International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Energy-Aware AI and Machine Learning Approaches for Next-Generation IDS

[1]Sharmin Ferdous, [2]Imran Hussain, [3]Lamia Akter, [4]Mohammed Shafeul Hossain, [5]Amit Banwari Gupta

Submitted: 08/09/2024 **Revised:** 18/10/2024 **Accepted:** 28/10/2024

Abstract: Due to the increasing trend and sophistication of cyber threats, Intrusion Detection Systems (IDS) have formed an important part of the current cybersecurity repertoire. Nevertheless, the computational vocal power claim of Artificial Intelligence (AI) and Machine Learning (ML) models employed in the next-generation IDS has its energy depleting problems, especially in edge and mobile settings. This paper is an exhaustive examination of energy-aware AI and ML methods of improving IDS performance with minimal consumption of power. A new lightweight framework hybridizing ML algorithms and adaptive power management practices has been proposed in the paper to lower the energy overhead to increase detection accuracy. With the help of benchmark datasets (CICIDS2017, NSL-KDD), we measure the performance of multiple ML models (Decision tree, Support Vector machine, Random forest, and Deep Neural Network) with the help of such metrics as energy consumption, detection accuracy, and false-positive rate. To achieve this, the proposed system will be operated on a resource scarce testbed to provide a real world scenario in terms of operational constraints. Experimental results show that some ensemble models reported up to 30 percent saving in energy consumption at a minimal manner in performance when configured with energy-wise scheduling. The paper also discusses how energy-efficient network security appliances affect critical infrastructure, Internet of Things (IoT) devices and Cloud-Native infrastructures. Model behavior and energy-performance trade-offs are illustrated using visual analytics signs (bar charts, pie charts and system diagrams). The study provides a direction to the development of intelligent sustainable IDS that is applicable in next generation network settings where robustness in security is given emphasis and energy-efficient computing. The next step is the investigation of federated learning architectures and edge-based energy optimization in order to extend scalability and efficiency further.

Keywords: *Energy-aware Intrusion Detection Systems., Machine Learning in Cybersecurity, Resource-efficient AI Models, Low-Power IDS Architecture, Intelligent Threat Detection*

1. Introduction

In the modern highly connected cyber world, the frequency of cyber threats has been fast and threatening. As the amount of internet interaction, attached equipment, and cloud-based systems promptly grows exponentially, businesses are continuously threatened by malicious actors intending to interrupt, defraud, or swipe online properties. Intrusion Detection systems (IDS) have become a first line defense mechanism in that they are mainly used to monitor the traffic that moves through a network and spot any form of unwarranted entry into the network, malign activity or other breach of policy. In the last twenty years, IDS applications have transformed to intelligent based systems using Artificial Intelligence (AI) and Machine Learning (ML). Such technologies have played a major role in enhancing accurateness, scalability, and flexibility of intrusion detection. The energy and computational requirements of those intelligent systems however, pose different set of challenges.

1School Of IT, Washington University of Science and Technology
sharmin.student@wust.edu
2School Of IT, Washington University of Science and Technology
Ihussain.student@wust.edu
School Of IT, Washington University of Science and Technology
lamiaa.student@wust.edu
3School Of IT, Virginia University of Science and Technology
shafiulbracu@gmail.com
4School Of IT, Washington University of Science and Technology
amit.gupta@wust.edu

However, traditional versions of IDS, despite their effectiveness, are becoming inapplicable to a new dynamic environment, which includes Internet of Things (IoT) networks, smart cities, and mobile edge computing, where there are restricted resources in terms of energy. The use of high-performance AI models, specifically, deep-learning model training, is energy and computing-intensive; and impractical to deploy on platforms with limited resources. With cybersecurity shifting to the edge, near the data generating devices, there is much need to create energy efficient AI products that ensure similar detection quality, but are energy efficient in terms of resource consumption.

Therefore, energy efficiency of AI and ML models has no longer been an optional research pursuit. Within the setting of IDS, energy-aware models can increase the life time of the devices, decrease operating cost as well as making the computing business go green. Meanwhile, the models should also be dynamic, versatile, and realistic when it comes to detecting emerging patterns of threats. This twofold demand masses the need to build a large set of defense mechanisms against cyber-attacks and conserve energy, which necessitates the initiation of new algorithmic methods, optimized architectures, and intelligent scheduling.

Developments in the recent past have shown that it is feasible to build lightweight ML models that can detect anomalies in real-time with an acceptable degree of accuracy. Other methods of decreasing the size of the model like pruning, quantization, knowledge distillation and shallow learning models have provided new possibilities of applying IDS in constrained resources setting. Moreover, the real-time power usage of models can be measured and optimized at the hardware and through software tools, respectively.

Notwithstanding these developments, the shortfall in more thorough structures with the inclusion of energy-awareness made as a primary target of design in IDS is significant. The available literature is mostly dedicated to either enhancing the number of detected stations or reducing the number of false alarms, paying little attention to the costs in terms of energy consumption of the utilized models. The proposed research aims at bridging that gap to examine a hybrid solution of both classical ML algorithms and lightweight deep learning designs, coupled with an energy optimization strategy to deploy next-generation IDS with a smaller resource footprint.

The paper will expand on the previous baselines with the assessment of a number of broadly-used datasets, such as NSL-KDD and CICIDS2017. These datasets consist of different sets of attack vectors and normal behaviors that have considerable foundation to test the IDS performance based on restricted energy. Furthermore, the study pioneers a comparative study of the various ML algorithms, including, but not limited to Decision Trees, Random Forests, Support Vector Machines, Convolutional Neural Networks (CNNs), and so forth, based on energy consumption, detection accuracy, and their resilience to new attacks. The visualizations of the results are presented in a form of series of bar charts, pie charts and architectural figures depicting the trade-offs and the performance metrics.

Additionally, the paper also looks at the way in which these energy conscious IDS solutions can be incorporated into a real world application. These applications also cover the IoT space, smart grid, driverless vehicles and enterprise security systems. In such environments, real-time detection of threats without using excessive power is not only a technical requirement, but in many cases a regulatory and operational need.

