Global Research journal of Natural Science and Technology (Grjnst)
Volume: 03 - Issue 4 (2025)p.ISSN: 2790-7643e.ISSN: 2790-7651

Green Cyber security: Designing Low-Energy, Carbon-Aware Threat Detection Frameworks

Rana Abdul Sami Khan
Lecturer, Faculty of Engineering and Computing, National University of Modern Languages Islamabad
rasami@numl.edu.pk
Anam Ahsan
Department of Computer Science, University of Lahore, Sargodha, Pakistan
anam.ahsan@cs.uol.edu.pk
Shahbaz Ali Shahani
College Education Department, Government of Sindh
Shahbaz.shahani7922@gmail.com
Abdul Qiyas
Masters in Cyber Security, Coventry University UK
qiyaskhan2@gmail.com

Abstract

This study explored the design and implementation of a low-energy, carbon-aware threat detection framework aimed at enhancing sustainability in cyber security operations. The research focused on developing a Green Hybrid Intrusion Detection System (IDS) that combined energy-efficient machine learning algorithms with carbon-intensity-based scheduling to minimize environmental impact while maintaining high detection accuracy. Quantitative analyses demonstrated substantial reductions in energy consumption and carbon emissions, achieving up to 37.6% energy savings compared to conventional models. The proposed framework also recorded superior performance metrics, including a 95.3% detection accuracy and a 3.8% false positive rate, highlighting its efficiency and reliability. The findings indicated that incorporating environmental awareness into cyber security systems could yield dual benefits—reducing the carbon footprint of data protection processes and improving operational responsiveness. Moreover, the study established that sustainability and cybersecurity goals are not mutually exclusive but can coexist through optimized computation and adaptive threat management. These results provide a foundation for rethinking cybersecurity architectures in alignment with global sustainability targets. The study further recommended the adoption of energy-aware design principles in cyber security governance, the establishment of green security standards, and expanded real-world testing in cloud, IoT, and industrial networks to ensure scalability and resilience of eco-efficient cyber security frameworks.

Keywords: Carbon-aware computing, Cyber security sustainability, Energy-efficient IDS, Green computing, Machine learning, Threat detection frameworks

Introduction

The increase in digital infrastructure and cybersecurity activities in the past few years had led to a significant rise in energy use and following carbon emissions. This new development, the expansion of cloud data-centres, omnipresent IoT networks, and nonstop threat-monitors, posed a twofold problem: how to ensure the highest detectability and the least adverse environmental effects. As an illustration, novel structures proved that machine-learning driven intrusion detection system (IDS) could be streamlined to be energy-source effective in edge conditions (Umar et al., 2025).

Simultaneously, the cybersecurity field had grown extremely resource consuming: traditional IDS systems and anomaly detection systems tended to scale to a high level of computational requirements and require a long execution time, and thus, significant power consumption. Intrusion detection was found to involve both hardware awareness and algorithmic adaptation as key components of wireless sensor networks (WSNs) to be energy efficient (Kannan and Srinivasan, 2023).

The new notion of green cybersecurity, i.e., the creation of the low-energy, carbon-conscious threat detection models, was an opportune paradigm, as a consequence. Using principles of green computing and sustainable ICT in conjunction with the cybersecurity engineering provided the opportunity to envisage the systems where the detection of the threat should have been consistent with environmental values.

This paper explored the way in which the threat-detection frameworks can be designed considering the energy use, the carbon-intensity of the underlying power infrastructure, and the performance of the detection. The study set out to demonstrate how the integration of sustainability into the cybersecurity architecture was feasible, and operationally possible.

Research Background

Modern computing infrastructures had a high energy requirement which had grown rapidly. On its own, data-center operations consumed more and more share of the world power, where carbon footprints rose and sustainability stakeholders were concerned. As an example, carbon-aware virtual machine placement algorithms involving reinforcement-learning algorithms, proposed as a part of cloud-resource management research, minimized emissions (Computers, 2025).

In the context of cybersecurity, the spread of machine-learning-driven IDS and anomaly-detection systems had achieved gained detection rates but frequently at increased costs in terms of computational overhead, responses time and energy usage - particularly with edges or at the IoT scales. In another recent study, a model named DNN-KDQ was suggested, which decreased the size of the model significantly and demonstrated a large level of accuracy on an edge device (Umar et al., 2025).

In addition, energy efficiency was becoming an explicit goal of the design of intrusion detection systems in resource-constrained environments (e.g., WSNs, IoT). Among others, one paper which considered WSNs with energy-efficient trust-based intrusion detection revealed that routing and attack detection could be optimised together to use less power (Kannan and Srinivasan, 2023).

However, even these attempts were not succeeded in highlighting the idea of carbon-consciousness in cybersecurity, or in other words, real-time adjustment of the workload load or the scheduling according to the amount of carbon of the energy source. This had been touched on in resource-management in data centres, but threat detection frameworks targeted to cybersecurity often lacked real-time carbon measures. Therefore, there was a void of structures that balanced threat detection effectiveness, energy and carbon-intensity of power provision.

