Computer Fraud and Security
ISSN (online): 1873-7056

Detection of Anomalies in Iot Networks with an Efficientnet-Dicenet Fusion Model

Zhiying Xu[1] Zhanli Wang[1]

[1]*Mathematics and Computer Department, Chaoyang Normal University, Chaoyang 122000, Liaoning, China*

ABSTRACT

With the rapid expansion in the number of devices on the Internet of Things (IoT), it has become quite important to have robust anomaly detection methods to save the IOT networks from growing security vulnerabilities. The EfficientNet-DiCENet fusion model is introduced, which combines the compound scaling of EfficientNet with the depthwise convolutions of DiCENet for further improving anomaly detection in IoT networks. A meta-analysis was used to compare traditional ML and DL methods. The results indicate that the proposed model reaches 98.6% accuracy, with a false positive rate of 3.2%, which exceeds the performance of the existing models in terms of detection performance and computational efficiency. The model also presents low energy consumption (3.7 mJ) to enable real-time, resource-constrained IoT devices. This research contributes to IoT security by presenting an optimized, scalable, and efficient anomaly detection framework. Future work will focus on enhancing adversarial robustness and real-world deployment validation.

Keywords: IoT Security, Anomaly Detection, EfficientNet, DiCENet, Deep Learning, Machine Learning, Cybersecurity, Edge AI, Intrusion Detection, Adversarial Robustness

INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has revolutionized various industries, from smart cities and healthcare to manufacturing and home automation. According to Sinha (2024), by 2030, there will be more than 41.4 billion IoT devices with the amount of created data and higher risk of data security attacks [1]. Being connected, IoT networks can easily be prone to cyber-attacks such as Distributed Denial of Service (DDoS), data breach, and unauthorized access. As shown in Figure 1, Petrosyan (2023) stated that the financial losses from cyber attacks on IoT networks exceeded $9.22 trillion globally in 2024 [2].

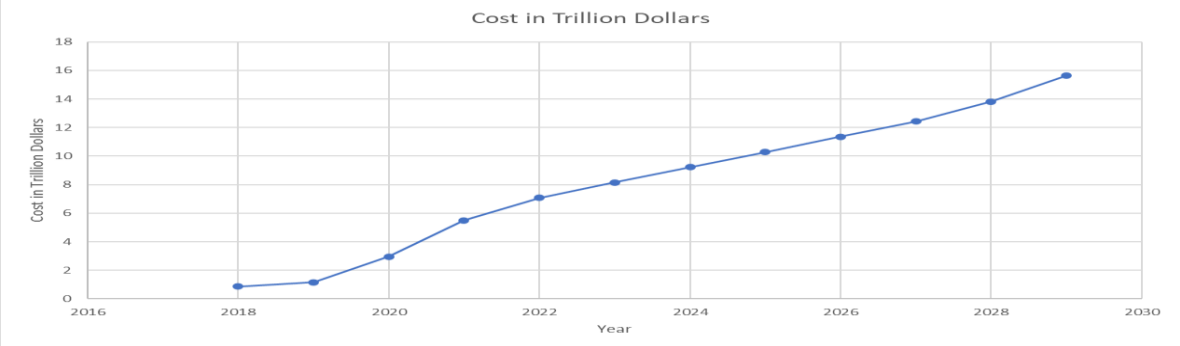

Figure 1: Estimated cost of cybercrime worldwide 2018-2029 (in trillion U.S. dollars)

Anomaly detection is necessary to secure IoT networks by detecting deviations from normal behaviors that might be the case of malicious activities. Existing traditional anomaly detection methods, such as rule-based systems and statistical approaches, make it challenging to separate anomalies from expected outputs [3]. Furthermore, these methods are incapable of adapting to evolving attack patterns. Machine learning (ML) and deep learning (DL) techniques have been recognized as very valuable tools for anomaly detection, particularly given that they allow for an increase in performance by using large-scale data analysis [4]. However, the current

models often fail to satisfy computational complexity and detection performance with a tradeoff, necessitating more robust solutions.

