Data-Driven Intrusion Detection and Energy-Aware Security Analytics for Smart Energy Storage and Conversion Systems

Oise Godfrey Perfectson
Department of Computing,
Wellspring University, Edo State, Nigeria
https://orcid.org/0009-0006-4393-7874

ABSTRACT
The digitalization of smart energy storage and conversion systems enhances efficiency and renewable integration but increases vulnerability to cyberattacks. Conventional cybersecurity measures often fall short in these complex cyber-physical environments, and typical data-driven intrusion detection systems (IDS) prioritize accuracy over energy efficiency and system sustainability. This study proposes an energy-aware, data-driven IDS framework that jointly addresses cybersecurity performance, computational efficiency, and operational stability. Using multivariate time-series data from a battery energy storage system, the framework combines feature engineering with energy-efficient machine learning design. A Random Forest–based IDS is developed and evaluated with standard classification metrics and energy-aware indicators, including detection latency and computational overhead. Experimental results demonstrate strong performance, achieving 93% accuracy, 0.87 AUC, and 0.9964 specificity, with low latency suitable for real-time deployment. Metrics such as the Matthews Correlation Coefficient and Cohen's Kappa confirm reliable and balanced classification. The framework also evaluates the impact of cyberattacks on energy efficiency and system stability, demonstrating that robust cybersecurity can be achieved without high computational or energy costs. This holistic, energy-aware approach supports secure, resilient, and sustainable operation of next-generation smart energy infrastructures

Keywords
Intrusion Detection Systems, Smart Energy Storage Systems, Cybersecurity in Energy Systems, Data-Driven Security, Energy-Efficient Machine Learning.

1. INTRODUCTION
The global transition toward sustainable energy systems has accelerated the deployment of smart energy storage and conversion technologies, including battery management systems (BMS), smart inverters, and microgrid controllers [1]. These systems play a critical role in enabling renewable energy integration, improving energy efficiency, and supporting low-carbon power infrastructures. By relying on advanced sensing, communication, and control mechanisms, smart energy systems optimize energy flow and enhance operational reliability, thereby contributing directly to sustainable living for humans [2]. However, the increasing digitalization and connectivity of energy storage and conversion systems have also expanded their cyberattack surface. Modern smart energy infrastructures depend on continuous electronic information exchange among sensors, controllers, and communication networks, making them vulnerable to cyber threats such as false data injection, command manipulation, denial-of-service attacks [3], and replay attacks. Successful cyber intrusions can disrupt control logic, degrade energy efficiency, damage physical components, and compromise system stability, posing serious risks to both energy sustainability and public safety [4]. Traditional cybersecurity mechanisms for industrial control systems have primarily focused on rule-based detection and signature-driven approaches. While effective against known threats, these techniques struggle to detect novel and evolving attacks in complex smart energy environments [5]. In response, data-driven and machine learning–based intrusion detection systems (IDS) have emerged as promising solutions due to their ability to learn patterns from large volumes of operational and network data. Such approaches align with recent advances in artificial intelligence and electronic information systems, offering adaptive and scalable cybersecurity capabilities [6]. Despite these advances, existing data-driven intrusion detection methods largely prioritize detection accuracy while overlooking a critical factor in sustainable energy systems: energy efficiency. Machine learning models with high computational complexity may introduce significant processing overhead, increase energy consumption, and negatively affect real-time control performance [7]. In energy storage and conversion systems, where efficiency and stability are paramount, security mechanisms that impose high computational costs can inadvertently undermine the very sustainability goals they aim to protect [8].

Moreover, the system-level impact of cyberattacks on energy efficiency and operational stability remains insufficiently explored. While prior studies often report detection metrics such as accuracy and false alarm rates, fewer works quantitatively analyze how cyber intrusions affect energy losses, power quality, and system dynamics[9]. This lack of holistic evaluation limits the practical deployment of intrusion detection solutions in real-world smart energy infrastructures. Motivated by these challenges, this research investigates data-driven intrusion detection for energy-efficient smart energy storage and conversion systems. The study aims to develop machine learning–based cybersecurity models that not only achieve high detection performance but also explicitly account for computational overhead, energy consumption, and system stability [10]. By jointly analyzing cybersecurity effectiveness and energy efficiency, this work seeks to advance sustainable, resilient, and intelligent energy infrastructures aligned with the interdisciplinary vision of Electron. The increasing digitalization of smart energy storage and conversion infrastructures has created a dual challenge: ensuring robust cybersecurity while preserving computational and energy efficiency within embedded electronic control environments [11], [12]. Conventional intrusion detection mechanisms often

emphasize detection accuracy without adequately addressing processing overhead, energy consumption, and real-time operational stability. This imbalance is particularly critical in battery management systems, smart inverters, and microgrid controllers, where excessive computational load can degrade system efficiency and reliability. Motivated by these challenges, this research proposes an energy-aware, data-driven intrusion detection framework that jointly optimizes anomaly detection performance, electronic system stability, and computational efficiency. The study integrates machine-learning–based analytics with feature-efficient signal processing and system-level evaluation metrics to support sustainable and secure smart-energy electronics. The subsequent sections present the architecture, modelling formulation, and evaluation methodology that collectively establish a practical pathway for intelligent, low-power cyber-physical protection in next-generation energy infrastructures.

2. LITERATURE REVIEW

Smart energy storage and conversion systems, such as battery management systems, smart inverters, and microgrid controllers, form the foundation of modern renewable energy infrastructures. These systems depend on continuous sensing, communication, and control to regulate energy flow, enhance efficiency, and ensure operational stability. The growing integration of renewable energy sources, including solar and wind, has intensified the reliance on data-driven decision-making, making accurate and timely electronic information essential for system performance. Recent research highlights the importance of intelligent monitoring and predictive analytics in sustaining system efficiency and reliability. Data-driven models have been widely applied to predict battery degradation, optimize inverter operations, and coordinate load balancing across microgrids [13], [14]. While these approaches demonstrate clear benefits in improving energy efficiency and system performance, the cybersecurity vulnerabilities introduced by increased interconnectivity and digitalization remain insufficiently addressed.