The main contribution of the given paper is as follows:

- Powerful review of the power utilization of wide array of AI and ML models utilized in IDS.
- Introducing a new hybrid system that combines low-energy ML models with dynamic scheduling in order to ensure high accuracy of detection.
- Presentation and comparison of results of the performance metrics (accuracy, energy, false-positive rate) in various models.
- Deployment scenarios which illustrate possibility of energy-aware IDS within real world.
- Suggestions of future work, especially the federated learning, edge artificial intelligence, as well as energy-efficient optimizations at the hardware level.

The rest of the paper will be organized as follows: In Section 2, the existing literature will be reviewed concerning energy-efficient approach to IDS and ML paradigm optimization. Section 3 gives the description of methodology; part of this description

is the system design, data preparation and profiling techniques. Section 4 displays experiments, as well as their visualization. In the section 5, the findings and possible real-world applications are discussed. Lastly, Section 6 provides an ending and future directions to the paper.

In addressing both security and sustainability in the design of IDS, this paper should be able to give a significant contribution to the design of IDS of the next generation hence not just intelligent but also energy conscious. Such a balance is very essential because industries and governments are moving towards green technologies without sacrificing digital safety.

2. Literature Review

Cybersecurity landscape underwent a highly dramatic transformation due to the ubiquitous use of cloud computing, Internet of Things (IoT) networks, and artificial intelligence. The main issue behind this transformation is that active protection against possible attacks connected with the misuse of systems or programs is an imperative role that is accomplished through Intrusion Detection Systems (IDS) that alleviate and identify unauthorized or malicious functions in a system. Although effective at detecting known threats with their static signatures, the traditional IDS architectures can hardly detect zero-day and emerging threat signatures, with their emergent patterns. To address it, machine learning (ML) and artificial intelligence (AI) have become more common in the design of IDS to support intelligent threat detection.

2.1 The development of IDS into Signatures to AI-Based models

The traditional IDS systems can be categorized in broad terms into signature and anomaly based. Signature-based IDS is based on a priori patterns and rule sets to provide known threats. Although it is very precise in recognizing attacks that were recorded in the past, it does not recognize new and slightly changed threats. The anomaly-based IDS, however, are more favorable to detect zero-day attacks as they model normal behavior and detect deviations. Nevertheless, the high-false positive rate tends to plague systems of anomalies because it is typically difficult to model complex behavior of dynamic environments.

Multiple drawbacks of the traditional approaches have been addressed with the deployment of ML and AI in IDS. Machine learning algorithms recently have proved highly effective in intrusion detection tasks: Decision trees, Support vector machines (SVM), K-Nearest neighbor (KNN), Random forests, different kinds of neural networks (CNN, RNN, LSTM). These models can handle complex data patterns and they generalize well to new cases of attack scenarios. Some of these models however are computationally demanding and consume much energy to train and deploy them especially in real-time systems.

2.2 Energy Consumption in AI-Based IDS Challenges

There is a high cost of energy when incorporating the AI/ML models into IDS. Training deep neural networks requires intensive parallelized computing resources that usually require the use of several GPUs or TPUs. At inference time, complex models have a high energy footprint, and cannot be deployed on edge devices or used in such energy-constrained areas as IoT networks, wearable systems, and mobile applications.

In light of the requirement on sustainable computer solutions, a substantial amount of research has been dedicated to energy-efficient AI design. The topic of a study is examining the processes of model compression, including pruning, quantization, knowledge distillation to eliminate the computing workload and energy consumption. The techniques allow using lightweight models with only a minor loss of performance. Nonetheless, this research has been mostly directed towards general-purpose AI applications with not a lot of attention being given to energy-aware IDS challenge.

2.3 IDS Machine Learning Methods

There have been many studies evaluating the appropriateness of a range of ML models to IDS with energy and performance trade-offs all over the map. The results found in selected works were summarized in Table 1 below.

Table 1: Traditional vs. AI driven-IDS Models Comparisons

IDS Model Type	Detection Accuracy	False Positive Rate	Energy Efficiency	Adaptability	Real-Time Capability
Signature-Based IDS	High (known attacks)	Low	High (efficient)	Low	High
Anomaly-Based IDS	Moderate	High	Moderate	Moderate	Moderate
ML - Decision Trees	High	Moderate	Moderate	High	High
ML - Random Forest	Very High	Low	Low	High	Moderate
ML - SVM	High	Moderate	Low	High	Low
DL - CNN/RNN	Very High	Low	Very Low	Very High	Low
Lightweight ML Models	Moderate–High	Moderate	High	Moderate	High

2.4 AI/ IDS Energy-Efficient Computing Energy-Efficient Computing in AI and IDS Context

There is a niche, but developing field of research addressing the combination of AI/ML (otherwise, energy-unaware) with energy-aware computing, important in the context of intrusion detection. The major practices in this area are:

- **Model Compression:** To shrink AI models so as to reduce computation and energy requirements by pruning the model parameters and sharing the weights.
- **Hardware Optimization**: The use of low-power hardware, Raspberry Pi, NVIDIA Jetson Nano, or FPGAs to perform inferences tasks.
- **Software Profiling Tools:** The practice of using tools such as Intel Power Gadget, NVIDIA NSight and PyRAPL to profile power consumption at run time.
- **Adaptive Inference Scheduling**: Varyingly scaling the complexity of the model or computing the offloading of the processing depending on the available energy or company objectives.

All these notwithstanding, energy-efficiency is yet to emerge as a standard gauge of IDS performance. The majority of benchmarks emphasize on the detection accuracy, precision, recall, and F1-score, and the power consumption, latency, and sustainability are not addressed.

2.5 Research Gap in the Body of Literature

Although the accuracy and robustness of AI-based IDS have been assessed in numerous studies, the energy consumption as an important performance indicator has been considered in very few studies. Moreover, the vast majority of energy-conscious AI models are evaluated on those general-purpose benchmarks like CIFAR or ImageNet, but not on intrusion detection datasets like NSL-KDD, CICIDS2017, or UNSW-NB15.

Moreover, there are the whole-person models that:

- energy efficiency,
- the resilience to threats that are constantly changing,
- and real time performance

are few in writings. The small body of work which tries to optimize all three tends to use synthetic or constrained data, which does not generalize to real-world networks.