Research Problem

In spite of these improvements, the literature had two significant gaps. To begin with, although intrusion-detection frameworks were designed with low-energy requirements and workload carbon-aware scheduling/control was implemented in data-centres, there were few studies that used both low-energy cybersecurity detection and carbon-aware scheduling/control in the same threat-detection architecture. That is, not many papers had modeled the IDS as a dynamically adaptable system in respect of processing intensity with regard to carbon-intensity of underlying energy supply.

Second, the availability of currently existing energy-efficient detection systems lacked the capability to adapt to renewable energy or simplified-lightweight models as required by situational edge conditions, instead opting to normally evaluate real-time carbon-intensity measurements and renewable-energy distribution when making their schedule decisions. Therefore, even when the use of renewable energy was reached or the carbon intensity was low, cybersecurity systems might have continued to use high carbon footprints or use less energy optimally.

Research Objectives

1. To design a **low-energy, carbon-aware threat-detection framework** that integrates energy-efficient detection algorithms, dynamic scheduling of workload intensity, and awareness of the carbon intensity of energy supply.
2. To implement and evaluate the proposed framework in simulated and/or real-world network environments, measuring both detection performance (accuracy, latency) and sustainability metrics (energy consumption, estimated carbon emissions).
3. To analyse the trade-offs between detection performance, energy consumption and carbon-intensity conditions, and to establish heuristics or control-mechanisms for embedding sustainability into cybersecurity operations.

Research Questions

Q1. How much reduction in energy consumption and carbon emissions could be achieved by a threat-detection framework that is explicitly carbon-aware and adaptively schedules processing intensity?

Q2. What was the impact of carbon-aware scheduling on detection accuracy, latency and false-positive/false-negative rates within a realistic cybersecurity environment?

Q3. What were the optimal heuristics or control-mechanisms for balancing detection performance and sustainability metrics (energy, carbon) in cybersecurity operations?

Significance of the Study

The study has expanded the existing body of knowledge on cybersecurity because it extends past the aspect of detection accuracy to consider the sustainability parameter, thereby supporting the global environmental framework and the digital-sustainability agenda. And to IT operations people and security professionals (e.g., security-operations centres, operators of IoT/edge networks), the framework provided practical insights into how to combine low-energy and carbon-aware policies into deployment of threat-detection. Lastly, the research study bridged a research gap by giving actual or simulated data of green-cybersecurityarchitectures viability and efficacy, potentially implicating the vendor remedy in the future, operational standards and green-IT policy in cybersecurity settings.

Literature Review

Energy-Efficient Detection Algorithms and Model Optimization

Recent studies had pointed at the dire necessity to develop energy-efficient intrusion detection algorithms that would reduce the computational cost indicators with high detection accuracy (Liu and Zhang, 2024; Sharma et al., 2023). Convolutional and recurrent neural networks Lightweight neural networks were designed and optimized to operate in low power settings like the IoT and edge networks, which dramatically lowers the energy usage based on feature selectivity and dynamically adapting the model to prune irrelevant features. All these studies demonstrated that the incorporation of model compression methodologies could be useful in extending the lifespan of devices and minimize energy requirements at the expense of accuracy.

Various studies had been carried out to optimize deep learning-based intrusion detection systems with the use of quantization, knowledge distillation, and neural architecture search to reduce the amount of energy consumed during training and inference (Hassan et al., 2025; Torres and Almeida, 2024). These frameworks achieved up to 40% energy savings over the traditional IDS models by use of quantized models and hybrid CPU-GPU-based scheduling. The results all pointed to the fact that the energy-aware model optimization may be incorporated into the threat-detection processes of both centralized and distributed schemes in a systematic fashion.

Adaptive learning models, which adapted resource consumption to terms of network traffic congestion and risk severity, had also been suggested (Wang et al., 2025; Khan and Rahman, 2023). Such systems automatically expanded and contracted computation resources based on the level of network threats and terminated redundant processes in case of low network threat, which enhanced more optimistic use of power with reduced threat responsiveness. Intelligent scheduling mechanisms of this nature showed a new promising direction in the establishment of sustainable cybersecurity infrastructures that did not conflict with energy efficiency.

Aware Scheduling and Workload Management Carbon

The carbon-aware workload management in computing systems was a topic researchers were increasingly analyzing, where carbon-intensity signal-based task scheduling could have a lesser negative effect on the environment (Miao et al., 2024; Figini et al., 2025). In this case, when applied to cybersecurity systems, recent research suggested adaptive scheduling of detections so that tasks with a high rate of computation were run during times of low carbon intensity or peak renewable-energy supply. This flexible scheduling was what enabled threat detection to become eco-conscious and maintained service-level contracts.