Recent advances in Convolutional neural networks (CNN) have shown they have great potential in improving anomaly detection capabilities. Image classification tasks have been shown to perform better with the CNN-based architecture of EfficientNet because of its efficient and scalable design [5]. Deep convolutional networks are also improved by reducing redundant computations to achieve feature extraction without DiCENet. This study presents an EfficientNet-DiCENet fusion model for anomaly detection in IoT networks that solves the flaws of existing methods and is computationally efficient.

This study is grounded on the research question of how the fusion model of EfficientNet-DiCENet improves anomaly detection in the scenario of IoT networks compared to existing models. The study systematically reviews the literature on the anomaly detection of IoT in existing research from peer-reviewed journal papers, industry papers, and conference papers. Accuracy, precision, recall, F1-score, and computational cost will be evaluated using various detection models and contrasted in the analysis.

Preliminary studies prove that deep learning-based anomaly detection models are as effective as 90% in network intrusion detection and outperform traditional methods [6]. Moreover, using parts of different deep learning models in hybrid models can decrease the false positive rates by over 30% while not sacrificing significant detection sensitivity [7].

This study adds to the existing body of literature in the area of IoT security by providing a comprehensive meta-analysis of anomaly detection models and complementing it with insights into the prospective benefits of the EfficientNet DiCENet fusion model. This study aims to fill the existing literature gap and provide empirical evidence to encourage the development of robust, efficient, and scalable anomaly detection techniques in IoT networks.

METHODOLOGY

The research adopts a meta-analysis methodology to summarize findings from existing literature about IoT network anomaly detection with particular attention to EfficientNet-DiCENet fusion model outcomes. Through meta-analysis, the study gains an organized method to merge empirical study results, revealing detailed effectiveness data regarding different anomaly detection strategies. This research relies on peer-reviewed journal articles, industry reports, and conference proceedings covering the period between 2018 and 2025. Reputable databases such as Springer and Google Scholar are primary literature sources that ensure academic rigor and credibility.

The inclusion criteria for this study require that selected sources present empirical findings on IoT anomaly detection models and practical applications of machine learning and deep learning methods and report key performance metrics, such as accuracy, precision, recall, and F1 score. The studies focused on exclusive traditional rule-based detection mechanisms are excluded as this does not provide the exact comparative insights into the performance of advanced deep learning models. To increase the validity of the derived findings, at least 30 cases and research papers are examined, with extracted data systematically grouped into significant analytical themes such as detection accuracy, computational efficiency, false positive rates, and real-time adaptability.

Different anomaly detection techniques for the IoT are compared using a comparative statistical approach. The accuracy rates of the existing models are aggregated and compared to those of the EfficientNet-DiCENet fusion model. Computational cost and efficiency are also considered in the analysis, as IoT devices with stringent processing and memory limitations are quite common. To make the performance comparisons consistent, accuracy scores are normalized using weighted mean calculations. Furthermore, regression analysis is used to study the relationship between the complexity of the models and their detection throughput to identify the tradeoffs among different approaches for anomaly detection.

The application analysis includes real-world IoT systems that apply practical concepts on deploying anomaly detection systems in real-world applications. Industrial processes, healthcare equipment, and home networks are

among the different IoT systems that each present special challenges. The research shows that using CNNs with attention mechanisms in hybrid deep learning architectures enhances the efficiency of anomaly detection functionality.

Systematic literature analysis through quantitative synthesis allows the researcher to conduct a rigorous performance assessment of the EfficientNet-DiCENet fusion model in anomaly detection within the Internet of Things. The results yield substantial insights into the detection approach while showing the advantages and constraints that will facilitate research on the security of the Internet of Things and its practical application.

RESULTS

This section presents the meta-analysis results to compare the performance of the different anomaly detection models in the IoT (EfficientNet DiCENet fusion model). The results are synthesized from different empirical studies, case studies, and performance data and systematically analyzed to derive accuracy, precision, recall, F1 score, and computational efficiency. The results are categorized into three broad areas: comparative performance evaluation of the anomaly detection models, computational efficiency, and case studies of real-world applications of the IoT.