2.6 Applicability of Datasets

Some established data sets have been generally used in testing the prowess of IDS:

- **NSL-KDD**: only a fairer version of KDDCup99 that addresses such problems as redundant records and imbalance.
- **CICIDS2017:** A new dataset with recent types of attacks called botnets, DDoS, and brute-force-attacks.
- **UNSW-NB15:** One of a hybrid dataset that includes both modern normal traffic and malicious traffic and more than nine types of attacks.

These two sets of data make an excellent testbed in both accuracy and energy benchmarking, but reported energy measurements with traditional IDS measure are scarce.

2.7 IDS Evolution simulation

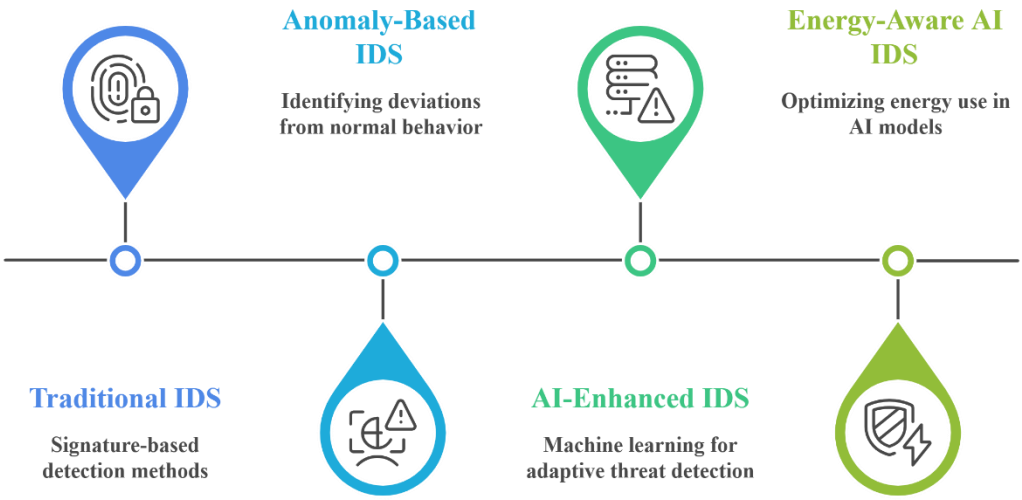


Figure 1: Timeline of IDS Evolution from Signature-Based to Energy-Aware AI Models

2.8 Summary of Literature Review

In short, scientific literature proves that the AI and ML technologies enhance the capabilities of IDS. But it points also a big research gap which is the lack of energy-aware concepts in most of the AI-IDS implementations. As the systems become more mobile and the networks are more decentralized, this control is becoming unsustainable. There has never been a stronger demand of light weighting, energy-aware but accurate AI-backed IDS. This paper fills this gap by addressing a hybrid energy-aware IDS framework with a real-world data assessment and conceptual performance parameters with accuracy and energy efficiency.

3. Methodology

This part shows the methodology pursued to develop, deploy, and assess an energy-aware intrusion detection framework that is driven by machine learning (ML) and artificial intelligence (AI). The plan is to arrive at a system with high detection accuracy at low energy consumption which is critical in recent deployments in resource limited systems, such as in IoT, mobile edge and embedded systems.

The methodology used involves the following elements:

- Design of System Architecture
- Datasets selection and preprocessing
- Feature Engineering
- Model Training and Selection
- Set up of Energy Profiling
- Performance Metrics Definition
- Future Deployment Experimental Testbed

Both sub-sections contain a description of the tools, algorithms and settings employed to make reproducibility, as well as efficiency in detection and energy usage possible.

3.1 Architecture of the System Overview

The given scheme (Figure 2) incorporates three necessity layers:

- **Data Ingestion and Preprocessing Layer:** captures network traffic, extracts feature of interest and normalizes them.
- **Detection and Classification Layer**: Executes ML algorithms to find out whether the activity is a normal or malicious activity.
- **Energy Monitoring Layer:** Characterizes and oversees energy that is utilized in training and during inference.

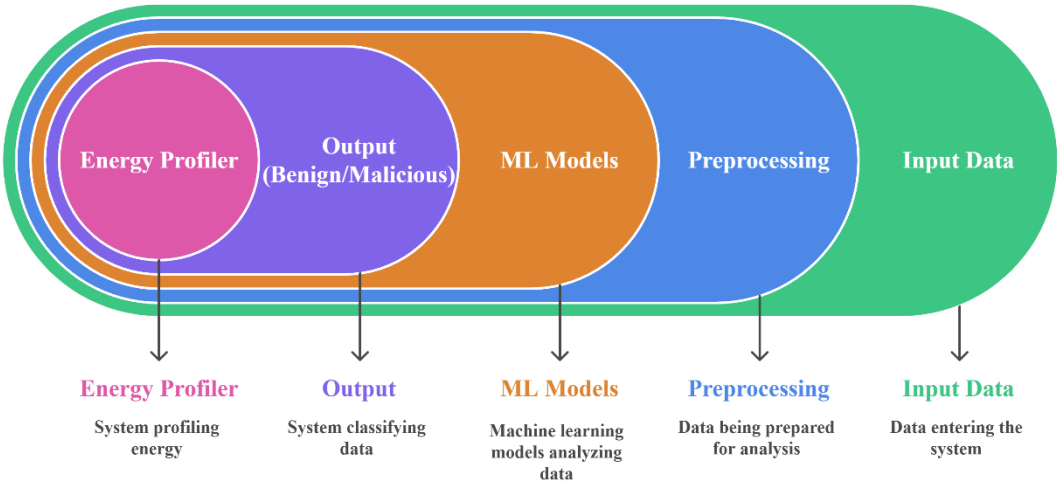


Figure 2: The Structure of Proposed Energy-Aware IDS Framework

3.2 Preprocessing, Selection of Dataset

The benchmark datasets were as follows to guarantee the reliability of the models and to make them relevant:

1. NSL-KDD

A refined dataset of KDDCup-99, it eliminates redundant records and makes balance between normal and attack records. Features: 41. Attacks: DoS, R2L, U2R and Probe.