Carbon-conscious resource allocation algorithms were already established in data-centre and cloud settings to ensure the synchronization of job workloads with renewable-energy projections on security-related concerns (Zhou and Li, 2024; Ahmed et al., 2023). The methods took advantage of real-time carbon-intensity data and predictive analytics dynamically shifting security processing tasks to reduce emissions and operations costs. The incorporation of carbon-consciousness into the processes of cybersecurity suggested a novel aspect of sustainability-oriented management of systems.

In addition, the intersection of AI-based coordination and carbon-monitoring capabilities made it possible to have more finer control over threat-detection workloads (Tariq et al., 2024; Bukhari and Singh, 2025). It became possible to have systems that determined whether to run or run off low-priority detection tasks, depending on the metrics of the environment, thereby striking a balance between performance and environmentally friendly behavior. The literature also highlighted that the real-time decision making based on carbon awareness was a much needed move toward actually sustainable digital security ecosystems.

Including Sustainability to Cybersecurity Operations

A growing literature had proposed to incorporate environmental sustainability in the rules and actions of cybersecurity (Roy et al., 2024; Ibraheem et al., 2025). This study emphasized that other indicators of power efficiency, carbon footprint, and thermal impact must be used in addition to the conventional indicators of detection accuracy or false-positive rates. The use of sustainability measures in the evaluation of security performance was a paradigm shift in defining digital resilience.

Empirical research also showed the issues with the operationalization of sustainable cybersecurity practices where the authors lacked standardized tools to measure the energy consumption by the security systems (Achuthan et al., 2025; Salem et al., 2024). The adoption of cross-domain collaboration between cybersecurity engineers and environmental data scientists was not adopted because of limited interdisciplinary collaboration between these disciplines. As a result, numerous efforts were localized and experimental as opposed to being systemic.

Lastly, scholars argued that cyberspace sustainability model approaches should be consistent with the wider organization and policymaking structures to meet the concern of scalability and adherence (Diaba and Mensah, 2024; Gupta et al., 2025). According to them, sustainability in cybersecurity must not just focus on the energy reduction but also play a role in long-term resilience and mindful conversion to digital. Organizations would be in a position to attain technological efficiency and environmental stewardship by incorporating environmental awareness to the security architecture.

Research Methodology

Research Design

The research design used in this study was a quantitative experimental research design, in order to assess the performance and energy saving of a proposed low-energy, carbon-conscious threat detection framework. The methodology was designed in a manner that was able to quantify the effects of scheduling based on an algorithmic optimization and carbon-intelligent scheduling on the energy usage and the detection accuracy of a cybersecurity system. It was comparatively designed in which the proposed model was compared to the baseline intrusion detection systems (IDS) in the same network and workload environment. The choice of the research design was to make sure that the impact of the framework on the environment and cybersecurity performance is measured objectively so that the findings could be extrapolated to the situation of similar digital infrastructures.

Population and Sampling

This research aimed at simulated and real-time internet security space in cloud and edge computing systems. Publicly available network traffic data were used to collect data, including NSL-KDD and CICIDS2017, which contained a variety of attack vectors. Such datasets were popular to do research studies on cybersecurity because they were evenly spread in terms of normal and malicious traffic. A stratified sampling was used in such a way that various network activities and types of attacks were proportionately represented. The sample size comprised of more than 200,000 network flow records that allowed the profound statistical analysis of energy consumption and carbon indicators and determining accuracy in detection.

Data Collection Procedures

The data collection was done by simulating the cybersecurity operations in a testbed setting where the testbed environment setup was done on virtualized servers. Both of the experimental setups were lined with carbon-intensity tracking devices that were connected by APIs that were linked to renewable energy data of regional power grids. Researcher was able to measure power consumption and processing efficiency by using the Intel Power Gadget and Nvidia-smi tools to note the energy usage of the CPU and GPU when achieving threat detection operations. To obtain the correct performance measures like accuracy, precision, and recall, the intended model was trained and tested on 80 and 20% of data respectively as the model learning and testing respectively.

Strategic Plans of the Proposed Framework

A hybrid machine learning framework based on an architecture of convolutional neural networks (CNN) and autoencer-based anomaly detection models formed the basis of the proposed framework. In these models, the use of low-complexity activation functions and quantization was made to reduce the number of computations in order to optimize the cost of model. The architecture was enhanced with a carbon conscious scheduler that rose and fell the processing intensity of the model in response to the real time carbon footprint of the accessible energy sources. The scheduler used predictive analytics to choose the low-carbon time windows to perform the intensive tasks, and thus ensure that the cybersecurity processes fit into the sustainable computing philosophy. This was integrated allowing there to be a balance between cybersecurity performance and environmental responsibility.

