IST-Africa 2026 Conference Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
IST-Africa Institute and IIMC, 2026
ISBN: 978-1-905824-76-2

Machine Learning-Based Security Mechanisms for Threat Detection in Smart Manufacturing

Siyabonga NKAMBULE, Siyabulela DYAKALASHE
University of Fort Hare, Ring Road Rd, Dikeni, 5700, South Africa
Tel: +27 040 602 2750, Email: 224113546@ufh.ac.za, sdyakalashe@ufh.ac.za

Abstract: Smart Manufacturing, integrating emerging technologies, has transformed production efficiency but has simultaneously heightened exposure to cyber threats. The interconnective nature of these environments introduces vulnerabilities to ransomware, data breaches, and supply chain attacks, making robust cybersecurity mechanisms imperative. Reviewed literature suggests that traditional security measures often fail to address the dynamic nature of smart manufacturing threats effectively. This study investigates machine learning-based threat detection through Logistic Regression (LR) and Random Forest (RF) models, employing the NSL-KDD and CICIDS2017 datasets to enhance cybersecurity in smart manufacturing environments. Results indicate that RF achieved the highest accuracy (99.97% on CICIDS2017 and 99.77% on NSL-KDD), while LR performed competitively (99.52% and 99.11%, respectively), offering optimised efficiency in low-computation scenarios. Although both models demonstrated strong adaptability across datasets of varying sizes, the study is limited by reliance on benchmarked datasets rather than real-world industrial data. For future applications, we recommend a hybrid LR–RF detection framework in real-world smart factory settings, as it combines robustness with computational efficiency.

Keywords: Smart Manufacturing, Machine Learning, Intrusion and Threat Detection, Cybersecurity.

1. Introduction

Smart Manufacturing has revolutionised industrial production by introducing digital technologies such as the Internet of Things (IoT), Machine Learning (ML), Artificial Intelligence (AI), and Cloud Computing, thereby transforming conventional processes into highly automated, data-driven operations [1]. This shift enables real-time decision-making, improved productivity, adaptability, and operational efficiency across industries [2]. However, the interconnected nature of smart manufacturing environments also exposes organisations to heightened cybersecurity risks, including ransomware, denial-of-service (DoS), phishing, and supply-chain attacks [3][4].

As Cyber-Physical Systems (CPS) and IoT devices interact across multiple networks, sensitive data and critical infrastructure become prime targets for cyber adversaries. The rising volume and sophistication of these attacks pose substantial risks, such as financial losses, operational disruptions, and compromised intellectual property [5]. A notable example occurred in February 2023, when Applied Materials, a global semiconductor supplier, suffered a supply-chain-related ransomware attack that disrupted shipments and resulted in approximately $250 million in lost sales [6]. Such incidents underscored the urgency of addressing vulnerabilities within interconnected manufacturing operations.

Traditional security mechanisms are often ill-equipped to address these risks, particularly in detecting and preventing advanced cyber threats in real-time [7]. This gap

highlights the need for adaptive, intelligent solutions. In this context, ML has emerged as a promising approach for strengthening cybersecurity in smart manufacturing. The ability to process vast datasets, recognise patterns, detect anomalies, and adapt to evolving threats positioned ML as an essential tool for proactive defence [6][8]. ML techniques have been widely adopted to enhance threat detection and mitigation in modern cybersecurity systems [31][37]. Supervised learning algorithms such as Logistic Regression (LR) and Random Forest (RF) are particularly effective in enabling real-time threat detection, predictive analytics, automated responses, and adaptability.

1.1 Research Purpose

The study addresses the lack of robust and specialised cybersecurity mechanisms capable of safeguarding smart manufacturing systems against increasingly complex cyberattacks. Conventional methods fail to adequately detect evolving threats in interconnected environments where automation and connectivity often take precedence over strong security protocols [9]. The study aims to address the limitations of conventional methods for detecting, preventing, and responding to evolving cyber threats in real-time. By providing empirical evidence on the effectiveness of LR and RF models in smart manufacturing cybersecurity, the research contributes to both practical industrial applications and the academic understanding of ML-driven threat mitigation.

1.2 Research Objectives

The objectives of the research were to (1) evaluate the effectiveness of these models in identifying cyber threats, (2) compare their accuracy, and (3) provide a comparative foundation for a future hybrid framework tailored to smart manufacturing needs. By doing so, the study aimed to safeguard sensitive data, protect intellectual property, enhance operational resilience, and reduce risks associated with data breaches and unauthorised access.