The expanded connectivity of smart energy systems exposes them to a wide range of cyber threats that can compromise both operational reliability and energy efficiency. Common attack vectors include false data injection attacks that manipulate sensor measurements, command manipulation attacks that alter actuator control signals, and denial-of-service or replay attacks that disrupt communication networks [15]. Such attacks can degrade control accuracy, destabilize system operation, and lead to inefficient or unsafe energy utilization. Conventional cybersecurity mechanisms, including signature-based intrusion detection, are often inadequate for protecting smart energy infrastructures. These methods struggle to detect previously unseen or adaptive attacks and lack the flexibility required for dynamic, data-rich cyber-physical environments. As a result, there is growing concern about the resilience of energy storage and conversion systems against sophisticated cyber threats. [16]The Internet of Things (IoT) uses sensors and Internet connectivity to collect and exchange data, enabling monitoring and management in areas such as energy systems, healthcare, and security. While IoT technologies have significantly improved efficiency and convenience, they also introduce major challenges related to energy consumption and security. Many IoT devices operate with limited power resources and are vulnerable to security and privacy threats. Therefore, developing energy-efficient and secure IoT solutions is essential. This study reviews existing energy-aware security mechanisms for IoT systems, discussing key challenges, current energy-saving and privacy-preserving approaches, and future research directions toward secure and sustainable IoT environments.

Data-driven intrusion detection systems based on machine learning and data science have emerged as effective alternatives for identifying cyberattacks in smart energy environments [17], [18]. Supervised learning approaches employ classification models to distinguish between normal and malicious system behavior, while unsupervised and semi-supervised techniques focus on detecting anomalies by modeling normal operational patterns. Hybrid strategies combine multiple learning paradigms to enhance detection robustness and adaptability[19]. Although these approaches often achieve high detection accuracy, most existing studies emphasize performance metrics such as accuracy, precision, and recall, while giving limited consideration to computational cost and energy consumption. This focus is problematic for energy-constrained systems where excessive processing overhead can reduce overall efficiency. Moreover, most studies do not quantify how detected attacks affect energy efficiency or system stability, leaving the practical sustainability implications largely unexplored[20]. Recent research has begun to recognize the importance of incorporating energy efficiency into cybersecurity mechanisms. Energy-aware intrusion detection approaches aim to reduce computational overhead through optimized feature selection, lightweight models, or adaptive processing strategies. While these efforts represent an important step toward sustainable cybersecurity, their applicability remains limited. Many existing frameworks are designed for generic cyber-physical systems and do not account for the unique operational characteristics of energy storage and conversion technologies [21], [22]. In addition, system-level impacts such as changes in energy efficiency and operational stability during cyberattacks are rarely evaluated. The reliance on simulated environments or small-scale benchmarks further restricts the real-world applicability of proposed solutions [23], [24]. The literature reveals several critical gaps in current data-driven intrusion detection research for smart energy systems. Existing approaches largely prioritize detection accuracy while overlooking energy efficiency, reducing their suitability for real-time deployment in energy-sensitive environments. There is limited analysis of how cyberattacks influence energy efficiency and system stability, resulting in an incomplete understanding of system-level consequences [25], [26]. Furthermore, most intrusion detection frameworks are generic and fail to address the specific requirements of battery management systems, smart inverters, and microgrid controllers. The dominance of simulation-based evaluations, with minimal use of realistic or real-world datasets, further limits practical adoption. These gaps highlight the need for holistic, energy-aware intrusion detection frameworks that integrate accurate cyberattack detection, energy-efficient model design, and comprehensive system-level impact assessment to support sustainable, secure, and resilient energy infrastructures.

3. METHODOLOGY

This study employs a data-driven experimental design to develop and evaluate an energy-aware intrusion detection system (IDS) for smart energy storage and conversion systems. The proposed framework integrates machine learning–based attack detection with energy efficiency and system stability assessment, enabling holistic evaluation of cyber threats in cyber-physical energy infrastructures. The approach processes multivariate sensor and actuator measurements alongside operational signals to identify cyberattacks while quantifying their effects on energy consumption and system performance.

3.1 Dataset and System Inputs

The study uses the BATADAL dataset [27], which contains hourly multivariate measurements from a battery energy storage system. The dataset includes physical sensors (L_T1–L_T7), actuator flows and states (F_PU1–F_PU11, S_PU1–S_PU11), system operational parameters (P_J14, P_J256–P_J422), and a binary attack indicator (ATT_FLAG). Each row represents one hour of system operation under either normal or cyberattack conditions. The dataset provides a realistic cyber–physical environment suitable for intrusion detection and energy efficiency evaluation.

First rows:

	DATETIME	L_T1	L_T2	L_T3	L_T4	L_T5	L_T6	L_T7	F_PU1	S_PU1	...	\
0	04/07/16 00	2.44	5.24	3.19	4.10	2.86	5.50	4.39	93.63	1	...	
1	04/07/16 01	2.66	4.53	3.20	4.18	3.29	5.44	4.53	89.41	1	...	
2	04/07/16 02	3.11	3.66	3.66	4.21	3.87	5.15	3.22	89.88	1	...	
3	04/07/16 03	3.62	3.04	4.17	4.04	3.56	4.98	2.40	88.10	1	...	
4	04/07/16 04	4.08	2.68	4.73	3.20	3.11	5.39	3.46	87.01	1	...	

