ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2026.0377

CARBON-NEUTRAL CYBERSECURITY CIRCUITS USING OSV-BISGA FOR SUSTAINABLE INDUSTRIAL APPLICATIONS

Thomas Samraj Lawrence
Department of Information Technology, College of Engineering and Technology, Dambi Dollo University, Ethiopia

Abstract

Industrial cyber–physical systems increasingly have relied on secure circuits that also have aligned with carbon neutral goals. Prior studies have emphasized detection accuracy, yet the energy footprint of security algorithms has remained marginally addressed. The need for energy-aware cybersecurity circuits has therefore emerged as a critical research direction. Conventional intrusion detection circuits have consumed excessive power due to continuous monitoring that has depended on computationally intensive learning models. These approaches have limited suitability for green industrial infrastructure, where both security assurance and energy efficiency have been demanded simultaneously. A lack of unified frameworks that have integrated low-power algorithms with sustainable circuit deployment has persisted. A novel energy-efficient framework that has been termed OSV-BiSGA has been proposed for industrial cybersecurity circuits. The framework has combined a one-class support vector model with a bidirectional snow geese optimization algorithm that has minimized redundant computations. Continuous monitoring that has been designed at the circuit level has adapted sampling rates dynamically, which has reduced idle power consumption. Green infrastructure principles that have included low-leakage components and adaptive voltage scaling have been incorporated into the circuit design. Optimization that has guided parameter selection has ensured minimal energy usage without degrading detection reliability. The proposed OSV-BiSGA framework achieves an accuracy of 0.95, precision of 0.93, recall of 0.94, and F1-score of 0.94 at a population size of 30, while reducing energy consumption to 40 J. Compared with Static One-Class SVM, PSO-Optimized IDS, and Always-On Deep Learning IDS, the framework reduces energy usage by up to 63% while maintaining superior detection performance.

Keywords:

Cybersecurity Circuits, Carbon Neutrality, Energy-Efficient Algorithms, Continuous Monitoring, Green Infrastructure

1. INTRODUCTION

The rapid expansion of industrial cyber–physical systems has intensified the demand for cybersecurity mechanisms that align with carbon neutral objectives. Modern industrial circuits have supported automation, real-time control, and data-driven decision processes, yet these advances have also increased exposure to cyber threats. Prior research has emphasized robust detection algorithms and resilient architectures that have protected industrial assets against attacks [1]. At the same time, sustainability concerns have motivated the adoption of energy-aware designs that have reduced power consumption across sensing, computation, and communication layers [2]. Green infrastructure that has integrated low-power circuits, adaptive resource management, and environmentally conscious deployment strategies has therefore emerged as a parallel research focus [3]. The convergence of cybersecurity and sustainability has thus become essential rather than optional.

Despite these advances, several challenges have persisted in industrial cybersecurity circuits. Continuous monitoring that has relied on always-on detection modules has increased energy dissipation, particularly in resource-constrained industrial nodes [4]. Many learning-based security mechanisms have depended on complex feature extraction and high-dimensional optimization, which has escalated computational overhead and carbon footprint [5]. These challenges have limited the practical deployment of secure circuits within green industrial infrastructures, where energy budgets and thermal constraints have remained strict.

The core problem has therefore involved the lack of a unified framework that has simultaneously addressed intrusion detection accuracy, continuous monitoring reliability, and energy efficiency at the circuit level [6]. Existing approaches have often optimized security performance in isolation, while sustainability considerations have been treated as secondary design constraints [7]. This separation has resulted in solutions that have performed well in controlled environments but have shown limited scalability and long-term feasibility in carbon-conscious industrial settings.

The primary objective of this research has been to design an energy-efficient cybersecurity framework for industrial circuits that supports carbon neutral goals without compromising detection effectiveness. The study has aimed to integrate continuous monitoring that has adapted dynamically to system behavior, alongside a lightweight learning mechanism that has minimized redundant computation. Another objective has involved embedding green infrastructure principles directly into the circuit-level design, rather than addressing sustainability as an external optimization layer.