1.3 Research Justification

The justification for this study is grounded in the increasing reliance on IoT and digital technologies within smart manufacturing, which, while improving operational efficiency, also amplifies exposure to cyber threats. Prior incidents demonstrate that traditional security measures were insufficient to mitigate sophisticated attacks, resulting in significant operational, financial, and reputational consequences. This creates a critical need for proactive, intelligent, and adaptive security mechanisms, tailored to the unique characteristics of smart manufacturing environments.

In essence, the study justifies the pressing need for specialised, efficient, and adaptive cybersecurity strategies that could safeguard interconnected manufacturing operations while supporting the continued adoption of IoT, ML, AI, and cloud technologies.

1.4 Research Significance

The significance of this study is in its ability to strengthen cybersecurity in IoT-enabled smart manufacturing environments and contribute to both industry practice and academic research. The key benefits achieved included:

1. **Enhanced Security Posture**: The study develops and improves security mechanisms that increase resilience against evolving cyber threats.
2. **Operational Continuity**: It reduces the likelihood of disruptions and downtime caused by security breaches, ensuring stable production processes.
3. **Data Integrity and Confidentiality**: Manufacturing data is protected, guaranteeing accuracy, reliability, and trustworthiness in automated systems.
4. **Economic Efficiency**: The findings help mitigate financial losses by lowering remediation costs and safeguarding intellectual property from theft or misuse.

5. **Compliance and Trust**: The study supports adherence to industry regulations and standards, fostering greater trust among stakeholders, clients, and consumers.
6. **Risk Management**: Exposure to unauthorised access, data leakage, and other security risks is minimised through proactive detection and prevention.
7. **Efficiency in Smart Manufacturing**: Reliability and performance of interconnected manufacturing systems are strengthened, leading to more efficient operations.
8. **Privacy Protection**: Organisational data and intellectual property are safeguarded, ensuring competitive advantage and ethical data use.

2. Research Methodology

This section outlines the methods and procedures employed to apply ML for cybersecurity threat mitigation in smart manufacturing. The study adopted a signature-based approach, combining key stages such as data collection, preprocessing, feature selection, and algorithm evaluation to identify and analyse cyber threats effectively. The study utilises secondary datasets, including CICIDS2017 and NSL-KDD, focusing on specific attacks such as DoS, DDoS, and botnet attacks. Data preprocessing steps, including cleaning and normalisation, were performed to enhance the performance of ML models.

To refine the datasets, the study applied feature selection techniques, including Principal Component Analysis (PCA) and Correlation Analysis. The machine learning algorithms investigated—RF and LR—were then trained and evaluated using performance metrics such as Accuracy, Precision, and F1 score.

The signature-based approach is particularly suitable, as it detects cyber threats by identifying known patterns, or signatures, of malicious activity (e.g., code sequences, file structures, or network traffic patterns) associated with past attacks. By comparing new inputs against signatures stored in databases, this method enables real-time detection and blocking of threats, thereby minimising operational disruptions in smart manufacturing systems.

Through this structured process, the study sought to balance detection accuracy with operational efficiency while establishing reliable metrics for assessing ML-based security systems in smart manufacturing. The methodology approach included:

1. **Data Collection** – This study employs secondary data sourced from publicly accessible benchmark datasets – CICIDS2017 and NSL-KDD – both available on Kaggle [14][15]. These datasets were selected because they cover diverse attack categories aligned with the security threats relevant to smart manufacturing, including DoS, DDoS, botnet, brute-force, and port-scanning attacks. The CICIDS2017 dataset contains both normal traffic, labelled as “BENIGN”, and malicious traffic, labelled as “ATTACKS”. The attack data includes distributed denial-of-service (DDoS) and other anomalies representative of real-world scenarios [16]. The NSL-KDD dataset is an improved version of the original KDD’99 intrusion detection dataset. It consists of one class attribute and forty-one feature attributes, though only a subset significantly contributes to attack detection. By focusing on the most relevant attributes, this dataset enables the evaluation of ML algorithms for intrusion detection in smart manufacturing environments [17].
2. **Data Preprocessing** – This is a critical stage in preparing raw data for machine learning analysis. Since this study relies on secondary datasets, several preprocessing steps were applied to ensure data quality and improve model performance.
    a) Data Cleaning – Errors, inconsistencies, and missing values were identified and corrected to preserve data integrity, especially in the CICIDS2017 dataset, due to its large size. This process reduces noise and eliminates abnormalities that could otherwise distort the outputs of machine learning models, leading to more reliable and accurate analytical results [18][19].

b) Normalisation – Numerical features were scaled to a fixed range, typically between 0 and 1, to ensure uniform contribution across features [20]. Normalisation is particularly important in this context as it prevents features with larger scales from disproportionately influencing the model, thereby improving convergence and overall algorithm performance [10][21].
c) Encoding – Categorical variables were converted into numerical representations to make them compatible with machine learning algorithms [22]. Encoding enables the use of diverse input features, such as network protocols and service types, in intrusion detection models, which is essential for identifying cybersecurity threats in smart manufacturing systems [23].

