KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 4, Oktober (2024), pp. 2013-2020

Hybrid Ensemble Model for Real-Time Intrusion Detection in IoT Networks Using Machine Learning and Deep Learning Techniques

Gregorius Airlangga
Universitas Katolik Indonesia Atma Jaya, Indonesia
E-mail: gregorius.airlangga@atmajaya.ac.id

Abstract

The rapid growth of the Internet of Things (IoT) has introduced new security challenges, as IoT devices are increasingly vulnerable to sophisticated cyberattacks. This study proposes a hybrid ensemble model combining classical machine learning algorithms (Random Forest, Gradient Boosting) with deep learning (Multi-Layer Perceptron) to improve the detection of malicious activities in IoT networks. The model leverages the RT-IoT2022 dataset, which includes diverse attack patterns such as DDoS, Brute-Force SSH, and Nmap scanning. The integration of these models using a Voting Classifier achieves superior performance by exploiting the strengths of each individual model. Evaluation results demonstrate that the hybrid model outperforms its individual components, achieving an accuracy of 99.80%, precision of 99.80%, recall of 99.80%, and F1-score of 99.80%. The proposed system demonstrates strong generalization across both frequent and rare attack types, making it well-suited for real-world IoT environments where high accuracy and low false-positive rates are critical. This study contributes to the development of robust and scalable intrusion detection systems that can adapt to evolving threats in real-time.

Keywords: *Intrusion Detection System (IDS), Internet of Things (IoT) Security, Machine Learning, Deep Learning, Hybrid Ensemble Model*

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has transformed industries by enabling interconnected devices to communicate seamlessly [1]–[3] From healthcare and smart homes to industrial automation, IoT technologies have created opportunities for real-time monitoring, predictive analytics, and automation [4]–[6]. However, as the number of IoT devices increases, so does their exposure to security vulnerabilities [7]. IoT networks, composed of heterogeneous devices with limited computational resources, are particularly susceptible to various forms of cyberattacks [8]. These attacks exploit weaknesses inherent in the distributed architecture of IoT, making traditional security methods insufficient for protecting against modern threats [9]. The security challenges in IoT networks are further exacerbated by the complexity and diversity of devices, protocols, and communication patterns [10]. While IoT networks are indispensable in many industries, their broad attack surface makes them a prime target for malicious activities [11]. Traditional Intrusion Detection Systems (IDS) are often incapable of addressing the real-time nature of these environments or keeping pace with the rapidly evolving threat landscape [12]. As a result, the need for advanced, adaptive intrusion detection mechanisms tailored to the unique characteristics of IoT networks has become critical.

Researchers have explored various approaches to improving IDS, particularly through machine learning and deep learning techniques [13]. These methods offer the potential to detect anomalies and prevent attacks before they can disrupt IoT operations [14]. However, while there has been significant progress, many existing solutions remain

ISSN: 2720-992X

inadequate in real-time, resource-constrained IoT environments [15]. Their limitations stem from difficulties in generalizing across different IoT scenarios and handling the vast and dynamic nature of the data generated by these networks [16]. To address these issues, more sophisticated, scalable, and efficient IDS systems are necessary. Over the past decade, several studies have focused on applying machine learning to detect intrusions in IoT networks [17]. These works highlight the efficacy of supervised and unsupervised learning algorithms in identifying malicious activities. For example, [18] introduced a Quantized Autoencoder (QAE) to detect anomalies in IoT environments using the RT-IoT2022 dataset. Their work emphasized the importance of balancing detection accuracy with computational efficiency, a critical consideration for resource-constrained IoT devices. Similarly, [19] reviewed existing security frameworks for IoT, identifying the need for energy-efficient, adaptable IDS solutions capable of operating across diverse IoT environments.