The novelty of this work lies in the coupling of a one-class support vector mechanism with a bidirectional snow geese optimization strategy within an industrial circuit context. Unlike conventional designs, the proposed OSV-BiSGA framework has balanced anomaly detection capability with energy-aware optimization, which has reduced unnecessary monitoring overhead. Furthermore, the framework has introduced adaptive operational modes that have aligned cybersecurity functions with carbon efficiency targets.

The main contributions of this study are twofold. First, a carbon-aware cybersecurity circuit framework that has integrated energy-efficient algorithms with continuous monitoring has been presented. Second, an optimization-driven design methodology that has demonstrated measurable reductions in power consumption while maintaining industrial security requirements has been validated through experimental analysis.

2. RELATED WORKS

Early studies on industrial cybersecurity have primarily focused on detection accuracy and system robustness. Several works have proposed machine learning-based intrusion detection systems that have utilized support vector machines, decision trees, and neural networks for identifying abnormal behavior in industrial control networks [8]. These approaches have demonstrated strong detection performance; however, their implementation has often involved high computational complexity, which has limited their suitability for energy-constrained industrial circuits.

Subsequent research has explored one-class classification techniques that have addressed scenarios where labeled attack data has remained scarce. One-class support vector models have been widely adopted due to their ability to model normal behavior effectively [9]. These models have reduced training complexity, yet their deployment in continuous monitoring environments has still incurred nontrivial energy costs, especially when combined with high-frequency sampling.

Optimization algorithms inspired by natural processes have also been investigated to enhance cybersecurity performance. Swarm intelligence techniques such as particle swarm optimization and genetic algorithms have been applied to parameter tuning and feature selection tasks [10]. These methods have improved detection efficiency, but iterative optimization processes have increased processing overhead, which has conflicted with green computing objectives.

In parallel, research on energy-efficient industrial circuits has emphasized low-power design strategies and adaptive resource management. Techniques such as dynamic voltage and frequency scaling have been introduced to reduce power consumption during low-load conditions [11]. While these methods have supported sustainability, they have rarely been integrated explicitly with cybersecurity functions, leading to fragmented design approaches.

Continuous monitoring frameworks have also been examined extensively. Prior works have proposed always-on monitoring architectures that have ensured rapid attack detection in critical infrastructures [12]. Although effective from a security perspective, such architectures have significantly increased energy usage, particularly when deployed across large-scale industrial networks.

More recent studies have begun to address green cybersecurity concepts. Some researchers have investigated energy-aware intrusion detection systems that have adjusted detection intensity based on perceived risk levels [13]. These approaches have represented an important step toward sustainable security, yet they have often lacked optimization mechanisms that have systematically minimized energy consumption at the algorithmic level.

Nature-inspired algorithms tailored for energy efficiency have gained attention in recent years. Optimization strategies based on migratory behavior, such as bird flocking models, have been explored for reducing computational redundancy [14]. These methods have shown promise in balancing exploration and exploitation with lower iteration counts. However, their application to industrial cybersecurity circuits has remained limited, and comprehensive frameworks that have combined such algorithms with one-class detection and green infrastructure principles have been scarce.

3. PROPOSED OSV-BISGA METHOD

The proposed OSV-BiSGA framework has been designed as an energy-efficient cybersecurity mechanism for industrial circuits that has aligned with carbon neutral goals. The method has integrated a one-class support vector model with a bidirectional snow geese optimization strategy that has reduced computational redundancy during continuous monitoring. A green infrastructure-aware circuit design has been incorporated, which has enabled adaptive operation under varying workload conditions. Continuous monitoring that has been implemented at the circuit level has dynamically adjusted sampling and processing intensity based on observed system behavior. As a result, the framework has maintained reliable intrusion detection while overall energy consumption has been significantly reduced.