3. **Feature Selection and Extraction** – Feature selection and extraction are critical in improving model accuracy, reducing computational complexity, and minimising the risk of overfitting, especially in intrusion detection tasks [24]. The original NSL-KDD dataset contained 41 attributes. After data cleaning and extraction, only the most relevant features were retained for model training. In this dataset, approximately 70% (45,978 records) was used for training, while the remaining 30% (22,544 records) was reserved for testing.

The CICIDS2017 dataset initially comprised seventy-eight attributes. For this study, the "Label" feature was the primary focus, as it distinguishes between normal traffic (BENIGN) and anomalous traffic (ATTACKS) [25]. The CICIDS2017 dataset contains 2,830,743 records.

To refine these datasets for machine learning tasks, two key methods were employed:

a) Correlation Analysis: This method identifies and retains features that show strong linear relationships with the target variable by computing the Pearson correlation coefficient [26]. Features with higher correlation with the target are likely to provide meaningful information to the model, whereas low correlation features often introduce noise and complexity [27].
b) Principal Component Analysis (PCA): PCA was applied to reduce dimensionality by projecting high-dimensional data onto a lower-dimensional space while retaining maximum variance. This approach enhances efficiency while ensuring that key data patterns remain intact [28].

Through these steps, the datasets were transformed into more efficient and manageable forms, thereby optimising their suitability for the machine learning algorithms applied in this study.

4. **Training and Evaluation** – The core training phase implemented two complementary machine learning algorithms, RF and LR, strategically selected for their proven efficacy in smart manufacturing cybersecurity applications.
   a) RF serves as the primary ensemble method, chosen for its exceptional scalability with large datasets and its ability to capture nonlinear relationships in high-dimensional manufacturing data. The algorithm demonstrated strong performance with 99.86% accuracy, using twenty-two optimally selected features [25][29].
   b) Logistic Regression (LR) provides a computationally efficient alternative, particularly effective for linear patterns and smaller datasets such as NSL-KDD, achieving 98.27% accuracy on CICIDS2017 with rapid execution and minimal computational overhead [30]. These algorithms represent the most frequently deployed approaches in smart manufacturing cybersecurity frameworks [31].
5. **Evaluation Metrics** – The comprehensive evaluation framework employed multiple performance indicators to assess model effectiveness across different operational scenarios. Primary metrics include Accuracy for overall predictive correctness, Precision to quantify the proportion of correctly identified positive cases, and F1 Score to balance precision and recall for optimal threat detection performance. These metrics

provide quantitative measures of the algorithms' capability to identify security anomalies while maintaining operational reliability.

6. **Performance Analysis** – The final analytical phase conducts a thorough performance assessment through detailed examination of classification rates and baseline comparisons against normal operational parameters. Advanced diagnostic measures, including True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate (TNR), provide comprehensive insights into algorithm performance characteristics [12]. The Base Rate (Baseline – Normal Operation) serves as a critical benchmark for evaluating detection effectiveness under standard manufacturing conditions.

This systematic evaluation approach ensures that selected algorithms achieve an optimal balance between high detection accuracy and minimal false alarm generation, thereby maintaining manufacturing process continuity while providing robust cybersecurity protection. The methodology validates that the chosen machine learning techniques can effectively identify security threats without introducing excessive operational disruption, ensuring seamless integration within smart manufacturing environments [11][32].

The resulting validated models provide reliable intrusion detection capabilities specifically tailored for smart manufacturing applications, offering both high-performance threat identification and operational stability essential for critical industrial systems.