Despite the advancements made, many existing approaches have significant limitations. Ensemble methods, such as Random Forest and Gradient Boosting, have been successfully applied in intrusion detection for IoT, offering high detection rates and robustness against noise. [20] demonstrated that ensemble models could effectively detect Distributed Denial of Service (DDoS) attacks. However, these models often fail to capture the complex temporal patterns of IoT network traffic, limiting their ability to generalize to different attack types. This has prompted a shift toward using deep learning models, such as Multi-Layer Perceptrons (MLPs) and Recurrent Neural Networks (RNNs), which are better suited to model temporal dependencies in network data [21]–[23]. The integration of classical machine learning techniques with deep learning models in hybrid systems has emerged as a promising direction for IoT IDS research [24], [25]. These hybrid models, combining the strengths of both approaches, aim to improve detection accuracy and generalization while remaining computationally efficient. For instance, hybrid models using Voting Classifiers have shown that combining the predictions of multiple algorithms can yield better results than using a single model [26]. By leveraging the strengths of Random Forest, Gradient Boosting, and deep neural networks, hybrid systems offer a more comprehensive solution to the security challenges faced by IoT networks [27].

This research seeks to design and develop an advanced, adaptive intrusion detection system tailored specifically for IoT networks. The goal of our work is to provide a scalable, efficient, and accurate IDS capable of detecting both known and novel cyberattacks. Our hybrid approach combines the strengths of classical machine learning models, such as Random Forest and Gradient Boosting, with deep learning architectures like MLPs, allowing for robust detection across diverse IoT environments. Our key contribution is the development of a hybrid ensemble model that integrates classical and deep learning techniques to enhance intrusion detection capabilities. By applying this model to the RT-IoT2022 dataset, we demonstrate that our system can detect a wide range of attack patterns, including brute-force attacks, DDoS, and Nmap scans, with higher accuracy than traditional methods. The use of a Voting Classifier further improves the overall performance by combining the predictions of multiple models, allowing for more reliable detection in complex network environments.

Additionally, we address the computational challenges posed by real-time IoT environments by optimizing our hybrid model for resource-constrained devices. This ensures that the IDS can operate effectively in real-world IoT scenarios, where computational power and memory are often limited. Our research demonstrates the viability of hybrid models in balancing detection accuracy with computational efficiency, providing a more adaptable and scalable solution for IoT network security. The remainder of this paper is structured as follows. First, we present the materials and methods used in the study, including the RT-IoT2022 dataset, which captures diverse IoT network traffic and attack scenarios. We then describe the preprocessing techniques applied to the

dataset, along with the architecture of our proposed hybrid model. This section also details the classical and deep learning models integrated into our system. Following this, we provide a comprehensive overview of the experimental setup, including the evaluation metrics used to assess the performance of our system.

2. Research Methodology

2.1. Dataset: RT-IoT2022

The RT-IoT2022 dataset is used as the foundation for the proposed intrusion detection system [28]. This dataset simulates real-time interactions within an IoT infrastructure, encompassing both normal and adversarial network behaviors. It integrates data from various IoT devices, including ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp, and simulates attack scenarios such as Brute-Force SSH attacks, Distributed Denial of Service (DDoS) attacks using Hping and Slowloris, and Nmap scanning techniques (TCP, UDP, OS detection, and XMAS tree scan). The RT-IoT2022 dataset provides an extensive and accurate representation of real-world scenarios through bidirectional traffic attributes, captured using the Zeek network monitoring tool alongside the Flowmeter plugin. The dataset comprises features such as packet statistics, flow duration, payload sizes, and network flag counts. These features facilitate a detailed analysis of network traffic patterns and allow the identification of known and emerging attack vectors. Given the dataset's broad range of network behaviors, the classification task becomes multi-class in nature, with classes representing different types of attacks such as DOS_SYN_Hping and NMAP_TCP_SCAN. This diversity makes the RT-IoT2022 dataset particularly well-suited for evaluating the effectiveness of machine learning models in detecting diverse attack types within IoT environments.