3.1 INDUSTRIAL DATA ACQUISITION AND ENERGY-AWARE PREPROCESSING

Industrial data acquisition has operated as the first stage of the proposed framework. The system continuously receives network traffic, sensor signals, and control messages from industrial circuits. Raw data streams have often contained noise, redundancy, and temporal irregularities, which have increased unnecessary processing load. To mitigate this issue, an energy-aware preprocessing module has been introduced.

Preprocessing has normalized incoming signals and filtered irrelevant features using lightweight statistical operations. Feature scaling has ensured numerical stability for the learning model, while redundancy elimination has reduced dimensionality. This stage has minimized switching activity within the circuit, which has directly contributed to lower power dissipation.

The preprocessing operation has been mathematically expressed as:

$$X_{\text{norm}} = \frac{X - \mu_X}{\sigma_X} \tag{1}$$

$$E_{\text{prep}} = \sum_{i=1}^{n} \left(P_i \cdot T_i \right) \tag{2}$$

where X is represented the acquired industrial data, μ_X and σ_X have denoted the mean and standard deviation, E_{prep} is indicated preprocessing energy consumption, P_i has denoted processing power, and T_i is represented execution time. The reduced E_{prep} has validated the effectiveness of the preprocessing stage.

3.2 ONE-CLASS SUPPORT VECTOR MODELING

The second stage has involved the learning of normal industrial behavior using a one-class support vector mechanism. Unlike multi-class classifiers, the one-class model has focused solely on legitimate operational patterns, which has made it suitable for industrial environments where attack samples have been scarce. The model has constructed a decision boundary that has enclosed normal data points within a high-dimensional feature space. Any deviation from this learned boundary has been treated as anomalous behavior. This design choice has reduced training complexity and memory usage, which has supported green circuit objectives.

The decision function of the one-class support vector model has been defined as:

$$f(x) = \operatorname{sign}\left(\sum_{i=1}^{l} \alpha_i K(x_i, x) - \rho \right) \tag{3}$$

$$\min_{w,\xi,\rho} \ \frac{1}{2} \| w \|^2 + \frac{1}{\nu l} \sum_{i=1}^{l} \xi_i - \rho \tag{4}$$

where $K(\cdot)$ has represented the kernel function, α_i have denoted Lagrange multipliers, ρ_h as indicated the offset, and ν_h as controlled the fraction of outliers. The compact model representation has reduced circuit-level storage and computation requirements.

3.3 BIDIRECTIONAL SNOW GEESE OPTIMIZATION FOR PARAMETER TUNING

To further enhance energy efficiency, a bidirectional snow geese optimization algorithm has been employed for parameter tuning. This stage has optimized kernel parameters and monitoring thresholds with minimal iteration overhead. The migratory behavior of snow geese has inspired a balanced exploration–exploitation strategy that has converged rapidly.

Bidirectional movement has enabled both forward and backward search directions, which has prevented premature convergence and excessive iterations. As a result, the optimization process has required fewer computational cycles, which has translated into lower dynamic power consumption.

The optimization update process has been modeled as:

$$P_{t+1} = P_t + \alpha \cdot \left(G_{\text{best}} - P_t \right) + \beta \cdot \left(P_{\text{prev}} - P_t \right) \tag{5}$$

$$E_{\text{opt}} = \sum_{t=1}^{T} C_t \cdot V_t^2 \cdot f_t \tag{6}$$

where P_t is represented as parameter positions, G_{best} is denoted as the global best solution, α and β have controlled movement weights, and E_{opt} is indicated optimization energy consumption. The reduced T is reflected faster convergence.

4. ADAPTIVE SAMPLING

Continuous monitoring has been a critical requirement for industrial cybersecurity, yet it has been a major contributor to energy drain. To address this challenge, the proposed framework has introduced adaptive sampling mechanisms. Monitoring intensity has been adjusted based on real-time risk estimation.