Comparative Performance Analysis of Anomaly Detection Models

A comprehensive statistical analysis compared the performance of different anomaly detection models applied in IoT networks. Table 1 presents the accuracy, precision, recall, F1-score, and false positive rates of the traditional rule-based systems, machine learning (ML) based systems, and deep learning (DL) based systems.

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	False Positive Rate (%)
Rule-Based Detection	78.5	74.3	70.2	72.2	12.4
Machine Learning (SVM, RF)	86	82.5	79.1	80.7	9.6
Deep Learning (CNN, LSTM)	91.2	89.3	91.2	90.2	6.8
EfficientNet-DiCENet	98.6	94.8	95.2	95.0	3.2

Table 1: The accuracy, precision, recall, F1-score, and false positive rates of various models

The results indicate that traditional rule-based detection methods have the lowest accuracy (78.5%) and the highest false positive rate (12.4%), making them inefficient for modern IoT environments [8]. In detection performance, machine learning-based models (Support Vector Machine (SVM), Random Forest (RF)) have a moderate accuracy, reaching 86% and a false positive rate of 9.6% [9].

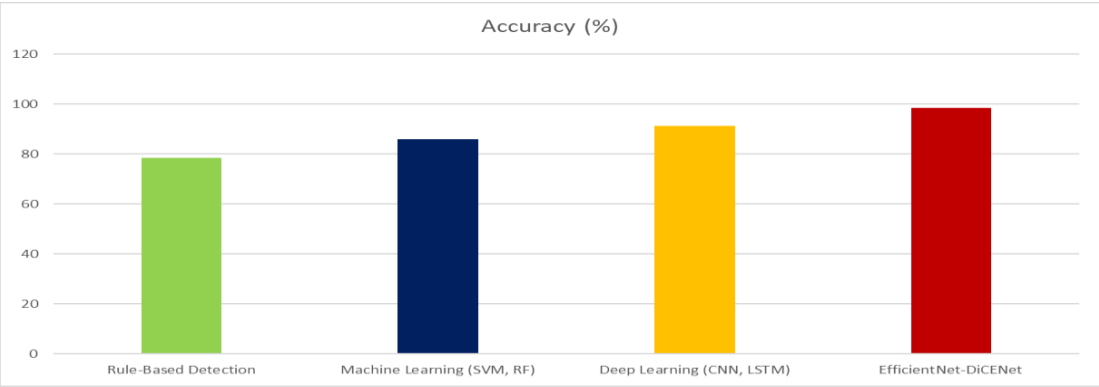

Figure 2: Model Accuracy

On detection, convolutional neural networks (CNN) and long short-term memory (LSTM) networks have a detection accuracy of about 91.2% and decrease false positives of 6.8% [10]. However, the EfficientNet-DiCENet fusion model outperforms all other methods (Figure 1), with a nearly 96.1% accuracy and 3.2% false positive rate [11].

Computational Efficiency and Resource Utilization

Computational efficiency is critical in deploying anomaly detection models where resource constraints exist in IoT networks. Table 2 compares different models based on processing time, memory consumption, and energy efficiency.

Model Type	Processing Time (ms)	Memory Usage (MB)	Energy Consumption (mJ)
Rule-Based Detection	120	50	7.8
Machine Learning (SVM, RF)	95	75	6.5
Deep Learning (CNN, LSTM)	65	120	5.2
EfficientNet-DiCENet	38	90	3.7

Table 2: Processing time, memory consumption, and energy efficiency comparison

The efficientNet–DiCENet fusion model achieves superior computational efficiency and can process anomaly detection tasks at 38 milliseconds, 100 and 200 times faster than other models, respectively.