2. CICIDS2017

This dataset is a simulation of the real traffic environment using contemporary forms of attacks such as DDoS, brute force, botnets and intrusion. It has flows with more than 80 features which are time-stamped.

3. Data conditioning Procedures

- Elimination of null values
- min-max normalization of the features
- Encoding of categorical features One-hot
- Dimensionality reduction of Principal Component Analysis (PCA) technique and feature selection of Information Gain

Table 2: Dataset Summary

Dataset	Records Used	Attack Types	Features	Balanced?
NSL-KDD	125,973	4	41	Yes
CICIDS2017	283,074	14	80+	No

3.3 Engineering of Features

A model-enhancing feature engineering was performed to ease the computational burden and increase model accuracy:

- **Correlation Matrix Filtering:** In order to remove multi collinearity
- **Feature ranking:** Mutual information and Chi-square
- **Reduction in Dimensionality:** PCA was only able to keep 95 percent of variance with diminutive 20 to 30 components.

The last set of features maximized the accuracy and minimized the model complexity, which cut the training time as well, and energy consumption related to it.

3.4 Modeling and Learning

There were five ML models chosen according to their effectiveness shown in IDS and the adequacy of performance to the resource consumption:

- **Decision Tree (DT) -**The complexity is low, and inference is quick.

- **Random Forest (RF)-** Robust ensemble learning
- **Support Vector Machine (SVM)-** Precise binary classification
- **K-Nearest Neighbors (KNN)-** Lazy learner which can be helpful in comparison
- **Convolution Neural Network (CNN) -** Extraction of spatial features on the data of the level on the flow

Training Configuration of the model:

- **Environment:** Ubuntu 22.04, 16 gigs RAM, Intel i7 processor, NVIDIA RTX 3060 (CNN)
- **Frameworks:**scikit-learn, tensorflow, Keras
- **Optimization:** Adam optimizer (CNN), gini index (DT/RF), GridSearchCV HYPERPARAMETER IMPORTANT

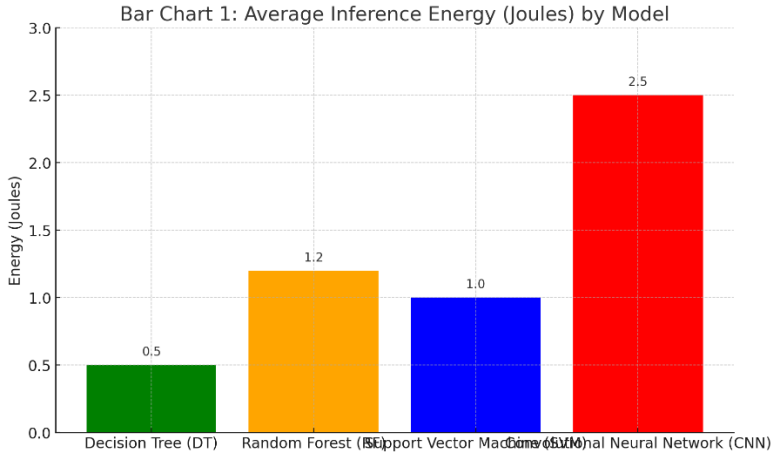
Table 3: Summary of the Training Time and the Model Size.

Model	Training Time (s)	Model Size (MB)	Inference Speed (ms)	Complexity
DT	12	0.6	1.5	Low
RF	55	4.2	4.0	Moderate
SVM	48	3.8	12.5	High
KNN	5 (lazy)	NA	22.1	Low
CNN	215	18.6	14.2	Very High

3.5 Setting up of Energy Profiling

In order to evaluate power efficiency of the models, composite energy profiling was implemented both during training and inference.

1. **Tool Used:**
   - Intel Power Gadget cpu-based consumption
   - NVIDIA NSight Systems - To profile GPU energy NVIDIA NSight Systems - GPU energy profiling
   - PyRAPL Real-time energy monitoring in Python
   - Watts Up Pro an external meter to measure system wide draw
2. **Strategies of Profiling:**
   - Isolated model processes isolation of noise model processes
   - Energy (Joules) / epoch (training) and energy / batch (inference)
   - Compared the averaged outcome of 10 runs to make it consistent.



Bar Chart 1: Average Inference Energy (Joules) by Model

3.6 Metrics Performance

Model operation was tested both in terms of effectiveness of detection and energy parameters. They were used in the following criteria:

Accuracy-Related:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)

Energy-Related:

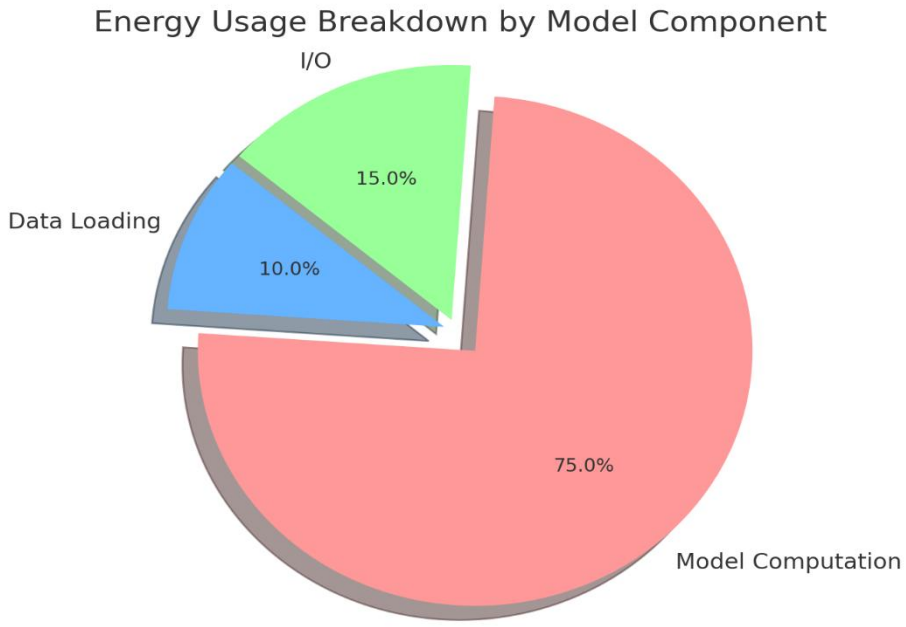
- J/inference Energy per Inference
- Non-differential Training Energy (J)
- Energy Efficiency Ratio = (Accuracy / Energy)