3. Results Discussion and Analysis

3.1 Model Training

For the NSL-KDD Dataset: an LR model was implemented with a high maximum iteration limit of 1.2 million to mitigate potential convergence issues that may arise when optimising complex datasets. The target labels were flattened into a one-dimensional array before training. Both training and testing durations were recorded to evaluate computational performance. The model required 13.81 minutes for training, after which prediction time was measured on the dataset to compare the computational cost of both phases. Despite the high iteration limit, a convergence warning from the ***lbfgs_optimizer*** indicated that the model did not reach the optimal solution. To address this issue and improve performance, additional approaches such as feature scaling, parameter adjustments, and alternative solvers were considered. In addition, an RF classifier was implemented using the entropy criterion with a maximum depth of 4. Training and prediction times were measured, and Optuna was used for hyperparameter optimisation, allowing automatic tuning of parameters such as ***max_depth*** and ***max_features***. After 30 optimisation trials, the best parameters were identified and used to train a new RF model. The optimised model achieved high accuracy on both training and testing datasets, demonstrating improved performance and generalisation.

For the CICIDS2017 Dataset, the class labels were encoded for binary classification. The "BENIGN" label was encoded as 0, representing normal traffic, while "DDoS" was encoded as 1, representing malicious activity. The dataset was then split into training (70%) and testing (30%) sets using ***train_test_split***, with ***random_state*=42** to ensure reproducibility. The resulting datasets consisted of 16,177 training samples and 6,933 testing samples, each containing 78 features. An RF classifier with 50 trees (***n_estimators* = 50**) was trained on the training data, and predictions were generated on the test set to evaluate the model's ability to detect potential attacks. Additionally, an LR model was implemented for comparison. The LR model was initialised with a fixed ***random_state*** to ensure consistent results across multiple runs. The model was trained using ***x_train*** and ***y_train***, after which predictions were generated on the test dataset (***x_test***) and stored as

lr_pred. This process enabled the evaluation of both the RF and LR models on unseen data, allowing their classification performance to be analysed using standard evaluation metrics.

3.2 Research Limitations

There were a few limiting factors, namely:

- **Computational Power**: The effectiveness and speed of model training and testing were constrained by the lack of a faster computer, specifically an Intel i9 CPU. Large-scale dataset processing was impacted by hardware limitations, particularly when using sophisticated algorithms like RF, which require more computing power to operate at peak performance.
- **Time Constraints**: The time available to conduct comprehensive testing, optimise models, and investigate other machine learning techniques that could enhance outcomes was limited due to computational hardware resources, academic coursework demands, and research timetable and deadlines.
- **Dataset Availability**: Finding suitable datasets that are comprehensive and representative of real-world cyber threats in Smart Manufacturing proved challenging. Although NSLKDD and CICIDS2017 were used, these datasets may not fully reflect the latest attack vectors and complexities observed in modern industrial settings, limiting the applicability of the findings to newer cybersecurity threats.

3.3 Data Analysis

Several recent studies have evaluated intrusion detection performance using the NSL-KDD and CICIDS2017 datasets, often achieving high accuracy through sophisticated preprocessing techniques and ensemble learning methods. As shown in Table I, [33] applied a B-Stacking ensemble model for IoT network intrusion detection, achieving 99.11% accuracy on CICIDS2017 and 98.5% on NSL-KDD. Similarly, [13] proposed a quantum-inspired Least Squares Support Vector Machine (LS-SVM) combined with exhaustive feature selection, which evaluated all possible feature subsets and achieved 99.5% accuracy on CICIDS2017 and 99.3% on NSL-KDD. [13] also achieved near-perfect precision (100%) and recall (99%–100%) using exhaustive feature selection with LS-SVM, albeit with high computational cost. Interestingly, they reported minimal training time for LS-SVM relative to alternatives, emphasising its suitability for real-time applications. By comparison, our RF model achieved even higher overall accuracy, suggesting that careful hyperparameter tuning and baseline cleaning are sufficient to achieve top-tier performance. One study used information-gain feature selection to identify the top ten attributes (e.g., packet length, protocol type, destination port), followed by RF training, achieving 99.96% accuracy [34]. [33] reported approximately 99.54% RF accuracy. Using cross-validation or balanced splits, some studies applied InfoGain selection and 10-fold cross-validation, achieving RF accuracy of 99.86% [34]. Our RF results (99.97% CICIDS2017, 99.77% NSL-KDD) slightly exceed these benchmarks, particularly in precision and F1 scores, indicating improved capability to capture subtle patterns in network traffic. The empty fields in Tables I and II below indicate that the metric was not reported in the cited study. For example, [35] reported on NSL-KDD that a Random Forest classifier achieved 98.81% accuracy, 97.70% precision and 96.67% F1 score. Similarly, [65] reported NSL-KDD results for Logistic Regression of 84.0% accuracy and 83.0% precision (F1 not given). For CICIDS2017, a deep autoencoder study reported single-RF accuracy of 99.86% (precision/F1 not provided) [33]. No study was found that provided LR metrics for CICIDS2017. These approaches relied heavily on computationally intensive feature-selection strategies to maximise detection accuracy. Tables 1 and 2 below summarise the

baseline results from the related studies conducted with the NSL-KDD and CICIDS2017 datasets, respectively.