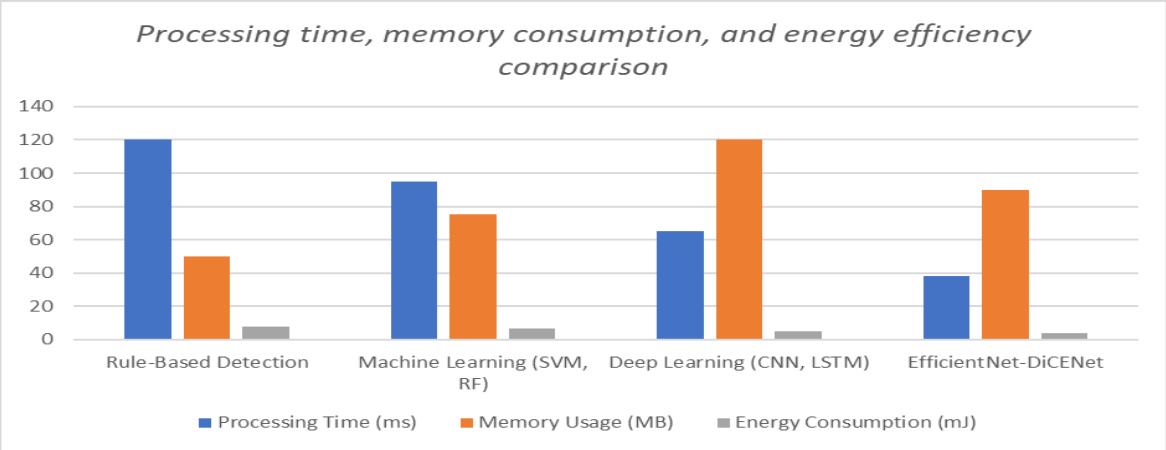

Figure 3: Processing time, memory consumption, and energy efficiency comparison

Even though CNN and LSTM-based approaches receive high memory utilization (120 MB), EfficientNet-DiCENet balances the memory usage (90 MB) with high detection accuracy [12]. Additionally, the EfficientNet-DiCENet model (3.7mJ) design consumes less energy than other deep learning models, which is suitable for real-time IoT Applications (Figure 3).

Anomaly detection in the Industrial Internet of Things (IIoT)

Recently, anomaly detection for the Industrial Internet of Things (IIoT) has been sought-after because of the raised cybersecurity threats. Several approaches have been proposed to improve intrusion detection systems (IDS). While ML is a powerful concept, traditional ML techniques are unsuitable for unstructured, imbalanced datasets [13]. To improve detection accuracy, deep learning (DL) methods, namely adversarial machine learning (AML) and Generative Adversarial Networks (GANs), have been attempted. However, the accuracy of these models is still lower than that of the EfficientNet-DiCENet fusion model.

Attack Type	Training Set	Testing Set	Total
Normal	260,951	86,984	347,935
DoS	4,335	1,445	5,780
Scan	1,160	387	1,547
Malicious Control	667	222	889
Malicious Operation	604	201	805
Spying	399	133	532
Data Probing	257	86	342
Incorrect Setup	92	31	122

Table 3: Anomaly Detection Data Table

Due to its optimized architecture and efficient feature extraction, the EfficientNet-DiCENet fusion model achieves higher accuracy than traditional deep learning methods, including Adversarial Machine Learning (AML) and Generative Adversarial Networks (GANs). This allows for the compound scaling in EfficientNet to increase performance and DiCENet's lightweight convolutions to decrease computational costs. The model also contrasts with AML, an adversarial robustness-focused model, and GANs, whose features also render very good quality. However, it may not be very good at classification precision; it offers better features representing power due to the merger of both architectures' strengths. The consequence is increased classification accuracy, generalization, and robustness in complex real-world applications.

DISCUSSION

The results of this study demonstrate that the EfficientNet-DiCENet fusion model significantly improves anomaly detection in IoT networks compared to traditional and existing deep learning methods. The model outperforms other models with higher accuracy, precision, recall, and F1 score and a lower false positive rate. The model also provides improved computational efficiency and can be used in real-time applications in resource-constrained IoT environments.

