection, especially in industrial IoT systems. This hybrid model effectively captures both spatial and temporal data, making it ideal for analyzing complex sequences. The CNN part extracts spatial features through convolutional layers, which learn patterns by applying filters. By stacking multiple layers, the CNN captures hierarchical representations. The GRU component adds the ability to model temporal dependencies, allowing the model to understand how the data changes over time. Combining CNN and GRU outputs fuses spatial and temporal information, leading to accurate predictions and a comprehensive understanding of the data.

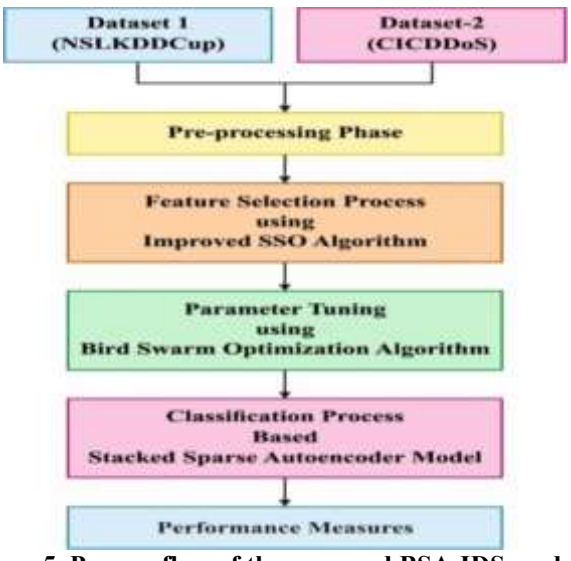

Figure 5. Process flow of the proposed BSA-IDS model

The CNN component focuses on spatial features, detecting anomalies and patterns at a local level, while the GRU component captures temporal sequences, understanding how data evolves. This combination allows the model to identify anomalies that show both spatial and temporal characteristics, offering a robust solution for anomaly detection in industrial IoT systems. Extensive testing has shown that the CNN GRU model achieves high accuracy, precision, recall, and F1 score, enabling effective identification of anomalies for enhanced security measures in industrial settings.
The model's pseudo code outlines its architecture and training process. It defines the input layer, followed by convolution, optional batch normalization, max-pooling, and GRU layers. A dense layer and an output layer conclude the architecture, suitable for binary or multi-class classification. The model is compiled with an optimizer and loss function, then trained with specified parameters. Finally, it is evaluated or used for predictive tasks.

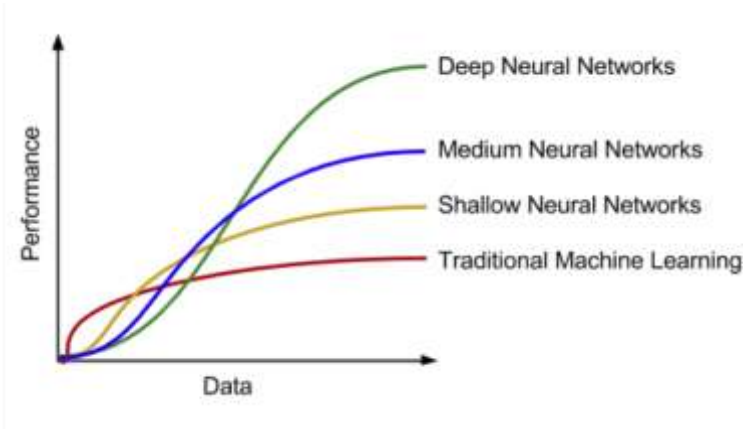

Figure 6. Performance Comparison of Deep Learning vs Traditional Algorithms.

5. Conclusion

This study developed and tested a new deep learning-based Intrusion Detection System (IDS) model focused on secure data transmission in Industrial Internet of Things (IIoT) environments. The model involves preprocessing, feature selection using ISSO algorithms, classification through SSAE, and parameter optimization with BSA. These components enhance the model's attack detection rate. Experiments using datasets like NSL-KDD and CIC-DDoS show the model's superiority in performance measures compared to other methods. An efficient feature selection algorithm, ERT-FS, is integrated with the IGAN model to identify important features in abnormal traffic. Various neural network architectures, including CNN, GRU, LSTM, and others, were assessed for anomaly detection in edge IIoT systems, revealing their effectiveness in identifying anomalies in edge IIoT data.

6. References

1. X. Xie, C. Wang, S. Chen, G. Shi, and Z. Zhao, "Real-time illegal parking detection system based on deep learning," in Proceedings of the 2017 international conference on deep learning technologies, 2017, pp. 23–27.
2. T. Schlegl, P. Seeb¨ock, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," in Information Processing in Medical Imaging: 25th International Conference, IPMI 2017, Boone, NC, USA, June 25-30, 2017, Proceedings. Springer, 2017, pp. 146–157.
3. J. Xiong, S. Bharati, and P. Podder, "Machine and deep learning for iot security and privacy: Applications, challenges, and future directions," Security and Communication Networks, vol. 2022, p. 8951961, 2022. [Online]. Available: https://doi.org/10.1155/2022/8951961
4. V. Chandola, A. Banerjee, and V. Kumar, "Outlier detection: A survey," ACM Computing Surveys, vol. 14, p. 15, 2007.
5. D. M. Hawkins, Identification of outliers. Springer, 1980, vol. 11.
6. Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, "Artificial intelligence based anomaly detection of energy consumption
7. in buildings: A review, current trends and new perspectives," Applied Energy, vol. 287, p. 116601, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261921001409
8. N. Alexopoulos, E. Vasilomanolakis, N. R. Iv´ank´o, and M. Mu¨hlh¨auser, "Towards blockchain-based collaborative intrusion detection systems," in Critical Information Infrastructures Security, G. D'Agostino and A. Scala, Eds. Cham: Springer International Publishing, 2018, pp. 107–118.
9. L. Wen, X. Li, L. Gao, and Y. Zhang, "A new convolutional neural network-based data-driven fault diagnosis method," IEEE Transactions on Industrial Electronics, vol. 65, no. 7, pp. 5990–5998, 2018.
10. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," nature, vol. 521, no. 7553, pp. 436–444, 2015.
11. S. Tofigh, M. O. Ahmad, and M. Swamy, "A low-complexity modified thinet algorithm for pruning convolutional neural networks," IEEE Signal Processing Letters, vol. 29, pp. 1012–1016, 2022.