2.2. Preprocessing Techniques

To prepare the RT-IoT2022 dataset for use with machine learning algorithms, several preprocessing techniques were applied. The dataset contains both categorical and numerical features, each requiring different treatments. Categorical variables, such as protocol (proto) and service type (service), were transformed using one-hot encoding. This process generated sparse binary vectors representing each category, ensuring compatibility with the learning algorithms without imposing an ordinal relationship between the categorical values. For the numerical features, including flow duration, packet counts, data rates, and flag counts, a standardization technique was applied. Specifically, the standard scaler was used to transform each numerical feature by subtracting the mean and dividing by the standard deviation, resulting in a mean of zero and unit variance for all features. This ensures that all features contribute equally during model training and prevents any feature from disproportionately influencing the learning process. The dataset was then divided into the feature matrix X and the target vector y, where y represents the attack type labels. Label encoding was applied to the target variable to map the categorical attack labels into integer values. Finally, the dataset was split into training and testing sets, with 80% of the data used for training and 20% reserved for testing. This ensures a robust evaluation of the model's generalization capabilities on unseen data.

2.3. Model Architecture

The proposed hybrid model combines classical machine learning algorithms with a deep learning architecture to fully exploit the strengths of both approaches. The hybrid system is comprised of Random Forest (RF), Gradient Boosting (GB), and a Multi-Layer Perceptron (MLP), and their outputs are combined using a Voting Classifier with soft voting. The Random Forest classifier is an ensemble learning

method that constructs multiple decision trees and aggregates their predictions. For a given input x, the predicted class is obtained by $\hat{y} = \arg\max_c \sum_{i=1}^{n} I(h_i(x) = c)$, where $h_i(x)$ represents the prediction of the i-th tree and $I(\cdot)$ is an indicator function. This aggregation reduces variance, mitigating the risk of overfitting, and ensures robust performance on complex datasets.

Gradient Boosting builds models sequentially, where each new model improves upon the errors of its predecessor. The model prediction is constructed as $F(x) = \sum_{m=1}^{M} \nu h_m(x)$, where $h_m(x)$ is the weak learner added at each iteration and ν is the learning rate. This method is highly effective in handling imbalanced datasets and difficult-to-classify instances. The deep learning component of the hybrid system, a Multi-Layer Perceptron, is a fully connected feed-forward neural network. The MLP consists of multiple hidden layers, each applying a non-linear activation function. The forward propagation for each hidden layer can be expressed as $h_1 = f(W_1 x + b_1)$, where $f(\cdot)$ is the ReLU activation function, W_1 and b_1 represent the weight matrix and bias vector, respectively, and x is the input. The final output layer applies the softmax activation function to generate probabilities for the multi-class classification. Dropout layers are used during training to prevent overfitting. The Voting Classifier combines the predictions of the RF, GB, and MLP models using soft voting. The predicted class for a given input x is determined by averaging the predicted class probabilities from each model: $\hat{y} = \arg\max_c \frac{1}{k} \sum_{i=1}^{k} P(M_i(x) = c)$, where M_i is the i-th model and $P(M_i(x) = c)$ represents the predicted probability of class c from model M_i. By leveraging the strengths of each model, the ensemble approach improves overall accuracy and robustness, particularly in detecting rare and complex attack patterns.

2.4. Model Training and Evaluation

Each component of the hybrid model was trained using the preprocessed training data. Random Forest and Gradient Boosting were trained with 100 estimators, and the random state was fixed at 42 to ensure reproducibility. The Multi-Layer Perceptron was trained using the Adam optimizer, with sparse categorical cross-entropy as the loss function. Training was conducted with over 10 epochs with a batch size of 32, and 20% of the training data was reserved for validation. To assess the models, several evaluation metrics have been conducted such as accuracy, precision, recall, and F1 score, which are defined as follows Accuracy $= \frac{TP+TN}{TP+TN+FP+FN}$, Precision $= \frac{TP}{TP+FP}$, Recall $= \frac{TP}{TP+FN}$, F1 Score $= 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision}+\text{Recall}}$ where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives.

The Voting Classifier was evaluated alongside each individual model. By combining the outputs of RF, GB, and MLP, the ensemble consistently outperformed the individual models in terms of detection accuracy, particularly in low-frequency attack types like Nmap scans and Slowloris DDoS. This evaluation demonstrated the hybrid model's effectiveness in detecting a diverse range of attacks while maintaining high performance across varied IoT traffic conditions. This hybrid approach, integrating classical ensemble methods with deep learning in a soft voting scheme, provides a robust and adaptive intrusion detection system. The model's flexibility and scalability ensure its applicability in real-time IoT environments, where security threats evolve continuously, and device constraints impose limitations on computational resources.