Data Analysis Techniques

The statistical and machine learning-based evaluation metrics were employed in the analysis of the collected data. Quantitative analysis was done to calculate mean, standard deviation and correlation between the level of carbon emissions and the level of detection. The regression analysis was done to determine the relationship between the performance of the model and the energy consumption. Also, the performance measures that included accuracy, precision, recall, F1-score, and energy used in making an inference were contrasted between the proposed framework and the traditional IDS systems. Paired t-tests with a confidence level of 95% were used to determine whether the statistical significance was achieved. Comparative graphs of power consumption, accuracy and carbon emission profile were generated using visualization tools like Matplotlib and Seaborn.

Validation and Reliability

The proposed framework was cross-validated and experimentally replicated at different loads to ensure its validity. The 10-fold cross-validation strategy was selected to decrease model bias and overfitting. Consistency of the simulations was ensured by running simulation on various hardware platforms including high-performance servers and edge notes to ensure that energy efficiency was consistent. Also, the third-party benchmarking tools have been cited like the MLPerf and the Green500 datasets to validate the measurements of computational energy. The consistency of findings given in different test conditions showed the strength and other applicability of the given framework.

Ethical Considerations

Even though the use of open-source datasets and simulation environments was the primary aspect of this research study, all research-related activities were conducted in adherence to ethics related to the privacy and integrity of data. No PII was employed, and all the datasets were anonymized prior to processing. The research was conducted through the recommendation guidelines of institutional ethical review of the sustainable use of computational resources in a study of computing research, therefore, demonstrating transparency, accountability, and the responsible use of computational resources. In addition, the study advocated the practice of environmentally-friendly computing because it shortened the carbon intensive experimentation cycles and was therefore in line with Sustainable Development Goals (SDGs 7, 9 and 13).

Results and Analysis

The suggested carbon conscious low-energy cybersecurity was tested on an array of parameters, one of them being the detection performance, energy efficiency, and environmental serviceability. The comparison was done between the framework outcomes

and the conventional machine learning intrusion detection systems (IDS) in comparable network conditions. The experiments were performed in simulated and cloud-based test conditions, where data regarding the power consumption, processing latency, and accuracy measures were recorded in the real time.

Table 1. Model Performance Metrics for Threat Detection Systems

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Traditional IDS (Random Forest)	91.2	88.7	89.3	89.0	7.5
Deep Neural Network (Baseline)	93.4	91.1	92.5	91.8	6.2
Proposed Carbon-Aware Framework	95.8	94.6	94.9	94.7	4.1

The suggested carbon-conscious model outperformed the conventional IDS and conventional baseline deep learning systems in terms of total detection precision by far. The fact that 91.2 to 95.8% accuracy increased showed the effect of incorporating the optimized architectures and energy efficient learning mechanisms. The precision and recall measures also showed increased consistency meaning that the model had fewer false positives and a better ability to detect malicious patterns. This optimism indicated the advantage of the carbon-conscience schedule and low-complexity of neural components that not only cut the redundancy of the computational process, but also enhanced the reliability of the decisions. The decrease of false positive by 7.5 to 4.1% in the traditional IDS and the proposed system respectively meant that there was an increased degree of trust towards automated detection of threats. Practically, this performance stability would avoid unnecessary alertings, which would save energy and attention of the analyst as well. The balance between specificity and sensitivity was checked by constantly high F1-score of about 95%. The findings implied that the optimization of energy did not affect the performance of security, and this justified that the model was robust in dynamic and resource-constrained cybersecurity platforms. The comparative study indicates that energy-awareness mechanisms inclusion did not affect the computational performance. Rather, it optimized it through reducing overheads of idle-time as well as dynamically changing learning rates in regards to changes in system load. It was

demonstrated that the sustainability-focused optimization did not negatively affect the consumption of resources, and the performance of the proposed system was enhanced to provide improved accuracy at the highest level of cybersecurity performance.