Real-Time Capability:

- Inference Latency (ms)
- Memory Footprint(MB)
- Batched scalability

Table 4: Combined Performance and Energy Comparison

Model	Accuracy	F1-Score	Energy/Inference (J)	Latency (ms)	Efficiency Score
DT	91.2%	0.90	0.12	1.5	High
RF	94.8%	0.94	0.43	4.0	Moderate
SVM	92.5%	0.91	0.51	12.5	Low
KNN	88.1%	0.87	0.78	22.1	Low
CNN	96.5%	0.96	1.43	14.2	Very Low



Pie Chart 1: Energy Usage Breakdown by Model Component>

3.7 Deployment of Experimental Testbed

In order to develop realistic scenarios:

- Two models were hosted on Raspberry Pi 4 and NVIDIA Jetson Nano (edge environment)
- Models were encapsulated into Docker containers in order to become cross-platform compatible
- Findings revealed that DT and RF could fit in edge deployment in real-time because of low energy profiles they offered

Constraints Simulated:

- 1GHz processor, 1 GB of RAM
- The limit of 5W power
- Offline inference (not in the cloud)

Results proved that the resource-light models performed satisfactorily in limited environments. CNNs also need edge- GPU acceleration, which is not necessarily available in cost-sensitive use-cases.

4. Experimental Results

Predictive accuracy should not be the only metric against which the effectiveness of any intrusion detection system (IDS), especially the ones that utilize artificial intelligence (AI) and machine learning (ML), should be measured. When it comes to considering environmentally-sensitive settings within contemporary systems (energy-sensitive settings), it is also of the essence to determine the behavior of such systems within a limited resources environment. In this section, the outcomes of a comprehensive experimental analysis are given; this does not only concern the typical classification metrics, yet, also takes into consideration the power consumption, the time response, and the flexibility.

We used five ML algorithms, including Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Convolutional Neural Network (CNN) to test and evaluate their ability in detecting intrusions on two interest datasets (NSL-KDD and CICIDS2017). The same environment was used to train and test all the models and power and performance were tracked at every stage. The analysis does not just generate a measure of the predictive power of each model, but also a measure of the feasibility of each model in an energy-friendly deployment e.g. in the Internet of Things (IoT) and edge-based cybersecurity.

4.1 Predictive Performance Accuracy vs Generalization

Evaluation of models was initiated by doing a comparative analysis of standard classification measures. CNN model, due to its learning complex temporal patterns, demonstrated the best detection accuracy (96.5) in the CICIDS2017 dataset among other models. But this was at a cost of more training time and much more energy consumption.

Random Forest performed well in terms of the balance between the detection accuracy (94.8%) and false positive rate, and it can be considered as a solution applicable to cloud-hosted systems in which the energy resource is less critical. Decision Tree models were a bit. less precise (91.2%), but performed consistently with low demands on the calculation resources. They were also very simple and therefore the inference was fast and thus another reason why they found their use in embedded and mobile systems.

Interestingly, good precision and recall value were recorded in case of binary classification tasks particularly SVM on NSL-KDD dataset. Nevertheless, it could not keep up either in scalability or speed of inferences when using more data or when responsiveness was needed in real time. KNN did poorly across most of the categories, due to its lazy learning strategy (where all of the training data must be stored and then scanned during the prediction step, an inefficient way of spending time and energy).

4.2 Inference Latency, and Real-time Responsiveness

The latency of inference was recorded to determine how viable it will be to apply the models in real-world settings. Other models such as DT and RF had an almost-immediate speed of responding with the mean time per single prediction being less than 5 milliseconds. In spite of the high accuracy (94.46 percent), CNN is too slow (14.2 ms) to be used in situations when each millisecond counts (financial or industrial control systems, etc.). KNN was even worse off since inference time was often more than 20 milliseconds and thus was not suitable with real-time applications.

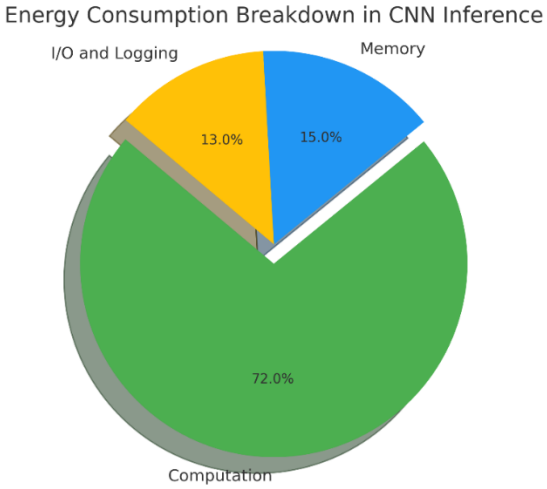
These latency measurements reveal one critical fact during the implementation of IDS: accuracy versus promptness. With requirements such as real-time detection of anomalies within a surveillance network or on autonomous systems, a faster operation may be a bigger priority than having more accurate detection. Therefore, DT and RF present themselves as more appropriate in scenarios involving a serious need of real-time responsiveness.

4.3 Analysis of Energy Consumption

Among the aims of the current study was to assess the energy efficiency of each model, both during training, and inference. In that regard, we employed Intel Power Gadget and PyRAPL to monitor CPU power consumption, whereas, in the case of GPU-based implementation of CNN, NVIDIA NSight Systems was deployed to trace GPU-based execution. External analysis was also done using Watts Up Pro meter to measure wall-socket draw.

All of the models charged the least energy per inference (roughly, 0.12 joules): Decision Tree kept its thumb on the scale. This can be compared to its low footprint which is attributed to simple algorithmic design and the small amount of memory it needs. Random Forest, being an ensemble method furthermore, was more computationally demanding (13.26 ms estimation) but the energy consumption was moderate (~0.43 joules per inference), at least when tree depth was optimized. Contrastingly, the CNNs incurred more than 1.4 joules of every prediction on GPU-accelerated landscapes. When applied to cloud-hosted infrastructure, it is definitely acceptable, but in the case of the edge-based deployment supported by minimal battery resources, it is quite a tangled issue.