3. Results and Discussion

The performance of the proposed hybrid ensemble model was evaluated on the RT-IoT2022 dataset using key metrics, including accuracy, precision, recall, and F1-score as presented in the table 1. The results for each model, namely Random Forest (RF), Gradient Boosting (GB), the Multi-Layer Perceptron (MLP), and the Voting Classifier, are summarized below. These metrics provide a comprehensive evaluation of the models' ability to detect both normal and attack traffic within the IoT network, offering insights into the strengths and limitations of each approach. The Random Forest classifier achieved an accuracy of 0.9978, with corresponding precision, recall, and F1-scores also at 0.9978. These metrics indicate that the Random Forest model effectively captures the relationships between features in the dataset and performs consistently across all attack types. The high precision reflects the model's ability to minimize false positives, which is crucial for reducing unnecessary security alerts in real-world IoT environments. Similarly, the recall score indicates that the Random Forest model effectively identifies a large proportion of true positives, meaning that the majority of attack instances were detected.

The balanced nature of the F1-score, which combines both precision and recall, further highlights the robustness of the Random Forest classifier. This consistency across evaluation metrics demonstrates that the Random Forest model is highly reliable for identifying both common and rare attack types. However, while the model performs well, its decision-tree-based nature could result in increased computational complexity, especially when scaling larger datasets or more complex network traffic. The Gradient Boosting model achieved slightly lower performance compared to Random Forest, with an accuracy of 0.9975 and identical precision, recall, and F1-scores of 0.9975. While these results are marginally lower than those of Random Forest, they still indicate that Gradient Boosting performs exceptionally well on the RT-IoT2022 dataset. The model's strength lies in its iterative approach to minimizing error, which allows it to focus on difficult-to-classify instances. This capability is especially important in detecting rare or stealthy attacks that may not be as prominent in the dataset.

Despite its excellent performance, Gradient Boosting has a slight disadvantage in terms of computational efficiency. The sequential nature of the model's training process, where each new tree corrects the errors of its predecessors, can lead to longer training times compared to Random Forest. However, this trade-off is often acceptable in cases where the model provides superior detection accuracy for difficult cases. In this instance, the performance difference between Random Forest and Gradient Boosting is minimal, and both models demonstrate excellent detection capabilities. The MLP model, representing the deep learning component of the hybrid architecture, achieved an accuracy of 0.9970, with corresponding precision, recall, and F1-scores of 0.9970. Although slightly lower than both Random Forest and Gradient Boosting, the MLP's performance remains competitive. The ability of the MLP to model non-linear relationships and capture complex patterns in the dataset is reflected in these metrics. However, deep learning models, such as MLP, may require more tuning and optimization to reach the same level of performance as classical models like Random Forest or Gradient Boosting.

The MLP's reliance on multiple layers of neurons and the use of dropout layers to prevent overfitting ensures that the model generalizes well to the testing set. The slight reduction in accuracy and other metrics could be attributed to the need for additional training epochs or the inherent challenges of fine-tuning hyperparameters in deep learning models. Nevertheless, the MLP demonstrates that deep learning architectures can effectively handle the complexities of IoT network traffic.

Furthermore, the Voting Classifier, which integrates the predictions of Random Forest, Gradient Boosting, and MLP using soft voting, achieved the highest performance among all models. The accuracy, precision, recall, and F1-score for the Voting Classifier were all 0.9980. This result indicates that the ensemble approach successfully leveraged the strengths of each individual model, resulting in superior detection capabilities across all attack types. The marginal improvement in performance, while small, demonstrates the effectiveness of ensemble learning in reducing the overall error and capturing the strengths of both classical machine learning models and deep learning architectures. The Voting Classifier benefits from the diversity of its constituent models, each of which excels in different areas. Random Forest contributes strong generalization and efficiency, Gradient Boosting provides refined error correction, and MLP captures non-linear relationships in the data. The soft voting mechanism, which averages the predicted probabilities of each model, ensures that the ensemble is both robust and adaptive. By combining multiple models, the Voting Classifier reduces the likelihood of false positives and false negatives, making it highly suitable for real-world IoT environments where the cost of misclassification can be significant.