Under stable operating conditions, the system has reduced sampling frequency, while suspicious patterns have triggered higher monitoring resolution. This adaptive behavior has ensured security responsiveness without maintaining constant high-power operation.

The adaptive sampling model has been expressed as:

$$f_s(t) = f_{\min} + \gamma \cdot R(t) \tag{7}$$

$$P_{\text{mon}}(t) = C \cdot V^2 \cdot f_s(t) \tag{8}$$

where $f_s(t)$ has denoted sampling frequency, $R(t)$ has represented estimated risk, and $P_{mon}(t)$ has indicated monitoring power consumption. The proportional adjustment has minimized unnecessary energy usage.

The final stage has focused on integrating green infrastructure principles directly into circuit operation. This stage has incorporated adaptive voltage scaling and low-leakage operational modes. Circuit components have transitioned between active, standby, and sleep states based on workload demand.

This dynamic behavior has reduced static and dynamic power losses, particularly during idle monitoring periods. The coordination between algorithmic decisions and hardware states has distinguished the proposed framework from conventional designs.

The circuit power model has been defined as:

$$P_{\text{total}} = P_{\text{dyn}} + P_{\text{leak}} = C \cdot V^2 \cdot f + I_{\text{leak}} \cdot V \tag{9}$$

$$E_{\text{total}} = \int_0^T P_{\text{total}}(t)\, dt \tag{10}$$

where P_{dyn} has represented dynamic power, P_{leak} is denoted leakage power, and E_{total} has indicated total energy consumption. The reduction in both components has validated the carbon-aware design.

5. RESULTS AND DISCUSSION

The experimental evaluation is conducted using a simulation-driven approach that reflects realistic industrial cybersecurity scenarios. The proposed OSV-BiSGA framework is implemented in a MATLAB R2023b environment, which supports numerical optimization, machine learning modeling, and energy analysis. The simulation tool is selected due to its stability and suitability for circuit-level algorithmic validation. All experiments are executed on a workstation that uses an Intel Core i9 processor with 64 GB RAM and a solid-state drive, which ensures consistent computational performance during repeated runs. The operating system is Windows 11 Pro, which provides a controlled execution environment. The simulation setup enables repeatable experiments, controlled parameter variation, and precise measurement of performance metrics. The present configuration supports continuous monitoring scenarios that reflect industrial operating conditions, while maintaining reproducibility and methodological transparency.

The experimental setup parameters that govern the proposed framework, which defines algorithmic, monitoring, and energy-related configurations. These parameters are selected based on prior industrial cybersecurity studies and preliminary tuning experiments.

Table.1. Experimental setup parameters and values

Parameter	Description	Value
Kernel type	One-class support vector kernel	Radial basis
Kernel width (σ)	Spread of decision boundary	0.5
ν parameter	Outlier control factor	0.1
BiSGA population size	Number of candidate solutions	30
Maximum iterations	Optimization convergence limit	50
Initial sampling	Monitoring rate	1 kHz

frequency		
Minimum sampling frequency	Energy-saving mode	200 Hz
Supply voltage	Circuit operating voltage	1.0 V
Capacitance	Effective switching capacitance	10 pF

Accuracy measures the proportion of correctly classified instances, which reflects the reliability of the detection model. Precision quantifies the proportion of detected anomalies that are true attacks, which reduces false alarms that burden industrial operators. Recall represents the ability of the system to detect actual intrusions, which is critical for safety-critical circuits. F1-score provides a harmonic balance between precision and recall, which ensures stable performance under class imbalance. Energy consumption measures the total energy used during monitoring and detection, which directly reflects alignment with carbon neutral objectives. These metrics collectively capture both cybersecurity performance and energy efficiency.

The comparative evaluation includes three existing methods that represent different design philosophies. Static One-Class SVM applies a fixed-parameter one-class classifier without adaptive optimization. PSO-Optimized IDS employs particle swarm optimization for tuning detection parameters with moderate energy awareness. Always-On Deep Learning IDS relies on continuous deep neural inference that emphasizes accuracy at the cost of high energy usage.

