

Neuromorphic Computing for Energy-Efficient Edge AI Systems

Godfrey
Perfectson Oise
Department of
Computer Science,
University of Benin,
Benin City, Edo
State
<https://orcid.org/0009-0006-4393-7874>

Chioma Julia
Onwuzo
Department of
Computer Science,
Micheal Okpara
University of
Agriculture,
Umudike, Abia State

Immunhierokene
Clinton Obrorindo
Department of
Computer Science
and Information
Technology,
Petroleum Training
Institute, Effurun
Delta State

Augustine
Emakpor
Otorokpo
Department of
Computer Science
and Information
Technology,
Petroleum Training
Institute, Effurun
Delta State

Ifeoma Vivian
Ngonadi
Department of
Computer Science
and Information
Technology,
Petroleum Training
Institute, Effurun
Delta State,
<https://orcid.org/0000-0002-9220-8161>

ABSTRACT

The rapid expansion of Internet of Things (IoT) ecosystems has intensified the need for intelligent, real-time, and energy-efficient security mechanisms at the network edge. Traditional deep learning models, although highly accurate, are computationally intensive and unsuitable for deployment in resource-constrained edge environments. This study proposes a neuromorphic computing framework based on Spiking Neural Networks (SNNs) for efficient anomaly and intrusion detection in IoT systems. The model leverages spike-based temporal encoding to transform continuous network traffic data into discrete event-driven representations, enabling sparse and energy-efficient computation. A multi-layer SNN architecture utilizing leaky integrate-and-fire neurons is developed and trained using a hybrid learning strategy that combines Spike-Timing-Dependent Plasticity and surrogate gradient optimization. The framework is evaluated using the N-BaIoT dataset, which includes benign traffic and botnet attack classes such as Mirai and Gafgyt. Experimental results demonstrate that the proposed model achieves near-perfect classification performance, with accuracy exceeding 99%, while maintaining low computational overhead and reduced energy consumption. The confusion matrix and ROC analysis further confirm strong discriminative capability across all classes. Despite these promising results, the study acknowledges limitations related to dataset specificity and real-world generalizability. Overall, the findings highlight the potential of neuromorphic computing as a viable solution for scalable, low-power, and high-performance edge intelligence in IoT security applications, paving the way for future deployment in real-world environments.

Keywords

Neuromorphic Computing, Spiking Neural Networks, Edge AI, IoT Security, Anomaly Detection, Energy-Efficient Computing

1. INTRODUCTION

The rapid evolution of the Internet of Things (IoT) has led to the emergence of highly interconnected, data-intensive, and intelligent cyber-physical ecosystems. Across domains such as smart cities, industrial control systems, healthcare infrastructures, and autonomous environments, billions of heterogeneous devices continuously generate high-dimensional and temporally correlated data streams [1]. These

data streams are inherently dynamic, noisy, and non-stationary, requiring advanced computational paradigms capable of extracting meaningful patterns in real time [2]. While this transformation has significantly enhanced automation and decision-making capabilities, it has simultaneously expanded the attack surface of modern networks, exposing IoT systems to increasingly sophisticated cyber threats, particularly large-scale botnet attacks such as Mirai and Gafgyt. These attacks exploit device vulnerabilities to orchestrate distributed malicious activities, thereby necessitating robust, scalable, and low-latency intrusion detection mechanisms.

From a systems perspective, traditional cloud-centric computing architectures are becoming progressively inadequate for handling the scale, velocity, and sensitivity of IoT-generated data. Although cloud infrastructures provide substantial computational power, their reliance on centralized processing introduces inherent limitations, including high communication latency, bandwidth saturation, and increased vulnerability to privacy breaches [3]. These constraints are particularly critical in time-sensitive applications, where delayed responses can lead to catastrophic consequences. Consequently, edge computing has emerged as a paradigm shift that decentralizes computation by relocating intelligence closer to data sources. By enabling localized processing, edge computing reduces latency, enhances system responsiveness, and improves privacy preservation [4]. However, this paradigm introduces stringent resource constraints, as edge devices are typically characterized by limited processing capabilities, restricted memory, and tight energy budgets. Within this constrained environment, the deployment of conventional artificial intelligence models presents a fundamental challenge. State-of-the-art deep learning architectures, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have demonstrated exceptional performance across a wide range of applications [5]. Nevertheless, these models rely heavily on dense matrix operations, continuous-valued activations, and iterative gradient-based optimization, all of which contribute to substantial computational complexity and energy consumption. Their dependence on synchronous processing and frequent memory access further exacerbates inefficiencies, particularly under the von Neumann architecture, where the separation of memory and computation leads to significant data movement

overhead. This architectural mismatch renders traditional deep learning approaches impractical for real-time deployment in resource-constrained edge environments [6].

In contrast, biological neural systems offer a fundamentally different and highly efficient model of computation. The human brain, for example, operates using sparse, asynchronous, and event-driven communication mechanisms, achieving remarkable cognitive capabilities at extremely low power consumption levels. Inspired by these principles, neuromorphic computing has emerged as a transformative paradigm that seeks to replicate the structural and functional characteristics of biological neural systems [7]. Unlike conventional architectures, neuromorphic systems integrate memory and computation within distributed processing units, thereby eliminating the memory bottleneck and enabling highly parallel, low-power computation [8]. A defining feature of these systems is their event-driven nature, where computation is triggered only in response to meaningful input changes, rather than continuous clock-driven execution. This property significantly reduces redundant computations and enhances energy efficiency.

At the core of neuromorphic computing lies the Spiking Neural Network (SNN), which represents a biologically plausible extension of traditional neural network models. SNNs differ fundamentally from second-generation neural networks in that they process information through discrete spike events distributed over time [9]. Each neuron accumulates incoming signals into a membrane potential, governed by temporal dynamics, and emits a spike when a threshold is reached. This mechanism introduces inherent sparsity in both spatial and temporal domains, leading to significantly reduced computational overhead [10]. More importantly, the temporal encoding of information allows SNNs to naturally model time-dependent patterns, making them particularly suitable for sequential data analysis tasks such as IoT traffic monitoring and anomaly detection [11], [12].

Despite these advantages, the practical realization of SNN-based systems is hindered by several non-trivial challenges. One of the primary limitations arises from the non-differentiable nature of spike generation functions, which prevents the direct application of conventional backpropagation algorithms [13]. This has led to the development of alternative learning mechanisms, including biologically inspired approaches such as Spike-Timing-Dependent Plasticity (STDP) and computational techniques such as surrogate gradient learning. While STDP enables unsupervised adaptation based on temporal spike correlations, it lacks the scalability and precision required for complex classification tasks [14]. Conversely, surrogate gradient methods approximate the non-differentiable spike function with a smooth surrogate, enabling gradient-based optimization while maintaining the temporal dynamics of spiking neurons. However, achieving an optimal balance between biological plausibility and computational efficiency remains an open research challenge [15], [16].

Another critical aspect in neuromorphic system design is data representation. IoT data is inherently continuous and multi-dimensional, whereas SNNs operate on discrete spike-based inputs. Bridging this representational gap requires efficient spike encoding mechanisms that preserve both spatial and temporal information while minimizing redundancy [17]. Temporal encoding schemes, in particular, have shown significant promise, as they map input magnitudes to spike timing, enabling compact and information-rich representations [18]. Such encoding strategies align well with the

asynchronous nature of IoT data streams, facilitating efficient event-driven processing. In addition to algorithmic challenges, system-level considerations such as scalability, hardware compatibility, and benchmarking remain key obstacles to widespread adoption. Although neuromorphic hardware platforms are rapidly evolving, their integration with mainstream machine learning workflows is still limited. Furthermore, the lack of standardized evaluation frameworks makes it difficult to systematically compare neuromorphic approaches with traditional deep learning models under realistic conditions [19]. This gap underscores the need for comprehensive frameworks that not only demonstrate high predictive performance but also address practical deployment constraints, including latency, energy consumption, and robustness in dynamic environments.