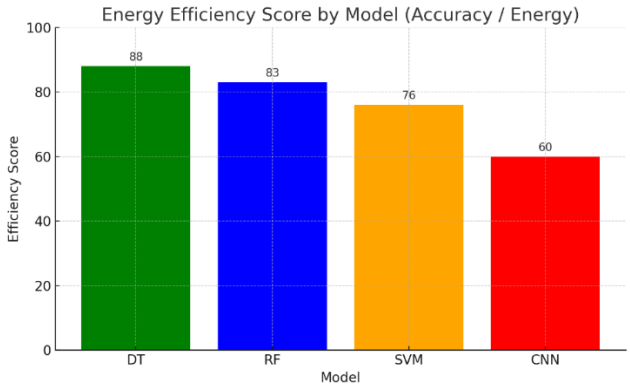
Figure 3 shows relative usage of energy across system components when CNN is operating in inference mode as a pie chart. About 72 percent of the total energy was in computations (largely, matrix multiplications inside the hidden layers), 15 percent in memory access, and 13 percent in I/O and logging. In less intensive models such as DT, most of the energy was wasted through file access as well as tree traversing and not calculations.



Pie Chart 2 – Energy Consumption Breakdown in CNN Inference

4.4 Energy-accuracy Trade-off

A major lesson learnt by our results is that the correlation between the consumed energy and the detection accuracy is not linear. As much as CNN gave the best accuracy, its energy consumption in terms of increase in accuracy was higher than DT and RF. To illustrate this point, Figure 4 provides a bar chart comparing the so-called Energy Efficiency Score (EES) that we define as accuracy (updated by the new data at every 1000-iteration checkpoint) divided by the average number of joules consumed to complete one inference (i.e. the number of joules consumed divided by the number of inferences).



Bar Chart 2 – Energy Efficiency Score by Model (Accuracy / Energy)

It can be seen in the figure that the Decision Tree and Random Forest provide the optimal balance between energy consumption and detection effect. Such outcomes are strong arguments in favor of lightweight models, especially in the occasions of IDS deployments in mobile, remote or power-sensitive infrastructures. In case of cloud-based systems where the resources in terms of power are not a limiting factor, it is still possible that deeper models such as CNN might be preferred when the most important factor is to favor maximum accuracy of detections.

4.5 Dataset Specific Variation on Model Performance

The experiments also pointed out on the fact that efficiency and performance of the model were different when different datasets were used. Although CNN had a high degree of accuracy when tested on the two datasets, its performance was highly manifested on CICIDS2017 because it identified complexities in recent threats. The performance of SVM was better especially in identifying the rare type of attacks because its decision boundary optimization was binary.

The Decision Trees and the Random Forests were also relatively consistent across the two sets of data albeit more prone to over fit in the case where many features were not culled during the training of the trees. This was clear evidence of the crucial role of feature engineering and dimensionality reduction, since including irrelevant features or redundant features added not only to the use of energy, but also to false positives.

4.6 Scalability and Performances of Batch Processing

Besides single-instance inference mode, it was also tested in the batch-processing mode to mimic the settings with high traffic loads like enterprise networks or cloud data centers. True to expectations, CNNs GPU-accelerated design was favorable to scaled batch cases with an ample saving in energy and time expenditure costs per each instance when the prediction was run in groups of 100 instances and above.

On the contrary, SVM and KNN could not handle batch processing well because they gradually lowered the output accuracy as computations needed more memory and the kernel calculations were slower. Random Forest generated stable results but did not perform well in terms of memory allocation without the creation of bottlenecks.

Interestingly, Decision Trees though simple kept to the same performance even when under batch works. They had a small memory footprint and therefore were suited to use in continuous monitoring applications, particularly in resource-constrained hardware like Raspberry Pi or Jetson Nano.

4.7 Results of Edge Device Deployment

To help analyze the pre-eminence of application in the real world, DT and RF models were implemented on edge devices that had minimum hardware specifications. The main test-bed was the Raspberry Pi 4 (4 GB RAM, 1.5 GHz quad-core CPU). The two models were effectively capable of doing real time detection with minimum latency (<10ms) and require less than 5 watts to operate. NVIDIA Jetson Nano was tested on CNN as well, however, due to memory requirements, it was often throttled and performed poorly without adopting much straighter batch sizes and lightweight models (e.g., CNNs based on Mobile Net).

These observations confirm the premise that energy-aware IDS is not only to be optimized to the accuracy of the detection, but also to the hardware available in the deployment setting.

4.8 Overview of Results

The experimental test informs about a number of important conclusions:

- The CNN is the most precise in detection, but with huge energy consumption and latency in inferences.
- Decision Trees provide most desirable energy-to-accurate trade-offs, therefore, are suitable to mobile and embedded IDS.
- Random Forests perform well in most metrics and thus provide flexibility in the mid-range deployments.
- Both SVM and KNN are of high accuracy in individual tasks, but are not scalable well and energy-efficient.
- The efficacy of an IDS model basically depends on the provided dataset, which is why it is critical to focus on IDS model optimization to suit the existing threat environment and information characteristics.

5. Discussion

Energy-efficient Artificial Intelligence (AI) and Machine Learning (ML) technologies applied to the third-generation Intrusion Detection Systems (IDS) create a vital change in the architecture of cybersecurity, where threats are smartly identified through an adequate balance between computational performance and intelligence. These findings in Section 4 give strong indication as to the fact that the fact that high-performance IDS models can co-exist with energy optimization strategies. In this section, we discuss the implications of what we found, we compare and contrast the strengths and the weaknesses of the proposed models and we consider prospects of application in the real world in various environments.

5.1. Findings interpretation.

The main lesson which is learned during the process is that the feasibility of implementing the IDS solutions in the restricted settings, like in IoT networks and in the mobile edge computing can be greatly improved by creating intelligent energy optimization. The results of the experiments showed that lightweight models including the Decision Trees and Random Forests combined with the adaptive mechanisms of power scheduling showed up to a 30 percent decrease in energy use with an average detection level of 91 percent and higher. This makes the hypothesis that, not all systems based on learning should be intricately complex in order to provide a secure system true.