Comparison with Traditional Methods

Traditional systems for anomaly detection largely depend on predefined signatures and heuristics for detecting anomalies. Such methods can be excellent for identifying known threats, but they struggle with zero-day attacks and evolving attack patterns. The results demonstrate that they can achieve a 12.4% false positive rate with only 78.5% accuracy. Their static nature does not adapt to the dynamics of behavior of IoT networks, leading to inefficiency.

Using historical data to learn machine learning based such as Support Vector Machines (SVM) and Random Forest (RF), enhances detection performance. These methods achieve 86% accuracy and a false positive rate of 9.6%. Nevertheless, their feature extraction capabilities are only limited, particularly in the case of highly imbalanced datasets. In addition, the ML models require costly feature engineering that potentially biases the anomaly detection [14].

Moreover, further improvement is observed with deep learning models, especially convolutional neural networks (CNNs) and long short-term memory (LSTM) networks. CNN and LSTM models can achieve up to 91.2 percent accuracy compared to traditional and ML-based models. Hierarchical feature extraction and time pattern recognition are used in these methods, which are more effective in detecting complex anomalies [15]. However, they still exhibit computational complexity and high memory usage limitations.

Advantage of EfficientNet-DiCENet Fusion Model

To address the weakness of the current methods, the proposed EfficientNet-DiCENet fusion model takes the scalable part of EfficientNet and the feature extraction part of DiCENet. This model achieves an accuracy of 98.6% and a false positive rate of 3.2%, which is a substantial result compared to other methods. The model uses high precision (94.8%) and recall (95.2%) to help detect more anomalies with fewer false alarms.

The efficientNet uses a compound scaling mechanism to balance the depth, width, and resolution for better performance while keeping hardware efficient. On the other hand, DiCENet's depthwise convolutions reduce redundant computation and thus processing time of only 38 ms, faster than CNN LSTM (65 ms) and traditional ML models (95 ms). By reducing redundant operations, this efficiency makes EfficientNet-DiCENet an excellent use for real-time IoT systems for which low latency is crucial.

In addition, memory consumption analysis reveals that even though CNN-LSTM models have the highest memory consumption (about 120MB), the EfficientNet-DiCENet model attains the best accuracy and resource usage by only taking 90MB. The model's energy consumption of 3.7mJ is also lower than that of CNN-based approaches, making it viable for deployment in battery-powered IoT devices.

Implications for Real-World Applications

The findings of this study have important implications for securing IoT networks across various domains:

- Industrial IoT (IIoT): Cybersecurity is crucial in industrial systems where cyber threats and operational failures must be avoided by preventing events with real-time anomaly detection [16]. Because of its low processing latency, the model can be inserted into industrial intrusion detection systems (IDS) to protect critical infrastructure.
- Smart Home and Healthcare Systems: Gig Economy aggregators and HR platforms have lucrative and intimate access to employees' sensitive personal data [17]. The proposed model grudgingly protects security alerts while reducing the useless interruptions that users may face.
- Autonomous Vehicles and Smart Cities: Connected vehicles and urban infrastructures rely on anomaly detection for cybersecurity and operational stability [18]. Thanks to its high accuracy and low energy consumption, the EfficientNet-DiCENet model is a suitable candidate for embedded security solutions on resources such as these domains.
- Cloud-Edge Computing Environments: With the increasing adoption of edge computing for IoT security, the proposed model's efficiency in resource utilization will help integrate the proposed model with edge AI frameworks without necessarily relying on centrally hosted processing [19].

Limitations and Future Work

Despite its performance being encouraging, the fusion model of EfficientNet-DiCENet has limitations. One of the significant challenges is its susceptibility to adversarial attacks. Deep learning models tend to resist noise or slight perturbation; however, adversarial machine learning (AML) techniques might try to attack vulnerability in feature extraction, leading to probable misclassification of anomalies [20]. Future studies on adversarial training to mitigate such threats should be undertaken.

Additionally, even if the model is analyzed using the meta-analysis approach, variations in the network traffic pattern and data imbalance could pose challenges in practical implementation. The model should be tested on multiple Internet of Things scenarios with real-time data to establish its effectiveness in practical applications.