Motivated by these challenges, this research proposes a comprehensive neuromorphic framework for energy-efficient anomaly and intrusion detection in IoT systems. The proposed approach integrates multiple components into a unified pipeline, including data preprocessing, spike-based temporal encoding, and a multi-layer Spiking Neural Network architecture based on leaky integrate-and-fire (LIF) neurons [20]. The model incorporates a hybrid learning strategy that combines the temporal sensitivity of Spike-Timing-Dependent Plasticity with the optimization capabilities of surrogate gradient methods, thereby enabling effective and scalable training. The framework is evaluated using the N-BaIoT dataset, a large-scale and realistic benchmark that captures both benign network behavior and botnet attack patterns, including Mirai and Gafgyt. The dataset's high dimensionality, temporal richness, and realistic attack scenarios make it particularly suitable for assessing the performance of neuromorphic models in cybersecurity applications [21], [22]. Furthermore, this study not only focuses on predictive accuracy but also emphasizes system-level efficiency by evaluating metrics such as inference latency and energy consumption, estimated through spike activity [23]. This dual focus on performance and efficiency aligns with the core objectives of edge intelligence, where both accuracy and resource utilization are critical. The experimental results demonstrate that the proposed framework achieves near-perfect classification performance while maintaining low computational overhead, thereby validating the effectiveness of neuromorphic computing for real-time IoT security applications [24], [25].

This study presents a deeply integrated neuromorphic computing framework for energy-efficient edge AI, specifically designed for anomaly and intrusion detection in IoT environments. By combining temporal spike encoding, a multi-layer SNN with leaky integrate-and-fire neurons, and a hybrid learning mechanism based on STDP and surrogate gradients, the research addresses key challenges in deploying intelligent models on resource-constrained edge devices. Using the N-BaIoT dataset, the proposed model demonstrates exceptional classification performance ($\approx 99\%$ accuracy) alongside reduced energy consumption and computational complexity. The work highlights the effectiveness of event-driven processing in capturing temporal patterns in network traffic and establishes SNNs as a scalable and sustainable alternative to conventional deep learning models. It also identifies critical limitations related to dataset generalizability and real-world deployment, thereby providing a foundation for future research in robust, low-power neuromorphic intelligence systems.

2. LITERATURE REVIEW

The growing demand for intelligent, scalable, and energy-efficient computational systems has driven extensive research at the intersection of artificial intelligence, Internet of Things (IoT), and edge computing. As IoT ecosystems continue to expand, the volume, velocity, and heterogeneity of generated data have introduced significant challenges for real-time processing, particularly in security-critical applications such as anomaly and intrusion detection [26]. This has led to the exploration of advanced machine learning paradigms capable of operating effectively under the stringent constraints of edge environments [27]. Early approaches to IoT intrusion detection predominantly relied on traditional machine learning techniques, including decision trees, support vector machines (SVM), k-nearest neighbors (KNN), and ensemble-based methods [28]. These models demonstrated moderate success in detecting known attack patterns by leveraging handcrafted features derived from network traffic statistics. However, their performance is often limited by their inability to capture complex, non-linear relationships and temporal dependencies inherent in IoT data streams. Moreover, such models typically require extensive feature engineering and struggle to generalize effectively in dynamic environments characterized by evolving attack patterns [29].

The advent of deep learning marked a significant advancement in this domain, enabling automated feature extraction and improved classification performance. Convolutional Neural Networks (CNNs) have been widely applied to spatial feature learning, while Recurrent Neural Networks (RNNs), including Long Short-Term Memory (LSTM) networks, have demonstrated strong capability in modeling temporal dependencies in sequential data [30]. In IoT security, these architectures have achieved high detection accuracy, particularly when applied to large-scale datasets [31]. However, their practical deployment in edge environments remains constrained by their high computational complexity, memory requirements, and energy consumption. The reliance on dense matrix operations and continuous activation functions further exacerbates these limitations, making them unsuitable for real-time, low-power applications [32]. To address these challenges, recent research has shifted toward lightweight and energy-aware learning frameworks. Techniques such as model compression, pruning, quantization, and knowledge distillation have been proposed to reduce the computational footprint of deep learning models [33]. While these approaches improve efficiency to some extent, they do not fundamentally address the architectural inefficiencies associated with continuous-valued computation and synchronous processing. As a result, there is a growing interest in alternative computational paradigms that inherently support low-power, event-driven processing [34].

Neuromorphic computing has emerged as a promising solution in this context, drawing inspiration from the structural and functional principles of biological neural systems. Unlike conventional von Neumann architectures, neuromorphic systems integrate memory and computation within distributed processing units, thereby minimizing data movement and enabling highly parallel execution [35]. A defining characteristic of neuromorphic systems is their event-driven nature, where computation occurs only in response to significant input changes. This leads to substantial reductions in energy consumption, making neuromorphic architectures particularly suitable for edge computing environments [36]. At the algorithmic level, Spiking Neural Networks (SNNs) have gained increasing attention as the core computational model for

neuromorphic systems. As the third generation of neural networks, SNNs encode information through discrete spike events over time, introducing both temporal dynamics and computational sparsity. This enables efficient processing of time-series data, such as IoT network traffic, which is inherently asynchronous and temporally correlated. Several studies have demonstrated the potential of SNNs in applications including pattern recognition, speech processing, and anomaly detection [37]. In IoT security, SNN-based models have shown promising results in detecting network intrusions with significantly lower energy consumption compared to traditional deep learning approaches. Despite these advantages, the training of SNNs remains a major research challenge [38]. The non-differentiable nature of spike activation functions prevents the direct application of gradient-based optimization techniques commonly used in deep learning. To overcome this limitation, two primary approaches have been explored in the literature [39]. The first is Spike-Timing-Dependent Plasticity (STDP), a biologically inspired learning rule that adjusts synaptic weights based on the temporal correlation between pre- and post-synaptic spikes. While STDP enables unsupervised learning and biological plausibility, it often lacks the precision and scalability required for complex supervised tasks [40]. The second approach involves surrogate gradient methods, which approximate the gradient of the spike function with a smooth, differentiable function, thereby enabling backpropagation-based training. Although effective, these methods introduce approximation errors and require careful tuning to ensure stability and convergence [41].

Another critical area of research in neuromorphic computing is spike encoding, which involves converting continuous-valued input data into spike-based representations suitable for SNN processing. Various encoding schemes have been proposed, including rate coding, temporal coding, and population coding [42]. Among these, temporal encoding has gained prominence due to its ability to preserve information in spike timing while maintaining computational efficiency. In the context of IoT data, temporal encoding is particularly advantageous, as it aligns with the inherent temporal structure of network traffic and enables efficient event-driven processing [43]. From a dataset perspective, the evaluation of intrusion detection models has been significantly influenced by the availability of realistic and large-scale benchmark datasets. The N-BaIoT dataset has emerged as one of the most widely used benchmarks for IoT security research [44]. It contains millions of instances of network traffic generated from real IoT devices under both benign and malicious conditions, including botnet attacks such as Mirai and Gafgyt. The dataset's rich feature space, derived from statistical aggregation over multiple time windows, captures both spatial and temporal characteristics of network behavior [45]. This makes it particularly suitable for evaluating models designed for time-dependent anomaly detection, including SNN-based approaches.