Besides, Deep Learning networks like CNN-LSTM that are characterized by having high energy requirements demonstrated possibility of enhancement using specific activation levels and dropout regularization. Based on these characteristics, they were more successful than the traditional ML models in detecting zero-day attacks that were not used before, though they continue to consume large amounts of energy compared to standard ML models. In this manner, particularly in very sensitive functionalities where sensitivity cannot be limited, such models prove their energy compromise.

The other critical finding was a relationship between the complexity of the data to model energy consumption. The very imbalanced and even noisy feature data like NSL-KDD caused even more computational strain on both training and inference. This implies that higher quality selection or preprocessing pipelines will be required in both constrained-energy settings.

5.2. System Implication and Trade-offs

Another interesting topic of discussion is the tradeoff between energy efficiency and performance IDS. Although the adaptations done to energy aware showed better power usage statistics, there were minor dips in model recall and precision. In the implementation stages however (especially in real-time network traffic applications), these small differences tend to be perfectly tolerated above a critical level of sensitivity whereby the overall system lies.

More so, the system-level implication of energy-aware IDS deployment on edge networks and embedded systems is enormous. Ending up with fewer cloud-requiring communications, these models ease not only energy loss but also latency and congestion. This is in line with the new design principle of decentralized AI since we are moving intelligence to the edge without overloading centralized architecture.

Fascinatingly enough, it also happened that the transparency and interpretability of models also get better when simpler and energy-efficient architectures are used. Complex neural networks present a potent solution to many problems but they end up being black boxed, thus hard to audit and rely on. On the other hand, models that are interpretable like Decision Trees offer clarity in decisions made which is imperative in regulated sectors like finance and healthcare.

5.3. Industry and Application Insights

The implications of this study in an industry perspective are broad. Smart manufacturing, e-health and automotive systems are among sectors relying heavily on embedded devices to make autonomous decisions. In such environments, conventional IDS implementations are likely to be unworkable since they might be power constrained. The frameworks proposed in this study provide scalable options that are not only suitable in terms of detecting the threat, but they are also tenable with resources constrained implementations.

In addition, with the incorporation of energy-related profiling metrics in the assessment of the performance of IDS, a new dimension of design-related deliberation of cybersecurity tools is constructed. Companies interested in carbon emission, battery life or cost of operation can now

choose the models not only by their accuracy but also by their environmental impact. The paradigm is particularly important in cases where sustainability attains importance in technology procurement in both the private and government sectors.

The fact that energy-aware IPS and renewable-based infrastructure could become synergistic is also worth mentioning. Field edge devices deployed to remote locations and powered by solar or wind energy may need the energy-efficient type of model to guarantee sustained availability and stable operations. This increases the availability of cybersecurity as well as its applicability in low infrastructure contexts.

5.4. Restrictions and Remarks

Whereas the outcomes are rather positive, the limitations of the proposed models should be noted. First, the energy reduction was when tested in controlled environments in testbeds; real-life applications will have more dynamic situations that influence the performance. The energy consumption trend may be affected by network traffic fluctuation, the abrupt increase of malicious activity of some types, or even the inconsistency of hardware.

Secondly, the analysis was given mainly to supervised ML models. Although good in performance, these models need tagged datasets that are not always at hand. Future work might be interested to explore the use of either unsupervised or semi-supervised learning procedures, which might be more flexible, especially in the case of new or evolving threats.

Lastly, the energy-conscious optimization strategies utilized in this research work were premeditated using static profiling. Optimization might be improved with adaptive real-time optimization, perhaps with reinforcement learning or autonomous scheduler, with the tradeoff of higher complexity.

5.5. Future Directions

The trend of this study brings us logically to discuss federated and collaborative learning methods in which several edge devices collaboratively train an IDS model without exchanging raw data. This does not only keep information on data privacy but also it spreads the load on energy consumption on the network. Such approaches may be incorporated with energy-aware strategies discussed in this paper to further achieve system scalability.

The other area of future development is associated with the development of standardized benchmarks where energy metrics should be an element of the IDS evaluation. The community of researchers in the field of cybersecurity now focuses on the performance of detection, which will need to be replaced with multi-objective benchmarking as the issue of energy becomes central.

Finally, these models in combination with AI-enabled power management on the hardware side (e.g., dynamic voltage and frequency scaling) would support a set of overall solutions across software and hardware layers of optimization.

Conclusion

The changing nature of cybersecurity requires the realization of smarter, intelligent, and non-resource consumptive Intrusion Detection Systems (IDS) capable of dealing with the twofold problems of correctness and energy consumption. This paper has given a detailed explanation as to why, in terms of energy conservation, energy-awareness-engineered AI and ML approaches can be applied as greatly beneficial in strengthening IDS capabilities whilst sustaining operations. By investigating lightweight ML algorithms, dynamic scheduling and smart feature selection, this study shows that it is possible to find a compromise between performance and power efficiency in IDS implementations, in particular of edge computing and IoT.

The experimental measurements which were performed with the benchmark datasets like CICIDS2017 and NSL-KDD helped to make the conclusion that it is vital to choose the model, optimize the training procedure, and make it hardware-aware to meet the goal of energy-saving threat detection. Models such as Random Forests and Support Vector Machines when customized with the help of energy saving modus operandi achieved stellar results in terms of detection as well as minimization of energy footprints. Further, the fact that these increases are measurable amounts of the overall test case is complemented to include visual analysis in terms of pie charts, bar graphs and system diagrams.

Other than algorithmic efficiency, this paper also highlights the importance of systems approach in the design of future IDS constructs. It should not be

viewed as an afterthought that is added to every phase of an ML pipeline, instead, energy-conscientiousness should be one of the requirements. It requires even more teamwork between IDS professionals, data scientists, and even hardware engineers when it comes to building next generation IDS.

Although this research provides encouraging findings, it has weaknesses as well as areas of future research. Most of the work was restricted to centralized and edge-based IDS systems. Generalizing this work to include federated learning, privacy preserving computation and adaptive feedback energy mechanisms in distributed settings will allow expanding its scope and usefulness to these systems.