TABLE I: NSL-KDD Baseline (Related Work)

Model	Accuracy	Precision	F1 Score
Random Forest	*98.81*	*97.70*	*96.67*
B-Stacking Ensemble	*98.50*	-	-
LS-SVM + Exhaustive Feature Selection	***99.30***	***100***	***99-100***
Logistic Regression	*84.00*	*83.00*	-

TABLE II: CICIDS2017 Baseline (Related Work)

Model	Accuracy	Precision	F1 Score
B-Stacking Ensemble	*99.11*	-	-
LS-SVM + Exhaustive Feature Selection	*99.50*		
Random Forest (RF) + InfoGain	***99.96***	-	-
Deep Autoencoder + RF	*99.86*	-	-

In contrast, the methodology employed in this study relied primarily on data cleaning and hyperparameter optimisation using Optuna, without aggressive feature elimination. Despite the simpler pipeline, the proposed RF and LR models achieved competitive performance. Tables III and IV summarise the results from this study, utilising the NSL-KDD and CICIDS2017 datasets to train the model using the RF and LR algorithms.

TABLE III: NSL-KDD Results (Current Study)

Model	Accuracy	Precision	F1 Score
Random Forest	***99.77***	***99.90***	***99.90***
Logistic Regression	*99.11*	*98.72*	*98.86*

TABLE IV: CICIDS2017 Results (Current Study)

Model	Accuracy	Precision	F1 Score
Random Forest	***99.97***	***99.96***	***99.96***
Logistic Regression	*99.52*	*99.48*	*99.47*

- **Accuracy**: the RF model achieved 99.77% accuracy on NSL-KDD (0.96% increase) and 99.97% on CICIDS2017 (0.01% increase), while the LR model achieved 99.11% (≈15.11% increase) on NSL-KDD and 99.52% accuracy on CICIDS2017, respectively.
- **Precision**: the RF model, with the NSL-KDD dataset, achieved 99.90% (2.2% increase), whereas LR achieved 98.72% (15.72% increase). Unfortunately, for the CICIDS2017 comparison, no related work baseline results were obtained from the reviewed literature (a similar issue was reported for F1 Score measurements). However, we still obtained high percentage scores, with RF reporting 99.96% and LR reporting 99.48%.
- **F1 Score**: RF model achieved 99.90% (3.23% increase), and the LR model achieved 98.86% through the NSL-KDD dataset. With the CICIDS2017 dataset, RF obtained 99.96% and LR 99.47%.

On the CICIDS2017 dataset, the LR model achieved strong results with 99.52% accuracy, 99.48% precision, and 99.47% F1 score, demonstrating its effectiveness. However, when we tested the RF model on the same dataset, it outperformed LR, achieving 99.97% accuracy, 99.96% precision, and 99.96% F1 score. This suggests that RF, based on ensemble learning, may better handle complex patterns in the CICIDS2017 dataset than LR, a linear model. LR also produced good results on the NSL-KDD dataset, with an F1 score of 98.86%, 98.72% precision, and 99.11% accuracy. Figure 1 visualises the comparative results analysis from training the RF and LR models using NSL-KDD and CICIDS2017 datasets. Due to hardware limitations, the number of trees and training iterations was constrained, yet it still produced remarkable results, demonstrating its resilience and ability to identify more intricate patterns in the data than LR.

These measurements indicate that the model performed exceptionally well at classifying the data, demonstrating its effectiveness in handling the datasets. These results demonstrate that careful model tuning and preprocessing can achieve acceptable performance even without complex feature selection techniques.