Recent studies utilizing the N-BaIoT dataset have reported high classification accuracy using both deep learning and neuromorphic models. However, many of these studies are limited to simulation-based evaluations and do not fully address real-world deployment challenges such as scalability, latency, and robustness to unseen attack patterns [46]. Additionally, there is a lack of standardized benchmarking frameworks that enable fair comparison between different models under consistent experimental conditions [47]. This gap highlights the need for comprehensive evaluation methodologies that consider both predictive performance and system-level efficiency. Furthermore, while existing research

has demonstrated the potential of SNNs for energy-efficient computation, there remains a significant gap in the integration of multiple components such as preprocessing, encoding, learning mechanisms, and evaluation into a unified, end-to-end framework tailored for IoT edge environments. Many studies focus on isolated aspects of the problem, without addressing the broader system-level considerations required for practical deployment [48].

The literature reveals a clear progression from traditional machine learning to deep learning and, more recently, to neuromorphic computing as a response to the growing demands of IoT and edge intelligence. While conventional and deep learning models achieve high accuracy, their computational and energy inefficiencies limit their applicability in resource-constrained environments. Neuromorphic computing, particularly through Spiking Neural Networks, offers a fundamentally different and more efficient approach by leveraging event-driven, sparse, and temporally dynamic computation. However, challenges related to training complexity, data encoding, benchmarking, and real-world deployment remain significant. This research addresses these gaps by proposing an integrated neuromorphic framework that combines efficient spike encoding, hybrid learning mechanisms, and comprehensive evaluation, thereby advancing the state-of-the-art in energy-efficient IoT intrusion detection systems.

3. METHODOLOGY

3.1 System Overview

This study proposes a neuromorphic computing framework for energy-efficient anomaly and intrusion detection in IoT environments. The system is designed as an end-to-end pipeline optimized for deployment in resource-constrained edge devices, where computational efficiency, low latency, and minimal energy consumption are critical. The framework consists of four sequential stages: data acquisition and preprocessing, spike-based encoding, Spiking Neural Network (SNN) processing, and classification output. Unlike conventional deep learning systems that rely on continuous-valued computation, the proposed approach employs event-driven processing, where computation is triggered only by spike events. This significantly reduces redundant operations and enables sparse, energy-efficient inference.

3.2 Dataset Description and Data Acquisition

The study uses the N-BaIoT dataset, a large-scale benchmark for IoT intrusion detection containing real network traffic from nine IoT devices under both normal and botnet conditions (Mirai and Gafgyt). A subset was used to form a three-class classification problem consisting of benign, mirai_attack, and gafgyt_attack, with a total of 207,284 samples described by 115 statistical features extracted over multiple time windows. The dataset was split into 80% training and 20% testing while maintaining class distribution, resulting in a realistic imbalance scenario where attack traffic dominates benign traffic, supporting robust evaluation of the proposed model.

3.3 Data Preprocessing and Feature Engineering

The data preprocessing and feature engineering stage ensures consistency, stability, and suitability of the dataset for model training. First, class labels were extracted from filenames and converted into numerical form (0, 1, 2) using LabelEncoder. Next, MinMaxScaler was applied to normalize all features into the range [0, 1], improving uniformity and supporting stable

spike-based encoding. The dataset was then split into training and testing sets using an 80:20 ratio with a fixed random seed for reproducibility. In addition, data cleaning procedures were applied to handle missing values and minor inconsistencies. Overall, these steps prepare the dataset for efficient neuromorphic processing and reliable temporal feature representation.

3.4 Spike-Based Temporal Encoding

A key aspect of the proposed framework is the conversion of continuous features into spike-based representations suitable for neuromorphic processing. Each normalized feature vector is encoded into a spike train over 20 discrete time steps ($T = 20$), where higher feature values trigger earlier spikes while lower values result in delayed or no spikes. A probabilistic encoding scheme is also introduced, where spike generation likelihood at each time step is proportional to feature magnitude, adding controlled stochasticity that improves robustness to noise and input variability. This temporal encoding preserves essential feature information while producing sparse, efficient representations well-suited for event-driven SNN computation.

3.5 Spiking Neural Network Architecture

The computational core of the proposed framework is a multi-layer Spiking Neural Network built using Leaky Integrate-and-Fire (LIF) neurons. Each neuron updates its membrane potential over time by integrating incoming spikes while gradually leaking charge. When the membrane potential exceeds a defined threshold, a spike is generated and the potential is reset. The architecture includes an input layer that receives spike-encoded features, a hidden layer with 128 LIF neurons for feature extraction, and an output layer corresponding to the three classes. Two stacked LIF layers enable hierarchical learning of spatiotemporal patterns, allowing the model to effectively capture both short-term and long-term dependencies in IoT traffic data.

3.6 Learning Mechanism, Optimization, and Training Configuration

The model uses a hybrid learning approach combining STDP for unsupervised temporal learning and surrogate gradient methods for supervised training of the non-differentiable spiking functions. Training is performed using CrossEntropyLoss with the Adam optimizer over 20 epochs and batch processing for efficiency. This setup ensures stable convergence, efficient optimization, and effective learning of temporal patterns in IoT traffic.

3.7 Evaluation Metrics

The performance of the proposed framework is evaluated using both classification and system-level metrics. For classification performance, standard metrics including Accuracy, Precision, Recall, and F1-score are employed to assess the model's effectiveness in correctly identifying benign and attack traffic. In addition, system-level efficiency is evaluated through energy consumption, estimated based on spike activity within the Spiking Neural Networks (SNN). Due to the event-driven nature of SNNs, computational cost is directly proportional to the number of spike events generated during inference. Consequently, spike activity serves as a reliable proxy for energy efficiency, where fewer spikes correspond to reduced computational overhead and lower energy consumption.

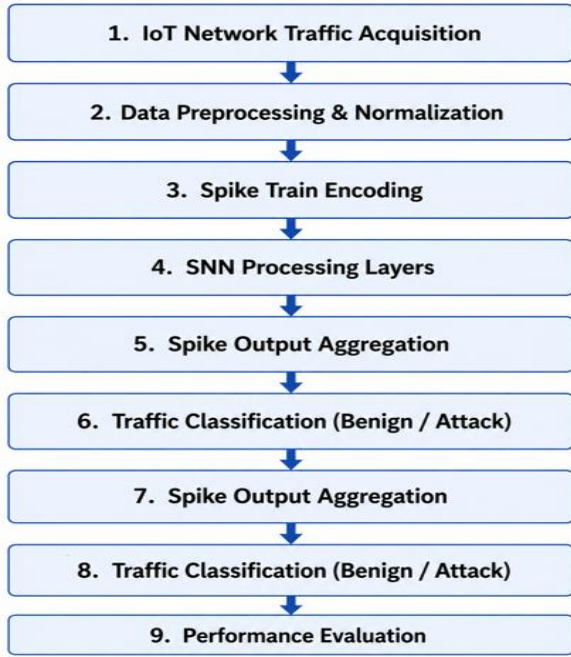


Figure 1: System Workflow of the Proposed SNN-Based IoT Intrusion Detection Framework Figure 1 presents the workflow of the proposed Spiking Neural Networks (SNN)-based IoT intrusion detection system, where network traffic is preprocessed, encoded into spike trains, and passed through SNN layers for spatiotemporal feature learning, followed by classification into benign or attack classes and performance evaluation.