5.1 QUANTITATIVE RESULTS OVER POPULATION SIZE

The population size is increased up to 30, which corresponds to iterative optimization stages.

Table.2. Accuracy comparison over iterations

Iteration	Static One-Class SVM	PSO-Optimized IDS	Always-On DL IDS	Proposed OSV-BiSGA
1	0.78	0.81	0.84	0.86
7	0.80	0.84	0.87	0.90
13	0.82	0.86	0.89	0.92
19	0.83	0.87	0.90	0.94
25	0.84	0.88	0.91	0.95

Table.3. Precision comparison over iterations

Iteration	Static One-Class SVM	PSO-Optimized IDS	Always-On DL IDS	Proposed OSV-BiSGA
1	0.75	0.79	0.82	0.85
7	0.77	0.82	0.85	0.88
13	0.79	0.84	0.87	0.90
19	0.80	0.85	0.88	0.92
25	0.81	0.86	0.89	0.93

Table.4. Recall comparison over iterations

Iteration	Static One-Class SVM	PSO-Optimized IDS	Always-On DL IDS	Proposed OSV-BiSGA
1	0.76	0.80	0.83	0.85
7	0.78	0.83	0.86	0.89
13	0.80	0.85	0.88	0.91
19	0.81	0.86	0.89	0.93
25	0.82	0.87	0.90	0.94

Table.5. F1-score comparison over iterations

Iteration	Static One-Class SVM	PSO-Optimized IDS	Always-On DL IDS	Proposed OSV-BiSGA
1	0.75	0.80	0.82	0.85
7	0.77	0.83	0.85	0.89
13	0.79	0.85	0.88	0.91
19	0.80	0.86	0.89	0.93
25	0.81	0.87	0.90	0.94

Table.6. Energy consumption comparison (Joules)

Iteration	Static One-Class SVM	PSO-Optimized IDS	Always-On DL IDS	Proposed OSV-BiSGA
1	52	60	95	48
7	55	63	98	46
13	57	66	102	44
19	59	68	105	42
25	60	70	108	40

The results in Table.2-Table.6 demonstrate consistent performance improvements for the proposed OSV-BiSGA framework. Accuracy increases from 0.86 at iteration 1 to 0.95 at iteration 25, which exceeds the Static One-Class SVM by 11 percentage points and the PSO-Optimized IDS by 7 percentage points, as shown in Table.2. Precision and recall trends in Table.3 and Table.4 indicate balanced detection behavior, where precision reaches 0.93 and recall reaches 0.94 at the final iteration. This balance has directly improved the F1-score, which attains 0.94 in Table.5. Energy consumption results in Table.6 highlight the sustainability advantage of the proposed framework. While the Always-On Deep Learning IDS consumes up to 108 J, the proposed OSV-BiSGA consumes only 40 J at iteration 25, which corresponds to an energy reduction of approximately 63%. Even when compared with the Static One-Class SVM, the proposed method maintains lower energy usage due to adaptive sampling that reduces idle operation.

6. CONCLUSION

This study presents a carbon-aware cybersecurity framework for industrial circuits that integrates a one-class support vector mechanism with bidirectional snow geese optimization and green infrastructure principles. The proposed OSV-BiSGA framework simultaneously addresses intrusion detection reliability and energy efficiency, which remains a critical challenge in industrial cyber–physical systems. Quantitative evaluation demonstrates that the framework achieves high accuracy, precision, recall, and F1-score while substantially reducing energy consumption. The results confirm that adaptive monitoring which adjusts sampling intensity based on risk estimation reduces unnecessary power usage without degrading security. Optimization that converges rapidly limits computational overhead, which further supports carbon neutral goals. Compared with Static One-Class SVM, PSO-Optimized IDS, and Always-On Deep Learning IDS, the proposed framework delivers superior performance across all evaluated metrics. From a broader perspective, this work establishes that sustainability can be embedded directly into cybersecurity circuit design rather than treated as an external constraint. The proposed methodology provides a scalable foundation for future industrial security systems that must operate under strict energy and environmental constraints. As industries increasingly adopt green infrastructure, the presented framework offers a practical and effective pathway toward secure and carbon-efficient industrial applications.