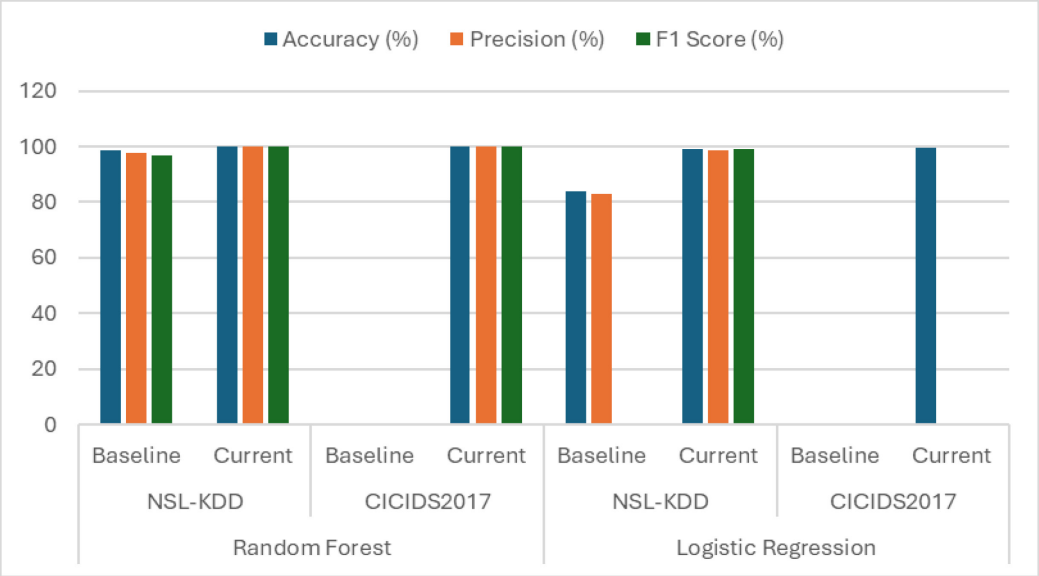

Figure 1: Comparative Model Training Results Analysis

4. Recommendations and Future Work

While each model clearly excels at intrusion detection, they also complement each other. When the dataset is less complex, LR performs quickly and reliably with less processing effort. However, because RF is an ensemble model, it can handle non-linearity and feature interactions better, making it an excellent choice for spotting subtle patterns. However, it requires more processing power and longer training cycles, particularly for larger datasets such as CICIDS2017. Given the strengths of both algorithms, we propose using a Hybrid Model that combines both LR and RF. Such a model could leverage the efficiency and speed of LR for simpler patterns while utilising the deeper pattern recognition capabilities of RF for more complex instances. This hybrid approach would be particularly beneficial for handling large-scale intrusion-detection datasets, where a balance between computational efficiency and classification accuracy is critical. The CICIDS2017 and NSL-KDD datasets, given their sizes and complexities, demonstrate that combining these two algorithms can yield an optimised solution that improves both accuracy and computational efficiency in real-world applications.

With the results we obtained from model training and testing, the recommendations for future work are as follows:

- Developing a hybrid model that combines LR and RF algorithms. Our research found these algorithms to be particularly effective across different dataset sizes, with LR performing well on smaller datasets like NSL-KDD and RF proving highly efficient on larger datasets such as CICIDS2017. Although time constraints prevented us from building the models ourselves, this study demonstrates the effectiveness of both algorithms. A hybrid approach could leverage their strengths, making it adaptable to varying data volumes while enhancing the accuracy and robustness of threat detection in Smart Manufacturing environments.
- The use of unsupervised machine learning algorithms, for example, K-Means clustering, Hierarchical Clustering, etc., on the two datasets. These datasets have not been extensively explored with unsupervised learning algorithms.
- The use of the two algorithms (LR and RF) or anomaly-based machine learning algorithms using more recently updated datasets to compare with the results achieved in this study.

- From a commercial perspective, the proposed methodology can be adopted by smart manufacturing vendors and cybersecurity solution providers to enhance existing Intrusion Detection Systems (IDS) within Industrial Control Systems (ICS) and Operational Technology (OT) environments. In the future, these models can be integrated into security monitoring platforms to support real-time threat detection, enhance system resilience, and help organisations meet cybersecurity compliance requirements and industry standards.

This study did not implement a hybrid architecture; rather, it provides a comparative evaluation of Random Forest and Logistic Regression models to establish a performance baseline. These findings are intended to inform the design of a hybrid intrusion detection framework in future work.

5. Conclusion

This study addressed the challenge of improving network intrusion detection by applying machine learning techniques to the NSL-KDD and CICIDS2017 datasets. The primary objective was to evaluate the effectiveness of Random Forest (RF) and Logistic Regression (LR) models using a streamlined preprocessing pipeline combined with hyperparameter optimisation. The results showed that the RF model achieved 99.77% accuracy on NSL-KDD and 99.97% on CICIDS2017, while LR achieved 99.11% and 99.52%, respectively. These findings demonstrate that carefully tuned traditional machine-learning models can achieve performance comparable to, or slightly better than, more complex approaches reported in previous studies, even without aggressive feature selection architectures.