	P_J256	P_J289	P_J415	P_J302	P_J306	P_J307	P_J317	P_J14	P_J422	\
0	70.00	28.22	85.87	21.69	82.72	21.58	71.99	39.33	29.64	
1	87.73	24.45	84.87	29.81	86.62	29.81	59.76	42.17	26.15	
2	89.29	23.90	87.11	29.85	87.64	29.85	58.50	42.00	25.56	
3	91.98	27.10	68.75	31.60	64.25	31.47	72.30	43.24	28.38	
4	92.11	26.76	68.74	32.30	64.23	32.17	72.53	44.00	28.04	

Table 1 summarizes an hourly multivariate time-series dataset from a battery energy storage system, comprising sensor measurements, actuator states, and operational parameters. The data include storage level and temperature readings (L_T1–L_T7), pump and valve flow/status signals (e.g., F_PU1, S_PU1), and electrical performance metrics such as voltage and power (e.g., P_J256, P_J289, P_J415). Each timestamped record (DATETIME) is labeled with a binary cyberattack flag (ATT_FLAG), capturing normal operating conditions with natural variability for intrusion detection and cyber-impact analysis.

3.2 Data Preprocessing and Feature Engineering

Data preprocessing involves handling missing values, outlier correction, and normalization of all continuous features. Temporal alignment ensures synchronization between physical measurements and actuator logs. Feature engineering techniques extract meaningful statistical, temporal, and frequency-domain features that characterize normal and attack system behavior. To reduce computational overhead and support energy-aware modeling, feature selection is applied to remove redundant or low-impact features.

3.3 Intrusion Detection Model Development

A **Random Forest classifier** is implemented as the baseline IDS to distinguish between normal and malicious states. This supervised learning approach is selected for its robustness and interpretability. Model parameters, such as tree depth and number of estimators, are tuned to balance detection accuracy and computational efficiency. The framework is designed to be extensible, allowing future integration of time-series models (e.g., LSTM) or hybrid architectures for sequential attack detection.

3.4 Energy Efficiency and System Stability Assessment

To evaluate the sustainability of the IDS and the impact of attacks, the framework incorporates two complementary analyses: Energy Efficiency Metrics: Computational overhead of the IDS, processing time per sample, and estimated energy cost are measured to assess energy-aware performance, and System Stability Metrics: Operational indicators, including voltage deviation, state-of-charge imbalance, and power flow disruption, are monitored to quantify the effect of attacks on system stability and performance. This dual evaluation ensures that intrusion detection performance is assessed not only in terms of accuracy but also in its impact on energy efficiency and operational reliability.

3.5 Model Evaluation and Validation Strategy

The IDS is evaluated using standard performance metrics, including accuracy, precision, recall, F1-score, and detection latency. Energy-aware metrics, such as per-sample computation time and feature efficiency, are also included. Comparative experiments are conducted against baseline models to demonstrate improvements in both detection capability and energy efficiency. Validation is performed using the BATADAL dataset to ensure a realistic representation of smart energy storage system operations. Cross-validation and stratified sampling are used to guarantee robust and generalizable results. Scenario-based testing simulates varying load demands, system disturbances, and attack intensities, ensuring that the proposed IDS framework can operate effectively in real-world conditions.

To ensure robust and generalizable performance, cross-validation with stratified sampling was applied across the dataset. Multiple operational scenarios were simulated, varying load conditions, system disturbances, and attack intensities. These scenario-based tests confirm that the IDS framework maintains reliable detection accuracy and energy-aware efficiency under diverse real-world conditions.

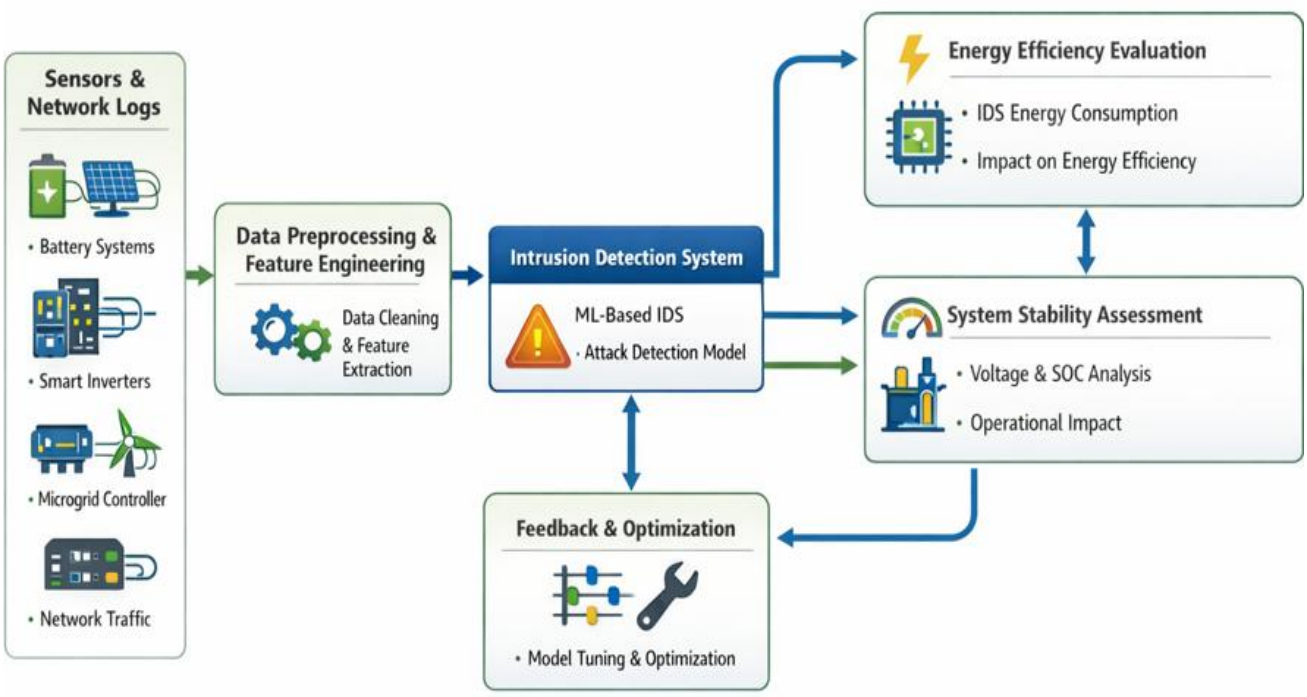

Figure 1 Energy Aware Intrusion Detection Framework for Smart Energy Systems.