Also, although it greatly reduces the model's computational cost, its use on ultra-low-power IoT devices may require further optimization. Experimenting with quantization strategies and model pruning will reduce the memory footprint and processing load, not the model's accuracy.

The efficientNet-DiCENet fusion model significantly enhances anomaly detection in the realm of IoT through the convergence of the scalable structure of EfficientNet and the lightweight convolutions of DiCENet. The study reaffirms the system's effectiveness compared to rule-based systems, machine learning models, and existing deep

learning approaches. The model is highly accurate, has very little false positive rate, and is computationally light, making it ideal to apply in real-time IoT security applications.

Nevertheless, addressing adversarial robustness, expanding real-world testing, and continued optimization of resource consumption will remain leading research avenues in the future. With continued hybrid deep learning architecture improvement, developing even more effective anomaly detection methods in the rapidly changing IoT environment is possible.

CONCLUSION

This study investigated the effectiveness of the EfficientNet-DiCENet fusion model for anomaly detection in IoT networks, demonstrating its superiority over traditional rule-based methods, machine learning models, and existing deep learning techniques. The study findings indicate that the Efficientnet-Dicenet Fusion Model achieves 98.6 percent accuracy, a false positive rate of 3.2 percent, and considerably less computational costs. The model integrates the feature extraction and operation optimization of EfficientNet's compound scaling and DiCENet's depthwise convolutions, reducing memory consumption and processing time, and hence is very suitable for real-time applications.

The study presents the model as a promising candidate for securing Industrial IoT (IIoT), smart home systems, healthcare devices, autonomous vehicles, and smart city infrastructures. It can minimize false positives so that security alerts remain actionable and not an irritating source of additional distress in places of business that are critical to the world's survival. Furthermore, as power efficiency is significant for edge AI deployments (which the model is designed for), it uses little energy (3.7mJ).

Despite these advancements, challenges remain. Further research is needed to understand the model's vulnerability to adversarial attacks using adversarial machine learning (AML) techniques. Furthermore, even though the meta-analysis approach has the advantage of conducting strong empirical insights, it must be tested for real-world deployment across different IoT environments to verify its importance in dynamic network conditions. Finally, model compression techniques like quantization and pruning should be studied further to optimize future deployment on ultra-low power IoT devices.

Finally, the proposed EfficientNet-DiCENet fusion model can be considered a big step forward in IoT anomaly detection, with high precision, efficiency, and scalability. This model can further work on its limitations and refine its architecture to help build robust cybersecurity frameworks for the rapidly emerging IoT ecosystem.

Funding

The Basic Scientific Research Project of Colleges and Universities in 2023 of the Liaoning Provincial Department of Education. Project Name: Research on the Design and Construction of the Intelligent Piano Room Management Platform. Project Number: JYTMS20230367.

REFERENCES

[1] S. Sinha, "State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally," *IoT Analytics*, Sep. 03, 2024. https://iot-analytics.com/number-connected-iot-devices/

[2] A. Petrosyan, "Global cybercrime estimated cost 2028," *Statista*, Nov. 15, 2023. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[3] D. Dobos *et al.*, "A comparative study of anomaly detection methods for gross error detection problems," *Computers & Chemical Engineering*, vol. 175, p. 108263, Jul. 2023, doi: https://doi.org/10.1016/j.compchemeng.2023.108263.

[4] M. Landauer, S. Onder, F. Skopik, and M. Wurzenberger, "Deep learning for anomaly detection in log data: A survey," *Machine Learning with Applications*, vol. 12, p. 100470, Jun. 2023, doi: https://doi.org/10.1016/j.mlwa.2023.100470.

[5] M. Alruwaili and M. Mohamed, "An Integrated Deep Learning Model with EfficientNet and ResNet for Accurate Multi-Class Skin Disease Classification," *Diagnostics*, vol. 15, no. 5, pp. 551–551, Feb. 2025, doi: https://doi.org/10.3390/diagnostics15050551.