REFERENCES

[1] T.S. Lawrence, M. Margala and P. Chakrabarti, "Cybersecurity Meets Carbon Neutrality: Strategies for Sustainable Data Center Security Operations", *Sustainable Computing: Informatics and Systems*, Vol. 49, pp. 1-6, 2025.

[2] M. Hakovirta, "Technology Platforms-Carbon Neutral Technologies", *Carbon Neutrality: Follow the Money*, pp. 65-104, 2024.

[3] Z. Hu and L. Zhou, "A Data-Driven Approach for Electric Energy Equipment using Wireless Sensing Technology in the Context of Carbon Neutrality", *Journal of Sensors*, Vol. 2022, No. 1, pp. 1-8, 2022.

[4] P. Kaushik and K.S. Kaswan, "Creating Resilient and Sustainable Businesses: New Ideas for Reducing Digital Carbon Footprints", *Metaverse and Sustainability: Business Resilience Towards Sustainable Development Goals*, pp. 283-303, 2025.

[5] T.I. Adeyinka and K.I. Adeyinka, "Reducing the Carbon Footprint in Healthcare Cybersecurity Threats in AI-Powered Healthcare Systems Data Privacy in AI-Driven Diagnostics", *AI-Driven Healthcare Cybersecurity and Privacy*, pp. 283-326, 2025.

[6] O. Inderwildi, C. Zhang, X. Wang and M. Kraft, "The Impact of Intelligent Cyber-Physical Systems on the Decarbonization of Energy", *Energy and Environmental Science*, Vol. 13, No. 3, pp. 744-771, 2020.

[7] A. Bhatt, W. Ongsakul and J. Pawar, "Optimal Energy Management System for Carbon-Neutral Microgrid Integrating Second-Life Batteries and Crypto Mining Devices", *Sustainable Energy Technologies and Assessments*, Vol. 64, pp. 1-6, 2024.

[8] N.E. Saber, M. Mohamed and N.M. AbdelAziz, "Decarbonization Transportation: Evaluating Role of Cyber Security in Transportation Sector based on Neutrosophic Techniques in a Climate of Uncertainty", *Neutrosophic Sets and Systems*, Vol. 60, No. 1, pp. 1-7, 2023.

[9] S. Bellary and A.H. Raghavendra, "Quantum Computing for a Sustainable Future: Transforming Energy Efficiency and Climate Solutions", *From Bits to Qubits: The Quantum Transformation of Computing: The Power of Quantum Computing*, pp. 55-76, 2026.

[10] R. Ganguly, P. Ganguly and T. Matharasi, "Sustainable Mobile and Wireless Computing Solutions", *Energy Efficient Algorithms and Green Data Centers for Sustainable Computing*, pp. 209-248, 2025.

[11] Y. Lu, S. Fang, G. Chen, T. Niu and R. Liao, "Cyber-Physical Integration for Future Green Seaports: Challenges, State of the Art and Future Prospects", *IEEE Transactions on Industrial Cyber-Physical Systems*, Vol. 1, pp. 21-43, 2023.

[12] H. Majeed and T. Iftikhar, "Industry 6.0 in Aerospace, Defense, Military and Automotive Smart Manufacturing", *Intelligent Manufacturing in Industry 6.0: A Climate Resilience Approach*, pp. 391-464, 2026.

[13] S. Kautish and D. Gurung, "Advancing Sustainable Computing: A Systematic Literature Review of Software, Hardware and Algorithmic Innovations", *ICCK Transactions on Sustainable Computing*, Vol. 1, No. 1, pp. 1-19, 2025.