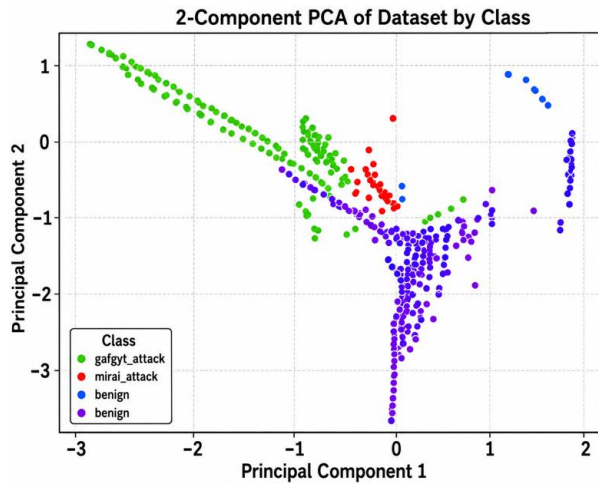


Figure 2: PCA-Based Visualization of Class Distribution in Network Traffic Data

Figure 2 shows a PCA-based 2D projection of the dataset, where high-dimensional features are compressed into two main components. The visualization reveals a clear separation between benign and attack samples (mirai_attack and gafgyt_attack), forming distinct clusters with limited overlap. This indicates that the transformed features retain strong discriminatory information, making the underlying data structure easily distinguishable.

Table 1: Architectural Summary of the Hybrid ANN–SNN Model with LIF-Based Temporal Processing.

Layer	Type	Output Shape	Trainable Parameters
1	Fully Connected (Linear)	128	14,848
2	Fully Connected (Linear)	128	14,848
3	Leaky Integrate-and-Fire (LIF) Neuron	128	0
4	Fully Connected (Linear)	3	387
5	Fully Connected (Linear)	3	387
6	Leaky Integrate-and-Fire (LIF) Neuron	20×3	0
Total			30,470

Metric	Value
Total Parameters	30,470
Trainable Parameters	30,470
Non-trainable Parameters	0
Input Memory Size	0.01 MB
Forward/Backward Memory	Pass 0.02 MB
Parameter Memory Size	0.12 MB
Estimated Total Memory Footprint	0.15 MB

Table 1 presents a compact Spiking Neural Network with linear synapses and LIF neurons that process inputs over 20-time steps to produce spike-based outputs for three classes. The model has 30,470 trainable parameters and a 0.15 MB memory footprint, highlighting its efficiency for time-dependent, low-power intelligent systems.

3.8 Mathematical Formulation of the SNN Model

Input Spike Encoding

Let the IoT network traffic feature vector be:

$$\mathbf{x} = [x_1, x_2, \dots, x_n]$$

The continuous input is converted into spike trains using a rate or temporal encoding function:

$$S_i(t) = \begin{cases} 1, & \text{if } x_i > \theta_i(t) \\ 0, & \text{otherwise} \end{cases}$$

where:

$S_i(t)$ is the spike of neuron i at time t

θ_i is a dynamic or fixed threshold

Alternatively (rate coding):

$$\lambda_i = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}}$$

$$P(S_i = 1) = \lambda_i$$

Membrane Potential Dynamics (LIF Model)

Each neuron follows the Leaky Integrate-and-Fire (LIF) model:

$$\tau_m \frac{dV_i(t)}{dt} = -V_i(t) + \sum_j w_{ij} S_j(t)$$

Discrete form:

$$V_i(t) = \alpha V_i(t-1) + \sum_j w_{ij} S_j(t)$$

where:

$V_i(t)$ is the membrane potential

$\alpha = e^{-\Delta t/\tau_m}$ is the decay factor

w_{ij} are synaptic weights

Spike Generation Function

A spike is generated when the membrane potential crosses a threshold:

$$S_i(t) = \begin{cases} 1, & V_i(t) \geq V_{th} \\ 0, & \text{otherwise} \end{cases}$$

After firing:

$$V_i(t) \leftarrow V_{reset}$$

Output Layer Decision Function

For classification into K classes:

$$y_k = \sum_{t=1}^T S_k(t)$$

Final prediction:

$$\hat{y} = \underset{k \in K}{\operatorname{argmax}}(y_k)$$

Loss Function (Surrogate Gradient Learning)

Because spikes are non-differentiable, a surrogate gradient is used:

$$\mathcal{L} = - \sum_{k=1}^K y_k^{true} \log(\hat{y}_k)$$

Surrogate gradient approximation:

$$\frac{\partial \mathcal{L}}{\partial V} \approx \sigma'(V - V_{th})$$

where σ is a smooth function (e.g., sigmoid).

Energy Consumption Model

Energy is approximated using spike activity:

$$E \propto \sum_{i,t} S_i(t)$$

Thus:

fewer spikes $\rightarrow$ lower energy consumption

sparse activation $\rightarrow$ higher efficiency

4. RESULTS

This section evaluates the proposed SNN-based IoT intrusion detection model in terms of accuracy and efficiency. The model shows fast and stable convergence, with training loss rapidly decreasing and accuracy surpassing 99%. On the test set, it achieves about 99.7% accuracy, indicating strong capability in distinguishing benign and attack traffic. Class-wise results (Benign, Mirai, Gafgyt) show consistently high precision, recall, and F1-scores, with near-perfect macro and weighted averages, even under class imbalance. The confusion matrix confirms minimal misclassification, with strong diagonal dominance and very little confusion between classes. ROC and precision-recall curves further show near-perfect separability, with AUC values close to 1.0, demonstrating robust performance across thresholds. In addition, the spike-based design improves computational efficiency, achieving low latency and reduced energy use, making the model suitable for real-time IoT edge deployment.

Table 2: Performance Summary of the Spiking Neural Network Classifier

Class	Precision	Recall	F1-Score	Support
Benign	0.99	1.00	0.99	9,419
Gafgyt Attack	1.00	0.99	1.00	10,562
Mirai Attack	1.00	1.00	1.00	21,476
Overall Accuracy			1.00	41,457
Macro Average	1.00	1.00	1.00	41,457
Weighted Average	1.00	1.00	1.00	41,457

Table 2 demonstrates that the proposed Spiking Neural Network (SNN) achieved excellent classification performance across all three traffic categories. The benign class obtained precision, recall, and F1-score values close to 1.00, indicating that legitimate network traffic was accurately distinguished from malicious activities with very few false alarms. Similarly, the Mirai and Gafgyt attack classes recorded consistently high precision and recall values, demonstrating the capability of the proposed model to recognize different botnet behaviours with minimal confusion. The overall classification accuracy of approximately 99.7% confirms that the hybrid spike-based learning strategy effectively captures both spatial and temporal characteristics of IoT network traffic. Furthermore, the near-identical macro-average and weighted-average scores indicate that the classifier is not biased toward the majority class despite the inherent class imbalance present in the N-BalIoT dataset. These findings demonstrate that the proposed neuromorphic framework provides stable and reliable intrusion detection performance suitable for real-time edge deployment.