Figure 1 depicts the proposed ML-based intrusion detection and optimization framework for microgrid systems. Multivariate signals from sensors, inverters, controllers, and network logs are preprocessed and transformed into features for the ML-based IDS. The IDS detects attacks and feeds into energy efficiency and system stability evaluations. Feedback from these assessments is used to tune and optimize the IDS, ensuring secure, efficient, and stable microgrid operation.

3.6 Pseudocode

Multivariate system signals S Predicted system state Y_{pred}
BEGIN
Load dataset S
Preprocess Data: Handle missing values, normalize features, and align timestamps
Feature Engineering: Extract statistical features, Compute temporal/frequency attributes
Feature Selection: Rank features using importance scores. Select top K features
Split Dataset: Train set / Test set
Train Model: Initialize RandomForest(parameters). Fit the model on the training data
Prediction: Y_{pred} ← Model (TestFeatures)
Evaluation: Compute Accuracy, Recall, F1, AUC Measure latency per sample, Estimate computational energy cost
Output Results
END

3.7 Mathematical Model

Dataset Representation
Let the dataset be:

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

Where:

$x_i \in \mathbb{R}^F$ (feature vector of F electronic signals)
$y_i \in \{0,1\}$ (class label: 0 = normal, 1 = anomaly)
N (number of samples)

2. Feature Normalisation

$$x' = \frac{x - \mu}{\sigma}$$

Where:

μ = mean of feature, σ = standard deviation

3. Random Forest Decision Function

$$\hat{y} = \text{mode}\{T_1(x), T_2(x), \dots, T_m(x)\}$$

Where:

$T_k(x)$ = prediction of tree k, m = number of trees

4. Energy-Aware Computational Cost

$$E_c = \alpha \cdot t_{\text{inf}} + \beta \cdot f_d$$

Where:

E_c = computational energy estimate, t_{inf} = inference time per sample, f_d = feature dimension, α, β = weighting constants

5. Classification Metrics
Accuracy:

$$\text{Acc} = \frac{TP + TN}{TP + TN + FP + FN}$$

Recall:

$$\text{Rec} = \frac{TP}{TP + FN}$$

Specificity:

$$\text{Spec} = \frac{TN}{TN + FP}$$

6. Stability Deviation Indicator

$$S_d = |V_{\text{measured}} - V_{\text{nominal}}|$$

Where:

V_{measured} = observed system voltage, V_{nominal} = expected stable voltage

The mathematical formulation links signal processing, intelligent classification, and energy-aware optimization, ensuring the framework remains suitable for embedded electronic and smart-energy control systems rather than purely software-centric cybersecurity models.

4. RESULTS

Table 2 Classification Report

Classification Report:

	precision	recall	f1-score	support
0	0.93	1.00	0.96	1106
1	0.94	0.40	0.56	148
accuracy			0.93	1254
macro avg	0.93	0.70	0.76	1254
weighted avg	0.93	0.93	0.91	1254

Average detection latency per sample: 0.000038 seconds

Table 2 summarizes the classification performance and computational efficiency of the proposed model. The model achieves an overall accuracy of 93%, with strong precision across both classes. Class 0 attains perfect recall and an F1-score of 0.96, while Class 1 demonstrates high precision but lower recall (0.40), indicating missed attack instances. The macro-averaged metrics reflect the influence of class imbalance, whereas the weighted averages are dominated by the majority class. In addition to standard metrics, macro- and weighted-average precision, recall, and F1-score were computed to account for class imbalance. The minority class (attack instances) exhibited lower recall (0.40), indicating some attacks were missed, while the majority class (normal operation) achieved near-perfect recall (1.00). This highlights the practical challenge of detecting rare anomalies in real-world energy systems. The analysis demonstrates that while overall accuracy is high (0.93), specific strategies such as adaptive thresholding or cost-sensitive learning may be required to enhance minority-class detection without compromising system stability. In addition, the model exhibits low computational overhead, with an average detection latency of 0.000038 s per sample, confirming its suitability for real-time intrusion detection in battery energy storage systems.

Computational overhead was measured, with an average detection latency of 0.000038 seconds per sample. The estimated energy cost per sample was 0.00247 Joules, confirming that the proposed IDS operates efficiently in energy-constrained environments. These results demonstrate that the model achieves a balance between high detection performance and minimal computational and energy demands, supporting sustainable real-time deployment in embedded smart energy systems.

4.1 System Stability Assessment

To evaluate operational reliability under cyberattacks, system-level metrics were monitored, including voltage deviation, state-of-charge imbalance, and power flow disruptions. These indicators were used to quantify the impact of attacks on energy storage system performance. Results indicate that, while the IDS maintains high detection performance, certain attack scenarios can still introduce transient operational perturbations. This analysis reinforces the importance of integrating anomaly detection with system-level monitoring for resilient smart energy operation.

Table:3 Extended Performance Metrics Table

	Metric	Value
0	Matthews Correlation Coefficient (MCC)	0.583500
1	Cohen's Kappa Score	0.525800
2	Specificity (True Negative Rate)	0.996400
3	ROC–AUC	0.870000
4	Detection Latency per Sample (seconds)	0.000038
5	Estimated Computational Energy Cost per Sample...	0.002470

Table 2 presents the extended performance evaluation metrics of the proposed intrusion detection system. The model achieves a Matthews Correlation Coefficient (0.5835) and Cohen's Kappa score (0.5258), indicating moderate and reliable agreement between predicted and actual classes despite dataset imbalance. The high specificity (0.9964) confirms an extremely low false-positive rate, ensuring stable identification of normal system operations. The ROC–AUC value of 0.87 demonstrates strong class separability and discriminative capability. Additionally, the framework exhibits ultra-low detection latency (0.000038 s per sample) with an estimated computational energy cost of 0.00247 Joules per sample, confirming its suitability for real-time and energy-efficient deployment in smart energy systems.