Table 1. Result Performance

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.9978	0.9978	0.9978	0.9978
Gradient Boosting	0.9975	0.9975	0.9975	0.9975
MLP	0.997	0.997	0.997	0.997
Voting Classifier	**0.998**	**0.998**	**0.998**	**0.998**

The results of the evaluation highlight several important considerations for designing an effective intrusion detection system for IoT networks. First, both classical machine learning models and deep learning architectures can achieve high detection accuracy, with Random Forest, Gradient Boosting, and MLP all performing exceptionally well on the RT-IoT2022 dataset. However, the hybrid approach provided by the Voting Classifier demonstrates that integrating multiple models leads to marginally better performance, particularly in terms of reducing classification errors. The consistent performance across metrics such as precision, recall, and F1-score indicate that the models are not only accurate but also balanced in their detection of both attack and normal traffic. This balance is critical for ensuring that the intrusion detection system performs well in diverse real-world scenarios, where the cost of false positives (false alarms) and false negatives (missed attacks) can vary significantly. The high recall values suggest that the models can detect even low-frequency attack types such as Nmap scans and SSH brute-force attacks. Moreover, the small performance differences between the models demonstrate the potential for trade-offs between complexity and accuracy. Random Forest and Gradient Boosting, as ensemble methods, offer strong performance with moderate computational overhead, while MLP provides a deep learning approach that, while requiring more tuning, still delivers competitive results. The slight advantage of the Voting Classifier suggests that in cases where detection accuracy is critical, an ensemble of models is the best solution.

4. Conclusion

This study presents an advanced hybrid ensemble model for intrusion detection in IoT networks, utilizing a combination of classical machine learning algorithms (Random Forest and Gradient Boosting) and a deep learning architecture (Multi-Layer Perceptron). The model was evaluated on the comprehensive RT-IoT2022 dataset, which contains both normal network traffic and various attack patterns,

providing a robust testbed for assessing the effectiveness of intrusion detection systems. The evaluation results demonstrate that all individual models such as Random Forest, Gradient Boosting, and MLP achieved high accuracy, precision, recall, and F1-scores, indicating their ability to detect a broad range of network intrusions. Random Forest and Gradient Boosting performed slightly better than MLP, but the Voting Classifier, which integrates these models using soft voting, consistently outperformed each individual model, achieving the highest performance with an accuracy, precision, recall, and F1-score of 0.9980. The marginal improvement provided by the Voting Classifier underscores the value of hybrid ensemble approaches in detecting diverse and complex attack patterns in IoT environments.

The results highlight the effectiveness of ensemble learning in balancing the strengths of both classical and deep learning models. By leveraging the complementary strengths of Random Forest, Gradient Boosting, and MLP, the proposed hybrid model provides superior detection accuracy, robustness, and adaptability. This approach addresses the evolving security challenges posed by real-time IoT networks, which require scalable and efficient solutions capable of detecting both frequent and rare attacks. In conclusion, the hybrid ensemble model provides a practical and powerful solution for intrusion detection in IoT networks. Its ability to achieve high performance across various attack types and its adaptability to real-world IoT environments make it a viable option for enhancing network security. Future research could explore the inclusion of more advanced deep learning architectures, further optimize the hybrid model, or investigate real-time deployment scenarios to improve the scalability and efficiency of IoT security systems. This work contributes to the ongoing development of robust, adaptive intrusion detection systems that can protect IoT infrastructure from an increasingly sophisticated landscape of cyber threats.

References

[1] R. S. Jha and P. R. Sahoo, “Internet of things (IoT)--enabler for connecting world,” in *ICT for competitive strategies*, CRC Press, 2020, pp. 1–7.

[2] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, “Evolution of IoT-enabled connectivity and applications in automotive industry: A review,” *Veh. Commun.*, vol. 27, p. 100285, 2021.

[3] O. C. Abikoye *et al.*, “Application of internet of thing and cyber physical system in Industry 4.0 smart manufacturing,” in *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation*, Springer, 2021, pp. 203–217.