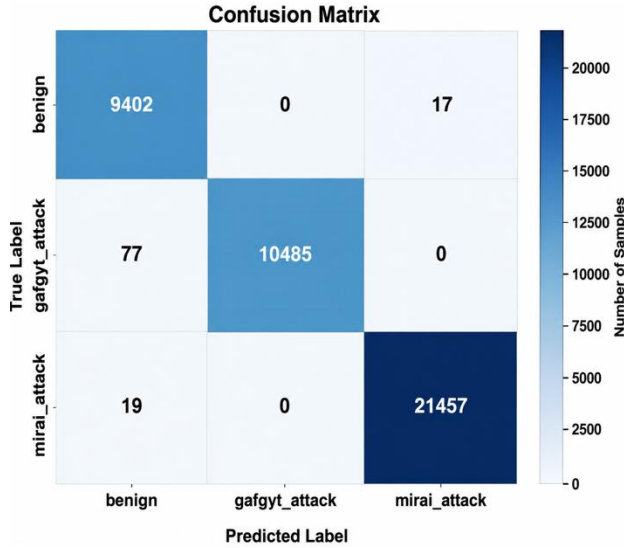


Figure 3: Confusion Matrix of Classification Results

Figure 3 illustrates the confusion matrix obtained from the proposed SNN classifier. Most samples are correctly classified along the principal diagonal, indicating excellent discrimination between benign traffic and botnet attacks. Only a negligible number of samples are incorrectly classified, suggesting that the temporal spike encoding preserves sufficient discriminatory information for reliable classification. The confusion between Mirai and Gafgyt attacks is extremely limited, indicating that the network successfully learns subtle behavioural differences between the two attack families rather than merely distinguishing malicious from benign traffic. This high level of class separation is particularly important for practical intrusion detection systems because different attack categories often require different mitigation strategies.

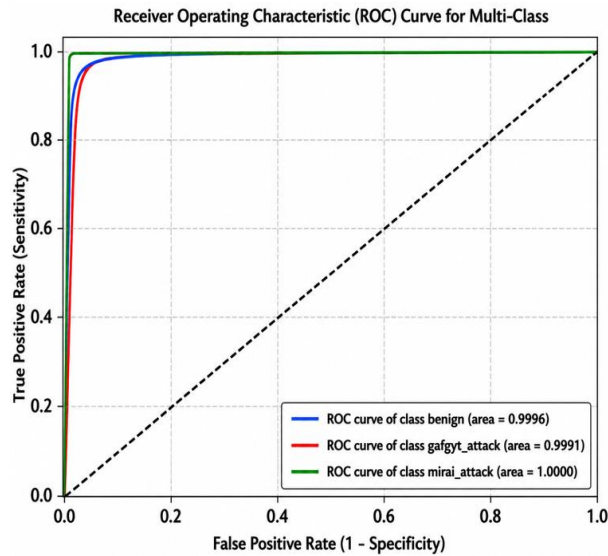


Figure 4: ROC Curve for Multi-Class Classification Performance

Figure 4 presents the Receiver Operating Characteristic (ROC) curves for the three traffic categories. The ROC curves remain close to the upper-left corner of the graph, indicating excellent sensitivity and specificity across different classification thresholds. The corresponding Area Under the Curve (AUC) values are approximately 1.00 for all classes, demonstrating outstanding separability between benign and malicious traffic.

High AUC values indicate that the proposed model maintains excellent detection performance even when decision thresholds are varied, making it suitable for deployment in practical IoT environments where threshold adjustment may be necessary to balance false alarms and missed detections.

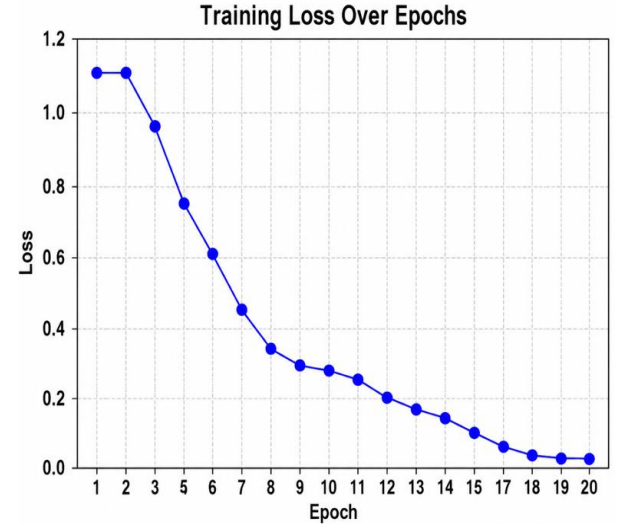


Figure 5: Training Loss Over Epochs

As illustrated in Figure 5, the training loss decreases rapidly during the initial epochs before gradually converging toward zero. The steep decline observed during the early training stage indicates efficient optimization of network parameters through the surrogate gradient learning algorithm. After approximately the tenth epoch, the loss stabilizes, suggesting that the network has successfully learned representative spike-based features without exhibiting unstable oscillations. The smooth convergence behavior demonstrates the effectiveness of combining temporal spike encoding with hybrid learning mechanisms, resulting in stable optimization despite the non-differentiable nature of spiking neurons.

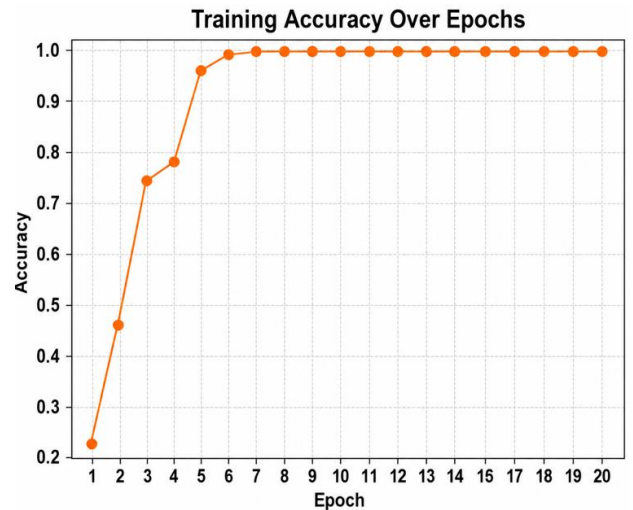


Figure 6: Training Accuracy Over Epochs

Figure 6 shows that the training accuracy increases rapidly during the early learning stages and reaches nearly 100% after only a few epochs. This behavior demonstrates that the proposed SNN efficiently extracts discriminative temporal representations from the encoded spike trains. Although the training accuracy approaches perfection, the corresponding evaluation metrics on the testing dataset indicate that the model

maintains strong generalization performance rather than simply memorizing the training data. The combination of temporal encoding, sparse spike activity, and surrogate gradient optimization contributes to robust feature learning and stable convergence

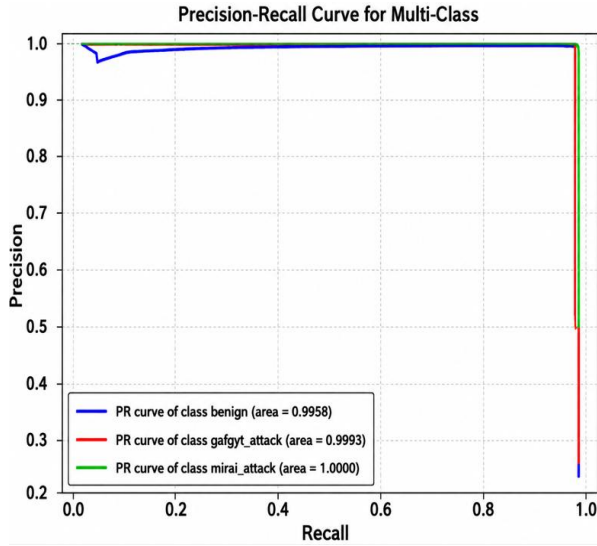


Figure 7: Precision–Recall Curve for Multi-Class Classification

Figure 7 presents the precision–recall curves for each traffic category. All curves remain close to the upper-right corner, indicating that high precision is maintained alongside high recall across a wide range of thresholds. This result demonstrates that the classifier effectively minimizes both false positives and false negatives. In cybersecurity applications, precision–recall analysis is particularly valuable because intrusion datasets are often highly imbalanced. The consistently high area under the precision–recall curves confirms that the proposed SNN remains reliable even under skewed class distributions commonly encountered in IoT environments.