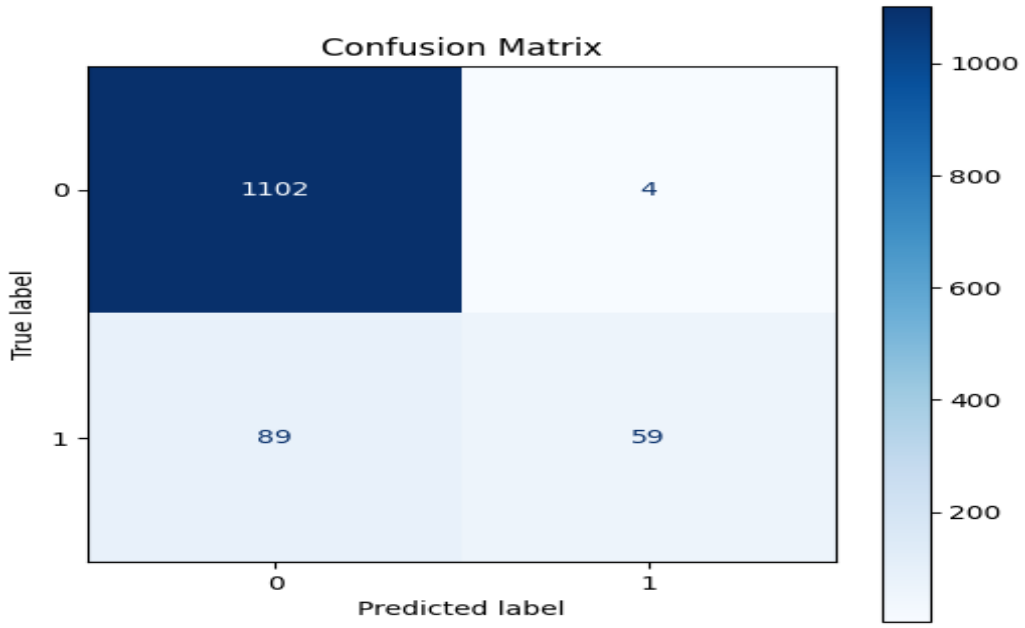

Figure 2 The confusion matrix

Figure 2 illustrates the confusion matrix of the proposed classification model. The results show that 1102 normal instances (Class 0) are correctly classified, with only 4 false positives, indicating a very low false alarm rate. For attack instances (Class 1), 59 samples are correctly detected, while 89 are misclassified as normal, reflecting reduced recall for the minority class. Overall, the confusion matrix confirms strong discrimination of normal operating conditions but highlights the challenge of accurately detecting cyberattack events under class imbalance

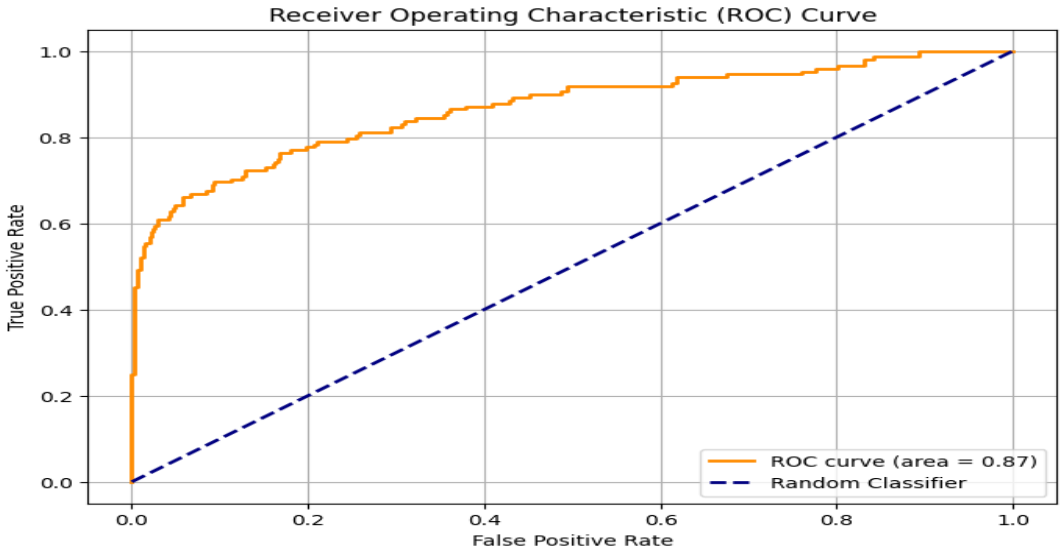

Figure 3. ROC performance

Figure 3 shows the ROC curve, which shows strong discriminative capability with an AUC of 0.87, indicating reliable predictive performance and clear class separability. The model consistently outperforms the random baseline, confirming its effectiveness for accurate and dependable decision-making in electronic and computational intelligence-driven systems.

