PAE-IDS: Adaptive Energy-Aware Intrusion Detection for Smart Grids Using PureChain

Nanteza Adah Lubwama [1], Love Allen Chijioke Ahakonye [2], Dong-Seong Kim [1] *, Jae Min Lee [1] †
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National of Technology*, Gumi, South Korea
(adah, loveahakonye, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—Smart grid security faces the dual challenge of maintaining robust intrusion detection while minimizing energy consumption. This paper presents the Adaptive Energy-Aware Intrusion Detection System (PAE-IDS), to achieve optimal balance between security effectiveness and energy efficiency. Our system implements risk-based segmentation, dynamic monitoring adjustment, and feedback-driven optimization. Experimental results on a 60,000-sample smart grid stability dataset demonstrate 40-60% energy reduction while maintaining 99.6% detection accuracy for high-risk segments. The proposed framework offers a scalable solution for resource-constrained smart grid environments. Additionally, it uses PureChain with low latency and high throughput.**

***Index Terms*—Energy efficiency, Intrusion detection, PureChain, Smart grid security.**

I. Introduction

Smart grids face a core challenge: ensuring continuous cybersecurity while minimizing the energy overhead of intrusion detection systems (IDS), which can consume up to 15% of grid management resources. As IDS have become integral to smart grid defense [1], their high computational demand creates a trade-off between security coverage and energy efficiency [2]. Existing IDS designs either favor lightweight models with reduced accuracy or complex models with heavy energy consumption, failing to adapt to the heterogeneous and dynamic threat landscape of smart grid networks.

The energy consumption of continuous high-intensity monitoring can account for up to 15% of total grid management overhead, making it economically and environmentally unsustainable [3]. This paper introduces the PureChain Adaptive Energy-Aware Intrusion Detection System (PAE-IDS). This adaptive framework applies five principles, such as Segmentation, Resource Utilization, Dynamics, and Periodic Action, to resolve the security-efficiency contradiction. The principles considered in this study include a risk-based segmentation strategy for intelligent resource allocation. This dynamic monitoring system adapts to real-time threat levels, a feedback-driven mechanism for optimizing detection thresholds and energy use, and PureChain, a consensus protocol [4] offering low latency and high throughput.

II. Summary of System Architecture

PAE-IDS implements a hierarchical architecture incorporating five principles to achieve optimal balance between security effectiveness and energy efficiency as shown in Figure 1.

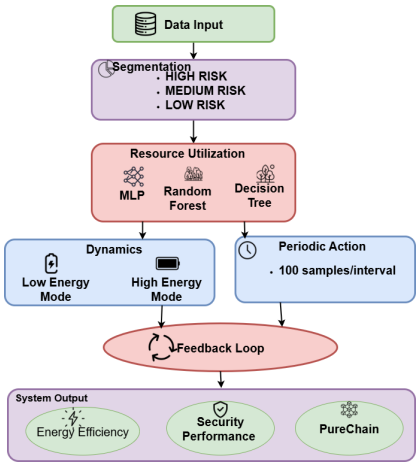

Fig. 1. Architecture of Improved BiLSTM

1) Segmentation: The system divides network traffic into risk-based segments using a composite risk score calculated from grid stability parameters and power variations as in Equation 1.

$$RS = |\sigma(\text{stab})| + \sigma(P_1 \dots P_4) + \sigma(G_1 \dots G_4), \quad (1)$$

where RS represents risk score, σ denotes standard deviation, P represents power consumption nodes, and G represents generation nodes.

2) Resource Utilization: This is tailored based on the risk segment identified during segmentation. For the high-risk segment, a Multi-Layer Perceptron (MLP) model is utilized, configured with a range of 100 to 50 neurons to capture complex patterns. In the case of medium-risk, a Random Forest (RF) model with 50 estimators is employed to balance predictive accuracy and computational efficiency. Finally, for the low-risk segment, a Decision Tree (DT) model is used, with a maximum depth of 5, ensuring simplicity and interpretability while maintaining adequate performance for low-risk conditions.

3) Dynamics: The monitoring intensity adapts based on anomaly detection rates. When the anomaly ratio exceeds the threshold θ, the system switches from lightweight to

comprehensive monitoring as in Equation 2.

$$M(t) = \begin{cases} M_{\text{high}} & \text{if } A(t) > \theta \\ M_{\text{low}} & \text{otherwise} \end{cases} \quad (2)$$

4) Periodic Action: Instead of continuous monitoring, the system processes data in configurable intervals (default: 100 samples), reducing unnecessary computational overhead.