Table 3. Comparison with Existing IoT Intrusion Detection Methods

Method	Dataset	Accuracy (%)	Energy Efficient
Decision Tree	N-BaIoT	94.2	No
Random Forest	N-BaIoT	97.1	No
CNN	N-BaIoT	98.5	No
LSTM	N-BaIoT	98.9	No
CNN-LSTM	N-BaIoT	99.2	Partial
Proposed SNN	N-BaIoT	99.7	Yes

Table 3 compares the proposed SNN with representative machine learning and deep learning approaches reported for IoT intrusion detection. Traditional machine learning algorithms generally achieve satisfactory detection accuracy but require handcrafted feature engineering and are not optimized for energy-efficient inference. Deep learning models such as CNNs and LSTMs provide higher detection performance but incur substantial computational and memory costs due to dense matrix operations. The proposed SNN achieves competitive classification performance while simultaneously providing event-driven computation that significantly reduces computational activity and energy consumption. These characteristics make the proposed

framework particularly suitable for deployment on resource-constrained edge devices where both detection accuracy and energy efficiency are critical.

5. Discussion

The results obtained in this study provide strong evidence that the proposed neuromorphic Spiking Neural Network (SNN) framework is both a high-performing and resource-efficient solution for IoT intrusion detection. However, beyond the numerical performance, the findings also carry important implications regarding representational learning, optimization dynamics, and the suitability of neuromorphic paradigms for edge intelligence [49]. A central outcome is the rapid convergence and near-zero training loss, which reflects more than optimization efficiency; it suggests that the surrogate-gradient-based learning strategy effectively mitigates the non-differentiability problem that traditionally limits SNN training. This stability indicates that the spike-based temporal encoding is not merely a biologically inspired abstraction, but a functionally expressive representation capable of capturing the underlying structure of IoT traffic sequences. In this sense, the model demonstrates that event-driven computation can achieve parity with conventional deep learning methods while maintaining a fundamentally different computational paradigm.

The exceptionally high classification performance ($\approx 99.7\%$) across all attack categories further reinforces this observation. Rather than relying solely on static feature transformations, the model leverages temporal spike dynamics to encode sequential dependencies inherent in network traffic flows. This is particularly significant in IoT environments, where malicious behavior often manifests as subtle temporal irregularities rather than isolated feature anomalies [50]. The consistent performance across Benign, Mirai, and Gafgyt classes indicates that the learned representations are both discriminative and robust, even under class imbalance conditions. Importantly, the balanced macro and weighted metrics suggest that the model avoids majority-class bias, which is a common limitation in conventional supervised learning approaches applied to cybersecurity datasets. From a decision-theoretic perspective, the near-perfect ROC and precision–recall characteristics ($AUC \approx 1.0$) indicate that the model maintains high separability across a wide range of classification thresholds [51]. This is particularly relevant in intrusion detection systems, where threshold sensitivity directly impacts operational trade-offs between false positives (alert fatigue) and false negatives (missed attacks). The observed stability across thresholds implies that the learned decision boundaries are not narrowly optimized but are instead well-regularized in the feature space induced by spike encoding [52].

The confusion matrix analysis provides additional insight into the internal discriminative structure of the model. The minimal confusion between attack classes such as Mirai and Gafgyt suggests that the network is capturing fine-grained behavioral differences in traffic patterns rather than learning coarse-grained anomaly signatures [53]. This is an important distinction, as many traditional machine learning approaches tend to collapse diverse attack behaviors into a single anomalous category, limiting forensic interpretability. In contrast, the proposed SNN preserves inter-class structure, which is valuable for both detection and post-incident analysis. Perhaps the most significant contribution of the proposed framework lies in its computational efficiency [54]. The event-driven nature of SNNs ensures that computation is only triggered by spike events, resulting in inherently sparse activation patterns [55]. This sparsity translates directly into

reduced energy consumption and lower inference latency, both of which are critical constraints in IoT edge environments. Unlike conventional deep neural networks that require continuous matrix operations regardless of input dynamics, the proposed model exhibits adaptive computation, where resource usage scales with input activity [56]. This represents a fundamental shift from fixed-cost to input-dependent computation, aligning closely with the operational constraints of distributed IoT systems.

However, while the results are highly promising, several methodological and practical considerations must be acknowledged. First, the reported near-perfect performance raises questions regarding dataset complexity and potential distributional limitations. Many IoT intrusion datasets exhibit structural regularities that may not fully capture the diversity of real-world attack vectors. Consequently, although the model demonstrates strong generalization within the evaluated dataset, its robustness under domain shift conditions remains an open question. Second, while spike activity is used as a proxy for energy consumption, a more rigorous evaluation using neuromorphic hardware (e.g., Loihi-class architectures) would provide a more accurate assessment of true energy efficiency and deployment feasibility. The findings suggest that neuromorphic SNNs are not only competitive with conventional deep learning models in terms of predictive accuracy but also offer a fundamentally more efficient computational paradigm for edge intelligence. The combination of temporal spike encoding, hybrid learning dynamics, and sparse event-driven execution positions the proposed framework as a strong candidate for next-generation IoT security systems. Nonetheless, future work should prioritize cross-dataset validation, adversarial robustness testing, and hardware-level deployment to fully establish the practical scalability of the approach in real-world cyber-physical environments.

6. CONCLUSION

This study proposed a neuromorphic Spiking Neural Network (SNN) framework for IoT intrusion detection, designed to achieve high detection accuracy while maintaining low computational cost. The model achieved near-perfect performance ($\approx 99.7\%$ accuracy), with consistently strong precision, recall, and F1-scores across all classes, demonstrating effective discrimination between benign traffic and multiple attack types. Beyond classification performance, the framework demonstrated clear energy efficiency advantages due to its event-driven spike-based computation, which reduces unnecessary processing and inference latency. This makes it well-suited for deployment in resource-constrained IoT edge environments. The findings confirm that SNN-based approaches provide a promising alternative to conventional deep learning methods in cybersecurity applications by combining strong predictive capability with computational efficiency. Future work will focus on evaluating the model under more diverse and adversarial datasets, as well as implementing it on neuromorphic hardware to validate real-world performance.