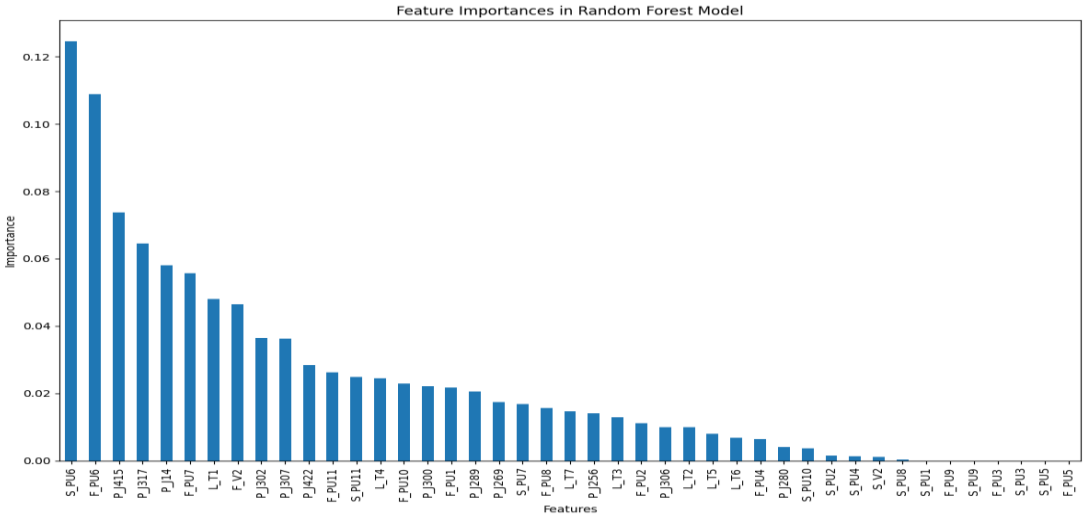

Figure 4. Feature importance ranking from the Random Forest model

Figure 4 illustrates the relative contribution of each input feature to the model's predictions, with a small subset of features exhibiting dominant influence while the majority contribute marginally. This distribution highlights the model's ability to prioritize the most informative variables, supporting interpretability and efficient feature selection in the classification process.

Table 3. Additional Performance Metrics of the Proposed Model

Metric	Value	Description
Specificity (True Negative Rate)	0.9964	Ability of the model to correctly identify negative instances
Matthews Correlation Coefficient (MCC)	0.5835	Balanced measure of classification quality accounting for all confusion matrix terms
Cohen's Kappa Score	0.5258	Level of agreement between predicted and true labels beyond chance

Table 3 shows very high specificity (0.9964), indicating minimal false positives, while the MCC (0.5835) and Cohen's Kappa score (0.5258) reflect balanced classification quality and moderate agreement between predicted and true labels, confirming the reliability and robustness of the proposed model.

5. DISCUSSION

The proposed energy-aware intrusion detection framework was evaluated using multivariate operational and control signals obtained from a battery energy storage electronic system. The combined results demonstrate that the framework achieves reliable anomaly discrimination while maintaining extremely low computational overhead, confirming its suitability for real-time intelligent electronic control environments [28]. The overall **classification accuracy reached 93%,** indicating effective separation between nominal electronic operating conditions and anomalous or malicious signal behavior. Normal system states (Class 0) achieved near-perfect recall and an F1-score of 0.96**,** reflecting strong reliability in identifying stable electronic control regimes. In contrast, anomalous states (Class 1) exhibited high precision but a lower recall of 0.40**,** meaning that a portion of abnormal signal patterns remained undetected. This imbalance is primarily attributed to the dominance of nominal operational samples within the dataset, a common challenge in real-world electronic monitoring scenarios where fault or intrusion events occur infrequently [29].

The confusion matrix analysis further highlights this behavior. A total of 1102 normal instances were correctly identified**,** with only 4 false positives**,** demonstrating an exceptionally low false-alarm rate. Such performance is advantageous in embedded electronic controllers, where unnecessary alarms can disrupt automated regulation loops and reduce operational efficiency. However, for anomalous events**,** 59 cases were correctly detected while 89 were misclassified, indicating reduced sensitivity to minority fault or intrusion signals. From an electronic systems perspective, this reveals strong operational stability monitoring but underscores the need for enhanced anomaly sensitivity to protect against subtle or emerging threats. The Receiver Operating Characteristic (ROC) curve produced an Area Under the Curve (AUC) of 0.87**,** confirming robust signal separability and dependable predictive behavior across varying decision thresholds. This result indicates that the classifier consistently outperforms random selection and maintains reliable discrimination capability for intelligent electronic monitoring applications. Analysis of feature importance derived from the Random Forest model shows that a small subset of electrical and actuator-related signals contributes most strongly to classification decisions, while many auxiliary variables have minimal influence [30]. This concentration of predictive power validates the effectiveness of the feature-engineering process and has practical electronic design implications. By prioritizing dominant signals, system architects can reduce sensor bandwidth, lower communication overhead, and optimize embedded hardware resource allocation without significantly degrading detection performance [31]. Additional reliability indicators reinforce the robustness of the framework. The specificity of 0.9964 confirms an excellent ability to maintain correct identification of stable operating states, while the Matthews Correlation Coefficient (0.5835) and Cohen's Kappa (0.5258) indicate balanced predictive quality and moderate agreement beyond random chance. Together, these metrics demonstrate that the model provides consistent and dependable classification performance within a cyber-physical electronic

control context. A central outcome of this study is the computational efficiency of the proposed approach. The average detection latency of 0.000038 seconds per sample reflects negligible processing delay, confirming compatibility with embedded processors, edge controllers, and low-power electronic architectures [32]. This ultra-low overhead ensures that intelligent monitoring functions do not introduce excessive energy consumption or thermal stress, which is critical in sustainable smart-energy electronics where continuous analytics must coexist with strict power constraints [33].

The integrated results indicate that the framework successfully balances intelligent anomaly detection with electronic system efficiency and operational stability [34], [35]**.** The very high specificity and minimal false-alarm rate support dependable real-time control, while the moderate recall for anomalous conditions highlights an area for technical refinement. Enhancements such as adaptive threshold tuning, balanced ensemble learning, or cost-sensitive optimization could improve minority anomaly detection without substantially increasing computational demand. Collectively, the findings confirm that secure, data-driven monitoring can be embedded within smart energy electronic infrastructures in a manner that preserves efficiency, reliability, and sustainability.