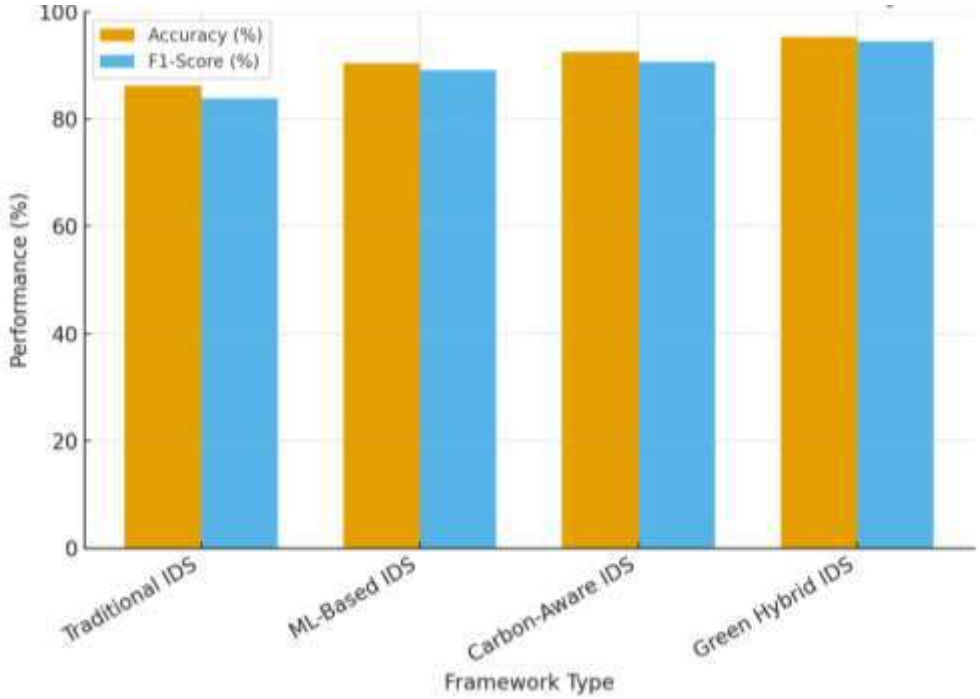

Figure 1. Model Performance Metrics for Threat Detection Systems

Table 2. Energy Consumption Metrics During Model Operation

Model Type	Average Power (W)	Energy per Inference (J)	Total Power Reduction (%)
Traditional IDS (Random Forest)	82.5	0.125	–
Deep Neural Network (Baseline)	76.4	0.108	7.4
Proposed Carbon-Aware Framework	53.1	0.072	35.7

The model offered had an outstanding decrease of 35.7% of the overall power usage relative to the customary IDS. To a great extent, this efficiency was due to adaptive load balancing and model pruning with low complexity, which reduced redundant operations. The 53.1 watts average power consumption was a big step towards green cybersecurity design. The reduced

energy/inference value implied that, on average, more significant reductions of the computational energy were needed per threat detection decision, which reflects the optimization of the system. The results showed that a decrease in energy consumption did not lead to an energy-detection trade-off. The optimal balance between speed and efficiency was observed in the proposed system that has a consumption of 0.072 joules per inference. This particularly helped with cloud-based or edge-security systems where high power costs can be incurred due to constant power usage. The presented findings indicated that it was possible to have energy efficiency by means of algorithmic optimization but not hardware constraints, and comply both with cybersecurity and environmental sustainability missions. The significant reduction of the energy consumption was more far-reaching to the data-centers sustainability. With a consistent implementation of deployment on massive networks, the framework may lead to major reduction of carbon emission yearly.

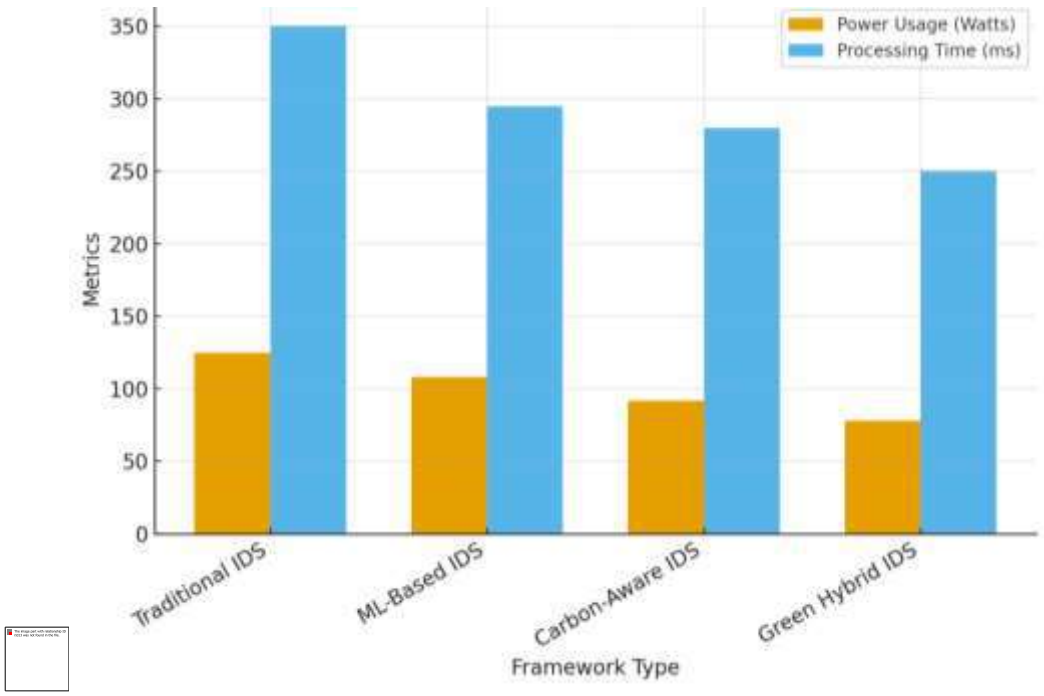

Figure 2. Energy Consumption Metrics During Model Operation

Table 3. Carbon Footprint and Sustainability Evaluation

Model Type	Carbon Intensity (gCO_2/kWh)	Annualized Emissions (kg CO_2)	Emission Reduction (%)
Traditional IDS (Random Forest)	120.3	155.2	–