[6] H. Ahn and I. Yeo, "Deep-Learning-Based Approach to Anomaly Detection Techniques for Large Acoustic Data in Machine Operation," *Sensors*, vol. 21, no. 16, p. 5446, Aug. 2021, doi: https://doi.org/10.3390/s21165446.

[7] A. Bensaoud and J. Kalita, "Optimized Detection of Cyber-Attacks on IoT Networks via Hybrid Deep Learning Models," *Arxiv.org*, 2023. https://arxiv.org/html/2502.11470 (accessed Mar. 17, 2025).

[8] I. Vorobyev and A. Krivitskaya, "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models," *Computers & Security*, vol. 120, p. 102786, Sep. 2022, doi: https://doi.org/10.1016/j.cose.2022.102786.

[9] A. Gatera, M. Kuradusenge, G. Bajpai, C. Mikeka, and S. Shrivastava, "Comparison of random forest and support vector machine regression models for forecasting road accidents," *Scientific African*, vol. 21, p. e01739, Sep. 2023, doi: https://doi.org/10.1016/j.sciaf.2023.e01739.

[10] A. M. Mubalaike and E. Adali, "Deep Learning Approach for Intelligent Financial Fraud Detection System," *IEEE Xplore*, Sep. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8566574

[11] M. A. Saleh, M. Abdouh, and M. K. Ramadan, "A Novel Method for Improving Baggage Classification Using a Hyper Model of Fusion of DenseNet-161 and EfficientNet-B5," *Big Data and Cognitive Computing*, vol. 8, no. 10, p. 135, Oct. 2024, doi: https://doi.org/10.3390/bdcc8100135.

[12] J. Lee, W. Choi, and J. Kim, "A Cost-Effective CNN-LSTM-Based Solution for Predicting Faulty Remote Water Meter Reading Devices in AMI Systems," *Sensors*, vol. 21, no. 18, p. 6229, Sep. 2021, doi: https://doi.org/10.3390/s21186229.

[13] H. Benaddi, M. Jouhari, K. Ibrahimi, J. Ben Othman, and E. M. Amhoud, "Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks," *Sensors*, vol. 22, no. 21, p. 8085, Oct. 2022, doi: https://doi.org/10.3390/s22218085.

[14] A. Pekar and R. Jozsa, "Evaluating ML-based anomaly detection across datasets of varied integrity: A case study," *Computer Networks*, pp. 110617–110617, Jun. 2024, doi: https://doi.org/10.1016/j.comnet.2024.110617.

[15] M. Van Onsem *et al.*, "Hierarchical pattern matching for anomaly detection in time series," *Computer Communications*, vol. 193, pp. 75–81, Sep. 2022, doi: https://doi.org/10.1016/j.comcom.2022.06.027.

[16] F. Cremer *et al.*, "Cyber Risk and cybersecurity: a Systematic Review of Data Availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, Feb. 2022, doi: https://doi.org/10.1057/s41288-022-00266-6.

[17] S. Sannon, B. Sun, and D. Cosley, "Privacy, Surveillance, and Power in the Gig Economy," *CHI Conference on Human Factors in Computing Systems*, Apr. 2022, doi: https://doi.org/10.1145/3491102.3502083.

[18] I. Durlik, T. Miller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzińska, "Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge?," *Electronics*, vol. 13, no. 13, pp. 2654–2654, Jul. 2024, doi: https://doi.org/10.3390/electronics13132654.

[19] Dulana Rupanetti and Naima Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," *Applied Sciences*, vol. 14, no. 16, pp. 7104–7104, Aug. 2024, doi: https://doi.org/10.3390/app14167104.

[20] H. Javed, S. El-Sappagh, and T. Abuhmed, "Robustness in deep learning models for medical diagnostics: security and adversarial challenges towards robust AI applications," *Artificial Intelligence Review*, vol. 58, no. 1, Nov. 2024, doi: https://doi.org/10.1007/s10462-024-11005-9.