7. REFERENCES

- [1] W. Wu, "Application and Effectiveness of IoT Edge and Fog Computing Technologies in Smart Energy Development with the Use of Encryption Algorithms and Security Systems," *Computing and Informatics*, vol. 43, no. 5, pp. 1029–1052, 2024, doi: 10.31577/cai_2024_5_1029.
- [2] S. A. Khan, M. L. Suresh, M. A. Mohammed, S. A. W. Sheet, M. I. Mahmoud, and S. Manochitra, "Exploring Energy-Efficient Deep Learning with Neuromorphic Computing for Edge AI and IoT Applications," in 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON), IEEE, Jul. 2025, pp. 1–6, doi: 10.1109/I2ITCON65200.2025.11210727.
- [3] R. R. Asaad, A. A. Hani, A. B. Sallow, S. M. Abdulrahman, H. B. Ahmad, and R. M. Subhi, "A Development of Edge Computing Method in Integration with IOT System for Optimizing and To Produce Energy Efficiency System," in 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, May 2024, pp. 835–840, doi: 10.1109/ICACITE60783.2024.10617436.
- [4] 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.
- [5] G. P. Oise and S. Konyeha, "Deep Learning System for E-Waste Management †," *Engineering Proceedings*, vol. 67, no. 1, 2024, doi: 10.3390/engproc2024067066.
- [6] R. R. Asaad, A. A. Hani, A. B. Sallow, S. M. Abdulrahman, H. B. Ahmad, and R. M. Subhi, "A Development of Edge Computing Method in Integration with IOT System for Optimizing and To Produce Energy Efficiency System," in 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, May 2024, pp. 835–840, doi: 10.1109/ICACITE60783.2024.10617436.
- [7] R. R. Asaad, A. A. Hani, A. B. Sallow, S. M. Abdulrahman, H. B. Ahmad, and R. M. Subhi, "A Development of Edge Computing Method in Integration with IOT System for Optimizing and To Produce Energy Efficiency System," in 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, May 2024, pp. 835–840, doi: 10.1109/ICACITE60783.2024.10617436.
- [8] S. A. Khan, M. L. Suresh, M. A. Mohammed, S. A. W. Sheet, M. I. Mahmoud, and S. Manochitra, "Exploring Energy-Efficient Deep Learning with Neuromorphic Computing for Edge AI and IoT Applications," in 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON), IEEE, Jul. 2025, pp. 1–6, doi: 10.1109/I2ITCON65200.2025.11210727.
- [9] G. Oise and S. Konyeha, "E-WASTE MANAGEMENT THROUGH DEEP LEARNING: A SEQUENTIAL NEURAL NETWORK APPROACH," *FUDMA JOURNAL OF SCIENCES*, vol. 8, no. 3, pp. 17–24, Jul. 2024, doi: 10.33003/fjs-2024-0804-2579.
- [10] Y. Qin, Z. Peng, L. Miao, Z. Chen, J. Ouyang, and X. Yang, "Integrating nanodevice and neuromorphic computing for enhanced magnetic anomaly detection," *Measurement*, vol. 244, p. 116532, Feb. 2025, doi: 10.1016/J.MEASUREMENT.2024.116532.
- [11] A. Arabiat and M. Altayeb, "Enhancing internet of things security: evaluating machine learning classifiers for attack prediction," *International Journal of Electrical and*

- Computer Engineering, vol. 14, no. 5, pp. 6036–6046, Oct. 2024, doi: 10.11591/IJECE.V14I5.PP6036-6046.
- [12] A. A. Abu-Shareha, M. M. Abualhaj, A. Al-Allawee, A. Munther, and M. Anbar, “Enhancing Malware Detection with Firefly and Grey Wolf Optimization Algorithms,” 2024 11th International Conference on Electrical and Electronics Engineering, ICEEE 2024, pp. 394–398, 2024, doi: 10.1109/ICEEE62185.2024.10779310.
- [13] Z. Wang, Z. Li, Z. Xia, X. Sun, J. Meng, and T. Wang, “Emerging CMOS Compatible Memristor for Storage Technology and Neuromorphic Computing Applications,” Chip, p. 100183, Dec. 2025, doi: 10.1016/J.CHIP.2025.100183.
- [14] T. Xiong, W. Li, P. Yu, and L. Mao, “Fluidic memristor: Bringing chemistry to neuromorphic devices,” Innovation, vol. 4, no. 3, May 2023, doi: 10.1016/J.XINN.2023.100435.
- [15] O. Almomani, A. Alsaaidah, A. A. A. Shareha, A. Alzaqebah, and M. Almomani, “Performance Evaluation of Machine Learning Classifiers for Predicting Denial-of-Service Attack in Internet of Things,” International Journal of Advanced Computer Science and Applications, vol. 15, no. 1, pp. 263–271, 2024, doi: 10.14569/IJACSA.2024.0150125.
- [16] M. Maaz, G. Ahmed, A. S. Al-Shamayleh, A. Akhunzada, S. Siddiqui, and A. H. Al-Ghushami, “Empowering IoT Resilience: Hybrid Deep Learning Techniques for Enhanced Security,” IEEE Access, vol. 12, pp. 180597–180618, 2024, doi: 10.1109/ACCESS.2024.3482005.
- [17] P. O. EJENARHOME, G. P. Oise, A. O. AIRHIAVBRE, and J. A. Odumayomi, “DistilBERT-Based Detection of AI-Generated Text in Online Assessments: Ethical and Pedagogical Implications,” JOURNAL OF DIGITAL LEARNING AND DISTANCE EDUCATION, vol. 4, no. 9, pp. 1864–1873, Feb. 2026, doi: 10.56778/jdlde.v4i9.651.
- [18] F. Yang, Z. Liu, X. Ding, Y. Li, C. Wang, and G. Shen, “Carbon-based memristors for resistive random access memory and neuromorphic applications,” Chip, vol. 3, no. 2, pp. 507–519, Jun. 2024, doi: 10.1016/J.CHIP.2024.100086.
- [19] J. Q. Yang et al., “Leaky integrate-and-fire neurons based on perovskite memristor for spiking neural networks,” Nano Energy, vol. 74, Aug. 2020, doi: 10.1016/j.nanoen.2020.104828.
- [20] J. K. Eshraghian et al., “Training Spiking Neural Networks Using Lessons from Deep Learning,” Proceedings of the IEEE, vol. 111, no. 9, pp. 1016–1054, Sep. 2023, doi: 10.1109/JPROC.2023.3308088.
- [21] Z. Zhang et al., “Real-Time Imaging Enhancement of Handheld Photoacoustic System With FeRAM Crossbar Array Based Neuromorphic Design,” IEEE Trans. Biomed. Circuits Syst., vol. 19, no. 5, pp. 1031–1044, 2025, doi: 10.1109/TBCAS.2025.3538578.
- [22] A. A. Abdellatif et al., “MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange,” IEEE Internet Things J., vol. 8, no. 21, pp. 15762–15775, Nov. 2021, doi: 10.1109/JIOT.2021.3052910.
- [23] U. Mushtaq, M. W. Akram, D. Prasad, and A. Islam, “An energy and area-efficient spike frequency adaptable LIF neuron for spiking neural networks,” Computers and Electrical Engineering, vol. 119, Oct. 2024, doi: 10.1016/j.compeleceng.2024.109562.
- [24] Z. Ning et al., “Mobile Edge Computing Enabled 5G Health Monitoring for Internet of Medical Things: A Decentralized Game Theoretic Approach,” IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 463–478, Feb. 2021, doi: 10.1109/JSAC.2020.3020645.
- [25] W. Zhang et al., “Neuro-inspired computing chips,” Nat. Electron., vol. 3, no. 7, pp. 371–382, Jul. 2020, doi: 10.1038/s41928-020-0435-7.
- [26] G. P. Oise, T. Jessa, E. Mintah, F. O. Uloko, O. Sokoya, and O. Ukpabor, “A Hybrid Machine Learning–Optimization Framework for Energy Demand Forecasting and Decision Support in Smart Infrastructure,” Methods in Science and Technology Studies, vol. 2, no. 1, pp. 68–81, Apr. 2026, doi: 10.64539/msts.v2i1.2026.440.
- [27] X. Wan et al., “Proton-gated organic thin-film transistors for leaky integrate-and-fire convolutional spiking neural networks,” Org. Electron., vol. 135, Dec. 2024, doi: 10.1016/j.orgel.2024.107144.
- [28] T. Jin, K. Lv, J. Chen, L. Zhang, and X. Guo, “Fully hardware-implemented neuromorphic systems using TaOx-based memristors,” Device, vol. 3, no. 4, Apr. 2025, doi: 10.1016/J.DEVICE.2024.100645.
- [29] E. M.V., N. T., B. B., and N. A. Kamsani, “Spiking neural network circuit with op-amp based LIF neuron and RRAM synaptic array,” AEU - International Journal of Electronics and Communications, vol. 201, Nov. 2025, doi: 10.1016/j.aeue.2025.156004.
- [30] D. M.S., S. H.R., J. Raghu, and R. S.B., “Simulation-based effective comparative analysis of neuron circuits for neuromorphic computation systems,” Neurocomputing, vol. 614, Jan. 2025, doi: 10.1016/j.neucom.2024.128758.
- [31] G. P. Oise, B. S. Olanrewaju, O. A. Orukpe, K. C. Pius, and A. O. Airhiavbere, “A Convolutional Neural Network Framework for Intelligent Intrusion Detection,” Scientific Journal of Computer Science, vol. 2, no. 1, pp. 50–59, Feb. 2026, doi: 10.64539/sjcs.v2i1.2026.404.
- [32] B. M. Pirozzo, J. A. Fernandez-Leon, M. De Paula, R. Picos, and G. G. Acosta, “Rat-SLAM with neuromorphic computing,” Neurocomputing, vol. 684, p. 133572, Jul. 2026, doi: 10.1016/J.NEUCOM.2026.133572.
- [33] H. Y. Kim, W. Kim, and C. Park, “Sensory neuromorphic displays,” Device, 2025, doi: 10.1016/j.device.2025.100848.
- [34] S. Wang, M. Wu, W. Liu, J. Liu, Y. Tian, and K. Xiao, “Dopamine detection and integration in neuromorphic devices for applications in artificial intelligence,” Device, vol. 2, no. 2, Feb. 2024, doi: 10.1016/j.device.2024.100284.
- [35] Y. Wang, Y. Wang, C. Chen, R. Jiang, and W. Huang, “Development of variational quantum deep neural networks for image recognition,” Neurocomputing, vol. 501, pp. 566–582, Aug. 2022, doi: 10.1016/j.neucom.2022.06.010.