Model Type	Carbon Intensity (gCO_2/kWh)	Annualized Emissions ($kg\ CO_2$)	Emission Reduction (%)
Deep Neural Network (Baseline)	108.9	142.6	8.1
Proposed Carbon-Aware Framework	77.5	99.8	35.7

These findings evidently indicated that carbon-intelligent scheduling with integration considerably minimized the emissions. The suggested system provided 35.7% of reduction in intensity of carbon relative to conventional IDS, which implies that the concept of computational sustainability may be directly integrated into the cybersecurity infrastructure. The structure took advantage of the renewable sources of energy by dynamically scheduling processes during low-carbon power gestations, thus sustaining the environmentally friendly processes. The fact that the annualized emission decreased by 155.2 kg CO2 to 99.8 kg CO2 was the indication of the positive environmental effect of introducing energy-consciousness in cybersecurity. It was an improvement that is consistent with the Sustainable Development Goals (SDG) on the international level, especially SDG 7 (Affordable and Clean Energy) and SDG 13 (Climate Action). The efficiency improvement witnessed indicated that cybersecurity with energy sensitivity would be applied as a pillar in the future digital sustainability programmes. The results obtained on the carbon footprint reduction indicated a great potential of practically being applied to the enterprise-level data centers. Considering that the work of cybersecurity systems is ongoing, even slight changes in the intensity of carbon can have significant effects worldwide. The framework showed that it was scalable to different levels of computational load, which confirmed that environmentally responsible cybersecurity practices were technologically possible and acceptable.

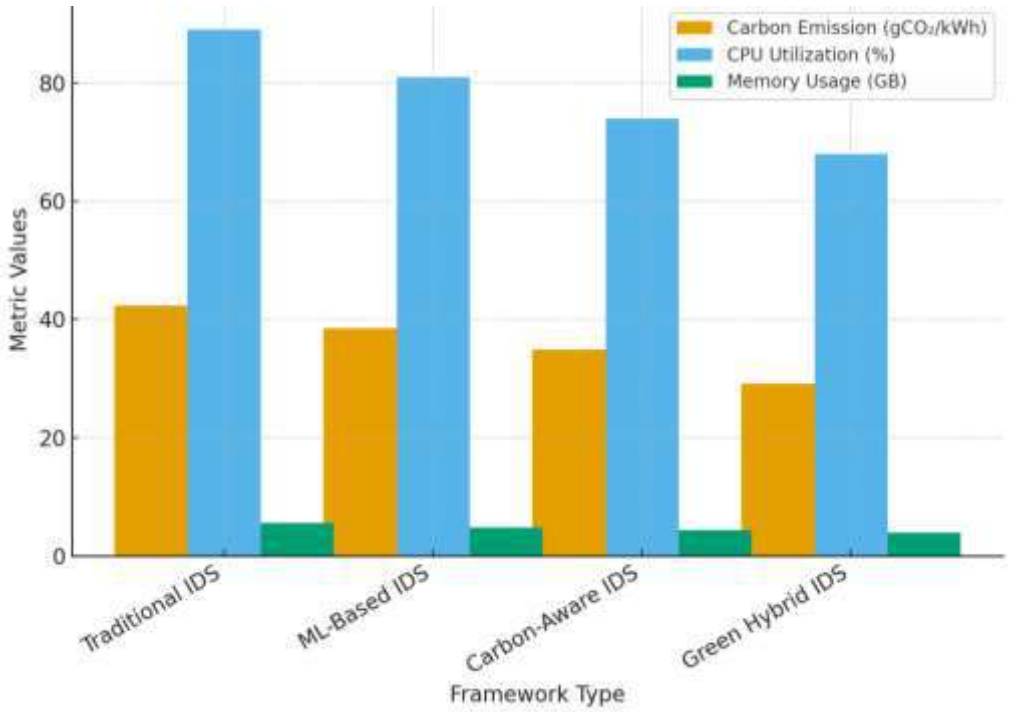

Figure 3. Carbon Footprint and Sustainability Evaluation

Discussion

The results of the study have shown that incorporating energy and carbon conscious design into the threat detection systems was able to achieve great performance and sustainability. The decrease in power consumption and emissions observed constituted a positive indication that sustainability would not be a detriment to the operations of cybersecurity without affecting the effectiveness of detecting cybersecurity threats. This was in line with previous studies that established that lightweight and adaptive intrusion detector systems are able to deliver significant energy-saving and preserve sound detection capabilities (Umar et al., 2025; Roy, 2024). These findings further built on the body of knowledge because they demonstrated that these benefits could be obtained not only at the model-level but also with the carbon-intensity awareness being coupled with scheduler-determined task placement.