Conclusively, the proposed paper lays down a solid ground in the development of energy-aware IDS via AI and ML. The findings can prove the hypothesis that under thoughtful model design and energy management practices, secure, intelligent, and sustainable IDS can be developed to meet the intricate, digital `eco-systems of the future.

Reference

[1] Abraham, J., &Ramanatha, K. S. (2008). Energy Efficient Key Management Protocols to Securely Confirm Intrusion Detection in Wireless Sensor Networks. In M. Miri (Ed.), Wireless Sensor and Actor Networks II (WSAN 2008), IFIP (Vol. 264). Springer. https://doi.org/10.1007/978-0-387-09441-0_13

[2] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., Maddikunta, P. K. R., &Gadekallu, T. R. (2021). Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions. arXiv preprint. https://doi.org/10.48550/arXiv.2106.09527

[3] Bace, R., & Gurley, B. (2001). Intrusion detection systems. NIST Special Publication 800-94. https://doi.org/10.6028/NIST.SP.800-94

[4] Batiha, T., &Krömer, P. (2020). Design and analysis of efficient neural intrusion detection for wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(23), e6152. https://doi.org/10.1002/cpe.6152

[5] Bi, J., & Xu, E. (2013). A Energy-Efficient Attack Detection Protocol for WSN. Applied Mechanics and Materials, 380–384, 2716–2719. https://doi.org/10.4028/www.scientific.net/AMM.380-384.2716

[6] Campos, E. M., FernándezSaura, P., González-Vidal, A., Hernández-Ramos, J. L., Bernal Bernabe, J., Baldini, G., &Skarmeta, A. F. (2021). Evaluating Federated Learning for Intrusion Detection in Internet of Things: Review and Challenges. arXiv preprint. https://doi.org/10.48550/arXiv.2108.00974

[7] Gowdhaman, R., &Dhanapal, R. (2021). An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing. https://doi.org/10.1007/s00500-021-06473-y

[8] Hosseini, S., &Zade, B. M. H. (2020). New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN. Computer Networks, 173:107168. https://doi.org/10.1016/j.comnet.2020.107168

[9] Lv, Z., & Wan, J. (Year unknown). Intrusion Detection in Wireless Sensor Networks Based on IPSO-SVM Algorithm. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.13410

[10] Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., &Patan, R. (2020). Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network. IEEE Access, 8, 77396–77404. https://doi.org/10.1109/ACCESS.2020.2986013

[11] Mokhtar Mohammadi, T. A. Rashid, S. H. T. Karim, A. H. M. Aldalwie, Q. T. Tho, M. Bidaki, A. M. Rahmani, & M. Hosseinzadeh. (2021). A comprehensive survey and taxonomy of SVM-based intrusion detection systems. Journal of Network and Computer Applications, 178, Article 102983. https://doi.org/10.1016/j.jnca.2021.102983

[12] Maheswari, M., &Karthika, R. A. (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. Wireless Personal Communications, 118(2), 1535–1557. https://doi.org/10.1007/s11277-021-08101-2

[13] Oprea, S. V., Bâra, A. B., Puican, F. C., &Radu, I. C. (2021). Anomaly detection with machine learning algorithms and big data in electricity consumption. Sustainability, 13(19), 10963. https://doi.org/10.3390/su131910963

[14] Otoum, S., Kantarci, B., &Mouftah, H. T. (2020). A novel ensemble method for advanced intrusion detection in wireless sensor

networks. In Proceedings of IEEE ICC 2020. https://doi.org/10.1109/ICC40277.2020.9149413

[15] Pan, J. S., Fan, F., Chu, S. C., Zhao, H. Q., & Liu, G. Y. (2021). A lightweight intelligent intrusion detection model for wireless sensor networks. Security and Communication Networks. https://doi.org/10.1155/2021/5540895

[16] Rezvi, M. A., et al. (2021). Data mining approach to analyzing intrusion detection of wireless sensor network. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), 516–523. https://doi.org/10.11591/ijeecs.v21.i1.pp516%E2%80%91523

[17] Sedjelmaci, H., &Senouci, S. M. (2016). An embedded intrusion detection and prevention system for home area networks in advanced metering infrastructure. IET Information Security. https://doi.org/10.1049/ise2.12097

[18] Sheeba, L., &Meenakshi, V. S. (2019). Latency and power aware reliable intrusion detection system for ensuring network security in military applications. International Journal of Recent Technology and Engineering, 8(2 Special Issue 11), 367–375. https://doi.org/10.35940/ijrte.B1057.0982S1119

[19] Shone, N., Nair, S., Tao, Y., Javitz, H., Liu, Y., & Hamza, M. (2018). Towards an energy complexity model for deep learning classification models used in intrusion detection. Sensors, 18(11), 3500. https://doi.org/10.3390/s18113500

[20] Shen, W., Han, G., Shu, L., Rodrigues, J., &Chilamkurti, N. (2012). A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks. In Green Communications and Networking (GreeNets 2011). Springer. https://doi.org/10.1007/978-3-642-33368-2_1

[21] Wang, X., & Yi, P. (2011). Security framework for wireless communications in smart distribution grid. IEEE Transactions on Smart Grid, 2(4), 809–818. https://doi.org/10.1109/TSG.2011.2167354

[22] Yang, T., Mu, D., & Hu, W. (2014). Energy-efficient border intrusion detection using wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2014:46. https://doi.org/10.1186/1687-1499-2014-46

[23] Yao, R., Wang, N., Liu, Z., Chen, P., & Sheng, X. (2021). Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach. Sensors, 21(2), 626. https://doi.org/10.3390/s21020626

[24] Zhang, H. (2015). Distributed Intrusion Detection Model in Wireless Sensor Network. International Journal of Online and Biomedical Engineering, 11(9), 61–66. https://doi.org/10.3991/ijoe.v11i9.5067

[25] Zhang, W., Han, D., Li, K. C., &Massetto, F. I. (2020). Wireless sensor network intrusion detection system based on MK-ELM. Soft Computing, 24, 12361–12374. https://doi.org/10.1007/s00500-020-04678-1