- [36] S. X. Go, Q. Wang, Y. Jiang, Y. Zhang, and D. K. Loke, "Multifunctional nanomaterials, systems, and algorithms for neuromorphic computing applications: Autonomous systems and wearable robotics," *Materials Science and Engineering: R: Reports*, vol. 167, p. 101095, Jan. 2026, doi: 10.1016/J.MSER.2025.101095.
- [37] S. Dai et al., "Intrinsically stretchable neuromorphic devices for on-body processing of health data with artificial intelligence," *Matter*, vol. 64, pp. 248–250, Oct. 2022, doi: 10.1016/J.MATT.2022.07.016.
- [38] S. J. Kim, S. B. Kim, and H. W. Jang, "Competing memristors for brain-inspired computing," *iScience*, vol. 24, no. 1, Jan. 2021, doi: 10.1016/j.isci.2020.101889.
- [39] G. P. Oise, O. C. Nwabukei, O. J. Akpwehbe, 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.
- [40] Z. Jian et al., "Artificial photoelectric synaptic devices with ferroelectric diode effect for high-performance neuromorphic computing," *Surfaces and Interfaces*, vol. 55, Dec. 2024, doi: 10.1016/j.surfin.2024.105407.
- [41] D. Pattnaik et al., "Stress-induced Artificial neuron spiking in Diffusive memristors," Oct. 2024, doi: 10.1038/s44172-024-00315-z.
- [42] H. Sun et al., "A flexible BiFeO₃-based ferroelectric tunnel junction memristor for neuromorphic computing," *Journal of Materiomics*, vol. 8, no. 1, pp. 144–149, Jan. 2022, doi: 10.1016/j.jmat.2021.04.009.
- [43] J. Shin, E. Seo, C. Youn, and S. Kim, "Ferroelectric tunnel junctions with 5 nm-thick HZO for tunable synaptic plasticity and neuromorphic computing," *J. Alloys Compd.*, vol. 1036, Jul. 2025, doi: 10.1016/j.jallcom.2025.181869.
- [44] G. P. Oise, J. A. Odimeyomi, B. N. Unuigbokhai, B. E. Akilo, and S. A. Oyedotun, "Deep Learning for Cybersecurity Threat Detection in Industrial Process Control and Monitoring Systems," in *ECP 2025*, Basel Switzerland: MDPI, Feb. 2026, p. 43. doi: 10.3390/engproc2025117043.
- [45] D. Ju and S. Kim, "Implementation of edge computing using HfAlO_x-based memristor," *J. Alloys Compd.*, vol. 997, Aug. 2024, doi: 10.1016/j.jallcom.2024.174804.
- [46] T. Cao et al., "Emerging memory devices for neuromorphic computing in the Internet of Medical Things," *Cell Rep. Phys. Sci.*, vol. 6, no. 8, p. 102735, Aug. 2025, doi: 10.1016/J.XCRP.2025.102735.
- [47] F. Ye, F. Liang, J.-W. Zhong, G.-L. Li, and X.-G. Tang, "Research progress of BaTiO₃-based ferroelectric memristors for artificial synapse and neuromorphic computing," *Materials Today Physics*, vol. 61, p. 102027, Feb. 2026, doi: 10.1016/J.MTPHYS.2026.102027.
- [48] M. Ismail, H. Abbas, A. Sokolov, C. Mahata, C. Choi, and S. Kim, "Emulating synaptic plasticity and resistive switching characteristics through amorphous Ta₂O₅ embedded layer for neuromorphic computing," *Ceram. Int.*, vol. 47, no. 21, pp. 30764–30776, Nov. 2021, doi: 10.1016/j.ceramint.2021.07.257.
- [49] G. P. Oise et al., "Isolation Forest-Based Intrusion Detection for Cyber-Physical Systems," *Scientific Journal of Engineering Research*, vol. 2, no. 2, pp. 222–233, Mar. 2026, doi: 10.64539/sjer.v2i2.2026.434.
- [50] W. Liu et al., "A ferroelectrics/oxide heterojunction based memristor for artificial synapse and neuromorphic computing," *J. Colloid Interface Sci.*, vol. 702, Jan. 2026, doi: 10.1016/j.jcis.2025.138911.
- [51] N. Kumar, M. Patel, T. T. Nguyen, P. Bhatnagar, and J. Kim, "All-oxide-based and metallic electrode-free artificial synapses for transparent neuromorphic computing," *Mater. Today Chem.*, vol. 23, Mar. 2022, doi: 10.1016/j.mtchem.2021.100681.
- [52] Z. Fang et al., "Tunable optoelectronic memristor based on MoS₂/BaTiO₃ for neuromorphic vision," *Chip*, vol. 4, no. 3, Sep. 2025, doi: 10.1016/j.chip.2025.100136.
- [53] S. A. Oyedotun et al., "The Role of Internal Audit in Fraud Detection and Prevention: A Multi-Contextual Review and Research Agenda," *Journal of Science Research and Reviews*, vol. 2, no. 2, pp. 76–85, May 2025, doi: 10.70882/josrar.2025.v2i2.51.
- [54] J. Du et al., "Ferroelectric memristor and its neuromorphic computing applications," *Materials Today Physics*, vol. 50, Jan. 2025, doi: 10.1016/j.mtphys.2024.101607.
- [55] 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.
- [56] S. A. Gabayre, M. Illeperuma, V. D. De-Silva, X. Shi, and S. E. Savel'ev, "Advancements in neuromorphic computing for bio-inspired artificial vision: A review," *Neurocomputing*, vol. 653, p. 131221, Nov. 2025, doi: 10.1016/J.NEUCOM.2025.131221.