5) Feedback: Historical performance data optimizes future threshold adjustments as in Equation 3.

$$\theta(t+1) = \theta(t) \times \alpha, \quad (3)$$

where α= 1.2 if mean anomaly ¡ 0.05, and α= 0.8 if mean anomaly ¿ 0.15.

6) Energy Consumption Modeling: Energy consumption is estimated using a complexity-weighted time metric, expressed as in Equation 4.

$$E = T \times C(M), \quad (4)$$

where T denotes the training or inference time, and $C(M)$ represents the model complexity, assigned as $C(\text{MLP}) = 10.0$, $C(\text{RF}) = 5.0$, and $C(\text{DT}) = 1.0$.

The PAE-IDSContract employs the PureChain`logIntrusion` function to record intrusion events with associated risk levels and anomaly counts, while `updateModel` enables validators to revise anomaly detection performance metrics. Experiments, conducted using PyTorch 1.10 on an NVIDIA Tesla V100 GPU (16GB VRAM) and Intel Xeon CPU with 32GB RAM, utilized the Smart Grid Stability Dataset ([5]), which comprises 60,000 samples with 12 features for binary stability classification. Risk segmentation categorized data into high (30%), medium (40%), and low (30%) risk levels.

III. Performance Evaluation

Table I confirms that the PAE-IDS design mitigates the security–efficiency trade-off in smart grid IDS, achieving 99.6% detection accuracy for high-risk segments while reducing energy consumption by 40–60%. Table II presents the training

TABLE I
Risk Segment Performance

Risk Level	Model Type	Accuracy	Energy	Training Time(s)
High	MLP	0.996	41.50	4.15
Medium	RF	0.947	13.32	2.66
Low	DT	0.821	0.12	0.12

settings of 500 epochs for the high-risk MLP, 50 trees for the medium-risk RF, and a single-pass depth-5 DT for low-risk cases. The recommended ranges are 300–500 epochs for MLP, RF 30–50 trees, and DT depth 3–5, which define optimal efficiency points where additional training yields marginal accuracy gains.

Figure 2 compares model performance in terms of throughput, latency, and transactions. Throughput scales with transaction volume, peaking at 500, while latency initially increases and then stabilizes. Rapid throughput stabilization enhances

TABLE II
Recommended Model Epochs and Parameters Based on Risk Level

Risk Level	Current Epochs	Recommended Range
High Risk	**500**	**300-500**
Medium Risk	**50 trees**	**30-50 trees**
Low Risk	**1 pass (depth=5)**	**1 pass (depth=3-5)**

energy efficiency, as high throughput and low latency minimize communication overhead, whereas prolonged latency elevates energy consumption through additional training rounds.

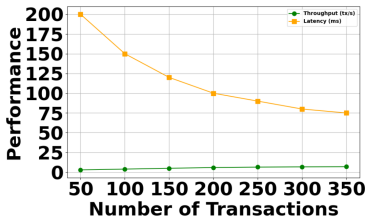

Fig. 2. Throughput of PureChain

IV. Conclusion and Future Work

The paper introduces PAE-IDS, an adaptive energy-aware intrusion detection framework for smart grids that integrates risk-based segmentation, dynamic monitoring, and feedback optimization. It achieves 40–60% energy savings while preserving high detection accuracy in critical areas, offering a scalable and efficient security solution for resource-constrained environments.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] J. A. Simioni, E. K. Viegas, A. O. Santin, and E. de Matos, "An energy-efficient intrusion detection offloading based on dnn for edge computing," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 20 326–20 342, 2025.

[2] L. Ahakonye, C. Nwakanma, J. M. Lee, and D.-S. Kim, "Low Computational Cost Convolutional Neural Network for Smart Grid Frequency Stability Prediction," *Internet of Things*, vol. 25, p. 101086, 04 2024.

[3] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Time-Efficient Deep Learning-Based Energy Consumption Prediction for Smart Factory," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 879–882.

[4] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Purechain-Enhanced Federated Learning for Dynamic Fault Tolerance and Attack Detection in Distributed Systems," *High-Confidence Computing*, p. 100354, 2025.

[5] V. Arzamasov, K. Böhm, and P. Jochem, "Towards Concise Models of Grid Stability," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018, pp. 1–6.