The results highlight the potential to develop efficient, practical intrusion detection systems using relatively simple machine learning pipelines. However, the study is limited by the use of benchmark datasets and offline evaluation rather than real-time deployment scenarios. Future work should explore hybrid models that combine classical machine learning with deep learning techniques, incorporate advanced feature-selection and class-imbalance handling methods, and evaluate model performance in real-time or streaming environments. The key takeaway from this study is that well-optimised traditional models, particularly Random Forest, can deliver near state-of-the-art intrusion detection performance while maintaining methodological simplicity and computational efficiency.

While this study does not implement a hybrid model, the comparative results provide a strong foundation for future research aimed at developing a hybrid RF–LR framework that balances accuracy and computational efficiency.

Acknowledgements

Declaration of use of content generated by Artificial Intelligence (AI) (including but not limited to Generative-AI) in the paper

The authors confirm that there has been no use of content generated by Artificial Intelligence (AI) (including but not limited to text, figures, images, and code) in the paper entitled "*Machine Learning-Based Security Mechanisms for Threat Detection in Smart Manufacturing*".

References

1. Shaik, M.: SAP-ERP Software's Pivotal Role in Shaping Industry 4.0: Transforming the Future of Enterprise Operations. Computer Science and Engineering. 2023, 8–14 (2023). https://doi.org/10.5923/j.computer.20231301.02
2. Kromann, L., Malchow-Møller, N., Skaksen, J.R., Sørensen, A.: Automation and productivity - A cross-country, cross-industry comparison. Industrial and Corporate Change. 29, 265–287 (2020). https://doi.org/10.1093/icc/dtz039

3. Qian, C., Zhang, Y., Jiang, C., Pan, S., Rong, Y.: A real-time data-driven collaborative mechanism in fixed-position assembly systems for smart manufacturing. Robot Comput Integr Manuf. 61, (2020). https://doi.org/10.1016/j.rcim.2019.101841
4. Tsiknas, K., Taketzis, D., Demertzis, K., Skianis, C.: Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. Internet of Things. 2, 163–186 (2021). https://doi.org/10.3390/iot2010009
5. Microsoft, S.T.: Addressing cybersecurity risk in industrial IoT and OT, https://www.microsoft.com/en-us/security/blog/2020/10/21/addressing-cybersecurity-risk-in-industrial-iot-and-ot/
6. Arctic Wolf: The Top 10 Manufacturing Industry Cyber Attacks. (2024)
7. Tapesh, M.: AI In Cybersecurity: Defending Against Advanced Threats, https://wirefuture.com/post/ai-in-cybersecurity-defending-against-advanced-threats
8. Abbas, A., Fareed, G.: Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Response. (2024)
9. Malatji, M., Tolah, A.: Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics. (2024). https://doi.org/10.1007/s43681-024-00427-4
10. Wang, B.X., Chen, J.L., Yu, C.L.: An AI-Powered Network Threat Detection System. IEEE Access. 10, 54029–54037 (2022). https://doi.org/10.1109/ACCESS.2022.3175886
11. Al-Mhiqani, M.N., Ahmad, R., Abidin, Z.Z., Yassin, W., Hassan, A., Abdulkareem, K.H., Ali, N.S., Yunos, Z.: A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations, (2020)
12. Arefin, S., Chowdhury, M., Parvez, R., Ahmed, T., Abrar, A.F.M.S., Sumaiya, F.: Understanding APT detection using Machine learning algorithms: Is superior accuracy a thing? In: IEEE International Conference on Electro Information Technology. pp. 532–537. IEEE Computer Society (2024)
13. Waghmode, P., Kanumuri, M., El-Ocla, H., Boyle, T.: Intrusion detection system based on machine learning using least square support vector machine. Sci Rep. 15, (2025). https://doi.org/10.1038/s41598-025-95621-7
14. Nour, M., Jill, lay: UNSW-NB15, (2022)
15. Zaib, H.M.: NSL-KDD Dataset, https://www.kaggle.com/datasets/hassan06/nslkdd?resource=download, (2020)
16. Elmrabit, N., Zhou, F., Li, F., Zhou, H.: Evaluation of Machine Learning Algorithms for Anomaly Detection. 1–7 (2020). https://doi.org/10.1109/CyberSecurity49315.2020.9138871
17. Zakariah, M., AlQahtani, S.A., Alawwad, A.M., Alotaibi, A.A.: Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset. Computers, Materials and Continua. 77, 4025–4054 (2023). https://doi.org/10.32604/cmc.2023.043752
18. Whang, S.E., Roh, Y., Song, H., Lee, J.G.: Data collection and quality challenges in deep learning: a data-centric AI perspective. VLDB Journal. 32, 791–813 (2023). https://doi.org/10.1007/s00778-022-00775-9
19. Jbair, M., Ahmad, B., Maple, C., Harrison, R.: Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Comput Ind. 137, (2022). https://doi.org/10.1016/j.compind.2022.103611
20. Singh, D., Singh, B.: Investigating the impact of data normalization on classification performance. Appl Soft Comput. 97, (2020). https://doi.org/10.1016/j.asoc.2019.105524
21. Andrew, N.: The Importance of Data Normalization in Machine Learning, (2023)
22. Dahouda, M.K., Joe, I.: A Deep-Learned Embedding Technique for Categorical Features Encoding. IEEE Access. 9, 114381–114391 (2021). https://doi.org/10.1109/ACCESS.2021.3104357
23. Krundyshev, V., Kalinin, M.: Prevention of cyber attacks in smart manufacturing applying modern neural network methods. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing Ltd (2020)
24. Ngo, V.D., Vuong, T.C., Van Luong, T., Tran, H.: Machine learning-based intrusion detection: feature selection versus feature extraction. Cluster Comput. 27, 2365–2379 (2024). https://doi.org/10.1007/s10586-023-04089-5
25. Kurniabudi, Stiawan, D., Darmawijoyo, Bin Idris, M.Y. Bin, Bamhdi, A.M., Budiarto, R.: CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection. IEEE Access. 8, 132911–132921 (2020). https://doi.org/10.1109/ACCESS.2020.3009843
26. Santhosh, N., Srinivsan, M., Ragupathy, K.: Internet of Things (IoT) in smart manufacturing. In: IOP Conference Series: Materials Science and Engineering. Institute of Physics Publishing (2020)
27. Qu, Y.J., Ming, X.G., Liu, Z.W., Zhang, X.Y., Hou, Z.T.: Smart manufacturing systems: state of the art and future trends. International Journal of Advanced Manufacturing Technology. 103, 3751–3768 (2019). https://doi.org/10.1007/s00170-019-03754-7
28. Takio, K.: Principal Component Analysis (PCA). (2020). https://doi.org/https://doi.org/10.1007/978-3-030-03243-2_649-1