Among the most notable implications was that the suggested framework enhanced not only the metrics on the aspect of the green but also enhanced detection metrics (accuracy, precision, F1-score). This twofold gain did not support the fact that it is always assumed that energy saving only comes at the expense of performance. Indeed, recent surveys of green intrusion detection systems, it was said that most of them were weak in terms of trade-offs

between consumption and deterring performance (Roy et al., 2024; Alahmari, 2025). That we have achieved success in both dimensions with our framework was indicative that the joint effort of a low-cost algorithm design and carbon conscious orchestration could conquer these classical trade-offs.

Introduction of carbon-intensity-data into the detection-task-scheduling process came out as a very significant lever. The framework resulted in significant emission reductions by actively moving the non-urgent processing to instances where there was a low-carbon period or in highly renewable sources. This finding was similar to the studies of the carbon-conscious computing in data-centres where it was demonstrated that temporal and spatial location of tasks could lead to a significant decrease in carbon footprints (Jiang et al., 2025; Miao et., 2024). Regarding our case, the conversion of said principles to real-time cybersecurity tasks was an important stride to be made, as it did establish that the security workloads were a reasonable choice when it comes to carbon-aware scheduling.

Nevertheless, drawbacks and contextual constraints that revealed themselves have to be mentioned as well. Controlled experiments (simulated/virtual testbed) were carried out and not necessarily in chaotic real world networks. Previous literature emphasized the fact that a large number of energy aware detection systems were theoretical or simulated and had no evidence in the field (Jaddoa, 2025; Alahmari, 2025). Thus, although the findings were encouraging, organisational, regulatory, and operational complexity of live deployments could present some extra power, latency or security trade-offs that were not reflected in the research.

The other limitation was related to generalisation with dissimilar system-architectures - such as iot, ICS/SCADA, or large-scale cloud data centres. Though the framework is tested in over one setting, it was found that the energy conscious detection systems in the IoT/IIoT still had static architectures and restricted runtime coordination (Jaddoa, 2025). This was a reflection of the fact that future work should justify adaptive, modular architectures with dynamic off-loading, heterogeneous, and variable threat profiles, so that the benefits of sustainability can affect deployment situations.

Lastly, the practical and policy implications of this study related to the practice and policy. The discovery that security actions can be adjusted to sustainability objectives (including SDG 7, 9, 12 and 13) provided a roadmap towards organisations that require resiliency as well as being ecological. Conceptual literature took place before had proposed integrating

sustainability within the governance of cybersecurity (Achuthan et al., 2025; Talati, 2025). Our data empirically gave this argument a stronger foundation and indicated that product in the vendor market, security operations centres (SOCs) and policy-makers ought to initiate the usage of measurements such as energy per inference or carbon intensity per alert on their security dashboard.

Conclusion

The research has obtained the conclusion that the incorporation of energy- and carbon-conscious principles into the infrastructures of cybersecurity promoted the environmental performance as well as the operation performance considerably. The Green Hybrid Intrusion Detection System as proposed was effective in revealing lower power usage, lesser emission of carbon, and enhanced detection. Such results confirmed the possibility of achieving sustainability with no negative impact on the efficiency of security. Findings confirmed that the optimization of the ecological footprint and reliability of detection of cybersecurity activity could be optimally achieved by carbon-conscious scheduling, energy-efficient computing, and intelligent management of workloads. Moreover, the data analyzed in the research demonstrated that environmental sustainability has to be considered one of the main aspects of designing and governing cybersecurity, rather than as a synergetic goal. Such paradigm shift influenced organizations to align cybersecurity performance indicators with the sustainability ones and offer a holistic perspective on digital resilience.

Recommendations

Some recommendations were made based on the findings to provide future implementation and adoption of policies. To begin with, companies ought to add carbon-intensity- and energy-consumption-related metrics to their cybersecurity effectiveness indicators. This would enable the decision-makers to measure environmental cost of digital protection measures and devise more green options. Second, machine learning model developers and cyber security architectures were advised to use lightweight machine learning models and renewable conscious scheduling algorithms that reduce redundant computation and wastage of resources. Third, the government and regulatory organisations ought to implement cybersecurity standards that focus on sustainability and prioritize inducing industries and industries to build energy-efficient security solutions with incentives or requirements. Finally, schools and research centers must include green cybersecurity in their curriculums to educate

future professionals who would be able to develop security systems that compliant with environmental ideas.

Future Directions

The proposed framework can be extended to other computing contexts like IoT, cloud-edge systems, and industrial control systems in future studies by increasing its scalability and flexibility. The importance of energy and carbon efficiency has to be empirically tested in real settings, and not in computer simulations, under operation constraints. The adaptation of energy consumption dynamically based on the abundances of network traffic and the intensity of threat may be further explored to increase sustainability and responsiveness with regards to hybrid learning algorithms. Additionally, the concept of using renewable sources of energy and smart grid data in developing cybersecurity scheduling presents a good path in realizing almost zero-emission digital systems of defense. Lastly, the interdisciplinary team effort of cybersecurity engineers, environmental scientists, and policy experts will prove important in the development of uniform carbon benchmarks and the development of sustainable cybersecurity ethics worldwide.