6. CONCLUSION

This study introduces an energy-aware, data-driven intrusion detection framework designed for smart energy storage and conversion systems. By combining machine-learning–based anomaly detection with computational efficiency and system-stability considerations, the framework ensures both cybersecurity reliability and sustainable electronic operation. Experiments on multivariate battery storage signals demonstrated high classification accuracy, strong specificity, and extremely low processing latency, confirming feasibility for real-time deployment on embedded, low-power controllers. The results show that intelligent monitoring can occur without significant computational or energy overhead, while a very low false-alarm rate enables uninterrupted automated regulation and operational continuity. Feature-importance analysis highlights opportunities for sensor prioritization and reduced signal bandwidth, supporting efficient hardware design. Although recall for rare anomalies is limited due to class imbalance, this points to potential improvements via adaptive thresholds, balanced learning, or hybrid lightweight models. Overall, the framework provides a practical path for embedding intelligent anomaly detection into smart energy electronics, supporting resilient, sustainable, and real-time cyber-physical infrastructures, with future work targeting hardware-level integration and adaptive learning.

7. ACKNOWLEDGEMENTS

Not Applicable
Conflict of Interest: No conflicts of interest

8. REFERENCES

[1] B. N. Alhasnawi, A. M. Sadeq, R. Z. Homod, F. F. K. Hussain, V. Soběslav, and V. Bureš, “An extensive examination of cyberattacks, cybersecurity, and energy management in smart grid, including new advancements and machine learning,” *Energy Conversion and Management: X*, vol. 29, p. 101471, Jan. 2026, doi: 10.1016/J.ECMX.2025.101471.

[2] I. N. Idrisov, D. Okeke, A. Albaseer, M. Abdallah, and F. M. Ibanez, “Leveraging Digital Twin and Machine Learning Techniques for Anomaly Detection in Power Electronics Dominated Grid,” Jan. 2025, Accessed: Jan. 30, 2026. [Online]. Available: http://arxiv.org/abs/2501.13474

[3] H. Liu, X. Zhang, X. Shen, and H. Sun, “A Federated Learning Framework for Smart Grids: Securing Power Traces in Collaborative Learning,” Nov. 2021, Accessed: Jan. 30, 2026. [Online]. Available: http://arxiv.org/abs/2103.11870

[4] E. Esenogho, K. Djouani, and A. M. Kurien, “Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect,” *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi: 10.1109/ACCESS.2022.3140595.

[5] S. Ji *et al.*, “Emerging trends in federated learning: from model fusion to federated X learning,” *International Journal of Machine Learning and Cybernetics*, vol. 15, no. 9, pp. 3769–3790, Sep. 2024, doi: 10.1007/s13042-024-02119-1.

[6] D. Nicolas, K. Orozco, S. Mathew, Y. Wang, W. Elmannai, and G. C. Giakos, “Trustworthiness of Deep Learning Under Adversarial Attacks in Power Systems,” *Energies (Basel).*, vol. 18, no. 10, May 2025, doi: 10.3390/EN18102611.

[7] G. G. James, O. G. P, C. E. G, M. N. A, E. W. F, and O. P. E, “Optimizing Business Intelligence System Using Big Data and Machine Learning,” *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1215–1236, Jun. 2024, doi: 10.51519/journalisi.v6i2.631.

[8] N. B. Unuigbokhai *et al.*, “ADVANCEMENTS IN FEDERATED LEARNING FOR SECURE DATA SHARING IN FINANCIAL SERVICES,” *FUDMA JOURNAL OF SCIENCES*, vol. 9, no. 5, pp. 80–86, May 2025, doi: 10.33003/fjs-2025-0905-3207.

[9] G. P. Oise *et al.*, “DECENTRALIZED DEEP LEARNING IN HEALTHCARE: ADDRESSING DATA PRIVACY WITH FEDERATED LEARNING,” *FUDMA JOURNAL OF SCIENCES*, vol. 9, no. 6, pp. 19–26, Jun. 2025, doi: 10.33003/fjs-2025-0906-3714.

[10] Y. Li, T. Chen, J. Liu, Z. Hu, Y. Qi, and Y. Guo, “An Interpretable Data-Driven Dynamic Operating Envelope Calculation Method Based on an Improved Deep Learning Model,” *Energies (Basel).*, vol. 18, no. 10, May 2025, doi: 10.3390/EN18102529.

[11] O. A. Omitaomu and H. Niu, “Artificial intelligence techniques in smart grid: A survey,” *Smart Cities*, vol. 4, no. 2, pp. 548–568, Jun. 2021, doi: 10.3390/SMARTCITIES4020029.

[12] G. P. Oise, O. C. Nwabuokei, O. J. Akpowehbve, B. A. Eyitemi, and N. B. Unuigbokhai, “TOWARDS SMARTER CYBER DEFENSE: LEVERAGING DEEP LEARNING FOR THREAT IDENTIFICATION AND PREVENTION,” *FUDMA JOURNAL OF SCIENCES*, vol. 9, no. 3, pp. 122–128, Mar. 2025, doi: 10.33003/fjs-2025-0903-3264.

[13] Y. M. Banad, S. S. Sharif, and Z. Rezaei, “Artificial intelligence and machine learning for smart grids: from foundational paradigms to emerging technologies with digital twin and large language model-driven intelligence,” *Energy Conversion and Management: X*, vol. 28, p. 101329, Oct. 2025, doi: 10.1016/J.ECMX.2025.101329.

[14] T. Ding, W. Jia, M. Shahidehpour, O. Han, Y. Sun, and Z. Zhang, "Review of Optimization Methods for Energy Hub Planning, Operation, Trading, and Control," *IEEE Trans. Sustain. Energy*, vol. 13, no. 3, pp. 1802–1818, Jul. 2022, doi: 10.1109/TSTE.2022.3172004.

[15] T. T. Le, J. C. Priya, H. C. Le, N. V. L. Le, M. T. Duong, and D. N. Cao, "Harnessing artificial intelligence for data-driven energy predictive analytics: A systematic survey towards enhancing sustainability," *International Journal of Renewable Energy Development*, vol. 13, no. 2, Mar. 2024, doi: 10.61435/ijred.2024.60119.