[4] M. Umair, M. A. Cheema, O. Cheema, H. Li, and H. Lu, “Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT,” *Sensors*, vol. 21, no. 11, p. 3838, 2021.

[5] R. Chataut, A. Phoummalayvane, and R. Akl, “Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0,” *Sensors*, vol. 23, no. 16, p. 7194, 2023.

[6] A. K. Tyagi, T. F. Fernandez, S. Mishra, and S. Kumari, “Intelligent automation systems at the core of industry 4.0,” in *International conference on intelligent systems design and applications*, 2020, pp. 1–18.

[7] X. Jiang, M. Lora, and S. Chattopadhyay, “An experimental analysis of security vulnerabilities in industrial IoT devices,” *ACM Trans. Internet Technol.*, vol. 20, no. 2, pp. 1–24, 2020.

[8] E. Bout, V. Loscri, and A. Gallais, “How machine learning changes the nature of cyberattacks on IoT networks: A survey,” *IEEE Commun. Surv. \& Tutorials*, vol. 24, no. 1, pp. 248–279, 2021.

[9] R. R. Krishna, A. Priyadarshini, A. V Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, 2021.

[10] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A review on the security of the internet of things: Challenges and solutions," *Wirel. Pers. Commun.*, vol. 119, pp. 2603–2637, 2021.

[11] S. Rizvi, R. J. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet of Things*, vol. 9, p. 100162, 2020.

[12] K. Sathupadi, "Ai-based intrusion detection and ddos mitigation in fog computing: Addressing security threats in decentralized systems," *Sage Sci. Rev. Appl. Mach. Learn.*, vol. 6, no. 11, pp. 44–58, 2023.

[13] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, 2021.

[14] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021.

[15] G. Kornaros, "Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective," *IEEE Access*, vol. 10, pp. 58603–58622, 2022.

[16] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, 2021.

[17] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 9395–9409, 2022.

[18] B. S. Sharmila and R. Nagapadma, "Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset," *Cybersecurity*, vol. 6, no. 1, p. 41, 2023.

[19] M. Elsisi, M. Amer, C.-L. Su, and others, "A comprehensive review of machine learning and IoT solutions for demand side energy management, conservation, and resilient operation," *Energy*, p. 128256, 2023.

[20] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," *Cybersecurity*, vol. 5, no. 1, p. 1, 2022.

[21] K. Lee, M. Eo, E. Jung, Y. Yoon, and W. Rhee, "Short-term traffic prediction with deep neural networks: A survey," *IEEE Access*, vol. 9, pp. 54739–54756, 2021.

[22] J. Zhang, Y. Zeng, and B. Starly, "Recurrent neural networks with long term temporal dependencies in machine tool wear diagnosis and prognosis," *SN Appl. Sci.*, vol. 3, no. 4, p. 442, 2021.

[23] Y. Li *et al.*, "Weather forecasting using ensemble of spatial-temporal attention network and multi-layer perceptron," *Asia-Pacific J. Atmos. Sci.*, vol. 57, pp. 533–546, 2021.

[24] M. A. Khan and Y. Kim, "Deep Learning-Based Hybrid Intelligent Intrusion Detection System.," *Comput. Mater. \& Contin.*, vol. 68, no. 1, 2021.

[25] A. Aldallal, "Toward efficient intrusion detection system using hybrid deep learning approach," *Symmetry (Basel).*, vol. 14, no. 9, p. 1916, 2022.

[26] S. Kumari, D. Kumar, and M. Mittal, "An ensemble approach for classification and prediction of diabetes mellitus using soft voting classifier," *Int. J. Cogn. Comput. Eng.*, vol. 2, pp. 40–46, 2021.

[27] N. Khan, M. I. Mohmand, S. ur Rehman, Z. Ullah, Z. Khan, and W. Boulila, "Advancements in intrusion detection: A lightweight hybrid RNN-RF model," *PLoS One*, vol. 19, no. 6, p. e0299666, 2024.

[28] J. B. Capital, "Real-Time Internet of Things (RT-IoT2022)." 2022. https://archive.ics.uci.edu/dataset/942/rt-iot2022}.