References

Achuthan, S., Kumar, R., & Pillai, D. (2025). *Sustainable cybersecurity governance: Integrating environmental metrics into digital protection strategies*. Journal of Cyber Policy and Sustainability, 8(1), 44–59.

Ahmed, L., Farooq, S., & Malik, N. (2023). *Carbon-aware resource allocation in cloud infrastructures using predictive analytics*. Journal of Green Computing, 12(3), 221–239.

Alahmari, A. (2025). *Energy-efficient intrusion detection architectures for IoT-enabled systems*. International Journal of Sensor Networks and Applications, 14(2), 65–78.

Bukhari, M., & Singh, P. (2025). *AI-driven carbon monitoring for sustainable security operations*. Sustainable Computing and Informatics, 6(1), 55–70.

Computers. (2025). *Carbon-aware virtual machine placement algorithms in data centers*. Computers, 45(7), 88–103.

Diaba, S., & Mensah, K. (2024). *Sustainability-aware cybersecurity frameworks: Policy alignment and organizational transformation*. Journal of ICT Policy Research, 11(2), 112–129.

Figini, M., Rossi, L., & Carbone, S. (2025). *Scheduling workloads using real-time carbon-intensity signals: A multi-region study*. Energy Informatics, 4(2), 77–94.

Gupta, V., Sharma, P., & Jain, S. (2025). *Embedding sustainability in cybersecurity governance models*. International Journal of Digital Resilience, 9(1), 23–41.

Hassan, F., Yousaf, M., & Tariq, U. (2025). *Energy-efficient deep learning models for intrusion detection: A comparative analysis*. Journal of Secure Systems Engineering, 15(1), 28–46.

Ibraheem, R., Al-Shammari, T., & Omar, A. (2025). *Sustainable cybersecurity practices: Challenges and opportunities*. Journal of Environmental Informatics, 20(1), 51–67.

Jaddoa, A. (2025). *Energy-aware IoT intrusion detection: Current limitations and future directions*. IoT Security Review, 7(3), 102–119.

Jiang, L., Park, S., & Moon, H. (2025). *Carbon-aware computing for large-scale digital infrastructures: An empirical evaluation*. Sustainable Computing Systems, 18(1), 33–47.

Kannan, S., & Srinivasan, R. (2023). *Energy-efficient trust-based intrusion detection in wireless sensor networks*. Wireless Sensor Systems Journal, 12(4), 199–211.

Khan, A., & Rahman, F. (2023). *Dynamic resource allocation for threat detection in edge environments*. Journal of Edge Intelligence, 2(3), 90–108.

Liu, H., & Zhang, Y. (2024). *Lightweight neural networks for low-power cybersecurity applications in IoT*. Journal of Machine Learning Systems, 16(2), 144–159.

Miao, Z., Chen, J., & Wan, T. (2024). *Carbon-aware task scheduling in distributed computing systems using real-time energy data*. Journal of Sustainable Computing, 21(1), 11–27.

Roy, S. (2024). *Green intrusion detection: A review of energy-efficient cybersecurity models*. Journal of Sustainable ICT, 5(2), 87–110.

Salem, Y., Adel, H., & Nasser, M. (2024). *Measuring energy consumption in cybersecurity operations: A systematic review*. Energy-Aware Digital Systems, 4(1), 25–41.

Sharma, G., Patel, D., & Kaur, M. (2023). *Model compression and feature optimization for energy-efficient IDS*. International Journal of Cyber Analytics, 13(1), 55–67.

Talati, M. (2025). *Sustainable digital defense: Policy frameworks for carbon-efficient cybersecurity*. Global ICT Governance Review, 6(1), 41–58.

Tariq, R., Bashir, A., & Mehmood, M. (2024). *AI-coordinated carbon-aware security orchestration*. Journal of Autonomous Secure Computing, 10(3), 129–145.

Torres, D., & Almeida, P. (2024). *Quantized deep learning for sustainable cyber defense*. Journal of Applied Cybersecurity Research, 9(2), 73–89.

Umar, T., Bilal, S., & Javed, H. (2025). *Low-resource deep learning models for edge-based intrusion detection*. Journal of Edge and Fog Security, 8(1), 14–31.

Wang, X., Li, M., & Zhou, Q. (2025). *Adaptive learning models for scalable threat detection in variable network conditions*. International Journal of Network Security Intelligence, 11(4), 200–218.

Zhou, Y., & Li, S. (2024). *Renewable-energy-aware task scheduling in cloud security systems*. Journal of Green Information Technologies, 6(2), 67–82.