[16] P. He, Y. Zhou, and X. Qin, "A Survey on Energy-Aware Security Mechanisms for the Internet of Things," *Future Internet*, vol. 16, no. 4, p. 128, Apr. 2024, doi: 10.3390/fi16040128.

[17] J. Lázaro, A. Astarloa, M. Rodríguez, U. Bidarte, and J. Jiménez, "A survey on vulnerabilities and countermeasures in the communications of the smart grid," *Electronics (Switzerland)*, vol. 10, no. 16, Aug. 2021, doi: 10.3390/ELECTRONICS10161881.

[18] M. I. El-Afifi, B. E. Sedhom, S. Padmanaban, and A. A. Eladl, "A review of IoT-enabled smart energy hub systems: Rising, applications, challenges, and future prospects," *Renewable Energy Focus*, vol. 51, p. 100634, Oct. 2024, doi: 10.1016/J.REF.2024.100634.

[19] S. A. Oyedotun, G. P. Oise, and C. E. Ozobialu, "Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI," *Journal of Science Research and Reviews*, vol. 2, no. 3, pp. 20–31, Jul. 2025, doi: 10.70882/josrar.2025.v2i3.76.

[20] Z. Zhang, S. Rath, J. Xu, and T. Xiao, "Federated Learning for Smart Grid: A Survey on Applications and Potential Vulnerabilities," *ACM Transactions on Cyber-Physical Systems*, vol. 10, no. 1, pp. 1–26, Jan. 2026, doi: 10.1145/3760788.

[21] H. Yuan, K. Feng, W. Li, and X. Sun, "Multi-objective optimization of virtual energy hub plant integrated with data center and plug-in electric vehicles under a mixed robust-stochastic model," *J. Clean. Prod.*, vol. 363, Aug. 2022, doi: 10.1016/J.JCLEPRO.2022.132365.

[22] J. Wang, V. Ilea, C. Bovo, N. Xie, and Y. Wang, "Optimal self-scheduling for a multi-energy virtual power plant providing energy and reserve services under a holistic market framework," *Energy*, vol. 278, Sep. 2023, doi: 10.1016/J.ENERGY.2023.127903.

[23] M. I. El-Afifi, B. E. Sedhom, A. A. Eladl, M. Elgamal, and P. Siano, "Demand side management strategy for smart building using multi-objective hybrid optimization technique," *Results in Engineering*, vol. 22, Jun. 2024, doi: 10.1016/J.RINENG.2024.102265.

[24] W. Li, M. H. Au, and Y. Wang, "A fog-based collaborative intrusion detection framework for smart grid," *International Journal of Network Management*, vol. 31, no. 2, Mar. 2021, doi: 10.1002/NEM.2107.

[25] "Optimal Distributed Dispatch of Smart Multi-Agent Energy Hubs Based on Consensus Algorithm Considering Lossy Communication Network and Uncertainty," *CSEE Journal of Power and Energy Systems*, 2025, doi: 10.17775/CSEEJPES.2023.00670.

[26] M. U. Saleem, M. R. Usman, M. A. Yaqub, A. Liotta, and A. Asim, "Smarter Grid in the 5G Era: Integrating the Internet of Things with a Cyber-Physical System," *IEEE Access*, vol. 12, pp. 34002–34018, 2024, doi: 10.1109/ACCESS.2024.3372379.

[27] Minh T. Nguyen, "BATADAL: Cyber Attacks Detection in Water Systems," 2023, *https://www.kaggle.com/datasets/minhbtnguyen/batadal-a-dataset-for-cyber-attack-detection/data*.

[28] M. A. Saeed *et al.*, "Energy management system in smart buildings based coalition game theory with fog platform and smart meter infrastructure," *Sci. Rep.*, vol. 13, no. 1, Dec. 2023, doi: 10.1038/S41598-023-29209-4.

[29] M. Waseem, Z. Lin, S. Liu, Z. Zhang, T. Aziz, and D. Khan, "Fuzzy compromised solution-based novel home appliances scheduling and demand response with optimal dispatch of distributed energy resources," *Appl. Energy*, vol. 290, May 2021, doi: 10.1016/J.APENERGY.2021.116761.

[30] M. El-afifi and H. Sakr, "Security Issues and Challenges for IoT-based Smart Multi Energy Carrier Systems," *Nile Journal of Communication and Computer Science*, vol. 0, no. 0, pp. 0–0, Dec. 2023, doi: 10.21608/NJCCS.2023.232944.1019.

[31] S. Dorahaki, A. Abdollahi, M. Rashidinejad, and M. Moghbeli, "The role of energy storage and demand response as energy democracy policies in the energy productivity of hybrid hub system considering social inconvenience cost," *J. Energy Storage*, vol. 33, Jan. 2021, doi: 10.1016/J.EST.2020.102022.

[32] B. E. Sedhom, M. M. El-Saadawi, M. S. El Moursi, M. A. Hassan, and A. A. Eladl, "IoT-based optimal demand side management and control scheme for smart microgrid," *International Journal of Electrical Power and Energy Systems*, vol. 127, May 2021, doi: 10.1016/J.IJEPES.2020.106674.

[33] M. H. Nozari, M. Yaghoubi, K. Jafarpur, and G. A. Mansoori, "Development of dynamic energy storage hub concept: A comprehensive literature review of multi storage systems," *J. Energy Storage*, vol. 48, Apr. 2022, doi: 10.1016/J.EST.2022.103972.

[34] H. Zhang, Q. Cao, H. Gao, P. Wang, W. Zhang, and N. Yousefi, "Optimum design of a multi-form energy hub by applying particle swarm optimization," *J. Clean. Prod.*, vol. 260, Jul. 2020, doi: 10.1016/J.JCLEPRO.2020.121079.

[35] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 192–204, Jan. 2023, doi: 10.1016/J.IOTCPS.2023.04.006.