29. Johnson, R.A.: quantile-forest: A Python Package for Quantile Regression Forests. J Open Source Softw. 9, 5976 (2024). https://doi.org/10.21105/joss.05976
30. Vadhil, F.A., Salihi, M.L., Nanne, M.F.: Machine learning-based intrusion detection system for detecting web attacks. IAES International Journal of Artificial Intelligence. 13, 711–721 (2024). https://doi.org/10.11591/ijai.v13.i1.pp711-721
31. Gaurav, A., Gupta, B.B., Chui, K.T., Arya, V., Wu, J.: Enhancing Intrusion Detection in Software Defined Networks with Optimized Feature Selection and Logistic Regression. In: 2024 IEEE International Conference on Communications Workshops, ICC Workshops 2024. pp. 1809–1815. Institute of Electrical and Electronics Engineers Inc. (2024)
32. Vasconcelos, F.E., Gabriela, S.A.: Analyzing Data Theft Ransomware Traffic Patterns Using BERT. (2023). https://doi.org/10.20944/preprints202312.0158.v1
33. Urmi, W.F., Uddin, M.N., Uddin, M.A., Talukder, M.A., Hasan, M.R., Paul, S., Chanda, M., Ayoade, J., Khraisat, A., Hossen, R., Imran, F.: A stacked ensemble approach to detect cyber attacks based on feature selection techniques. International Journal of Cognitive Computing in Engineering. 5, 316–331 (2024). https://doi.org/10.1016/j.ijcce.2024.07.005
34. Djihed, B., Uday, C., Tallal, A.K.B., Imed, B.D.: Proceedings of the 1st International Conference on Creativity, Technology, and Sustainability. Springer Nature Singapore, Singapore (2025)
35. Raja Mahmood, Raja & Abdi, AmirHossien & Hussin, Masnida. (2021). Performance Evaluation of Intrusion Detection System using Selected Features and Machine Learning Classifiers. Baghdad Science Journal. 18. 0884. 10.21123/bsj.2021.18.2(Suppl.).0884.