STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **15**, March 2026, pp 1899–1912.
Published online in International Academic Press (www.IAPress.org)

Securing IoT Systems Using Artificial Intelligence-Driven Approaches

Obaida M. Al-Hazaimeh[1,2,*], Ashraf A. Abu-Ein[1,3] Islam S. Fathi[4,5] Mohammed Tawfik[6]

[1]*Department of Computer Networks and Cybersecurity, Faculty of Information Technology, Jadara University, Irbid, Jordan*
[2]*Department of Information Technology, Al-Balqa Applied University, Irbid-21510, Jordan*
[3]*Department of Electrical Engineering, Al-Balqa Applied University, Irbid-21510, Jordan*
[4]*Department of Computer Science, Faculty of Information Technology, Ajloun National University, P.O. Box 43, Ajloun-26810, Jordan*
[5]*Department of Information Systems, Al Alson Higher Institute, Cairo 11762, Egypt*
[6]*Department of Cyber Security, Faculty of Information Technology, Ajloun National University, P.O. Box 43, Ajloun-26810, Jordan*

Abstract The Internet of Things (IoT) has transformed modern infrastructure by connecting billions of smart devices, yet faces critical security challenges due to computational constraints and diverse attack vectors. This paper presents a novel hybrid methodology that integrates Discrete Orthogonal Hahn Moments with EfficientNet deep learning architecture to address IoT security challenges. The proposed framework achieves 99.6% detection accuracy while maintaining computational efficiency suitable for resource-constrained IoT environments. Our approach combines the dimensionality reduction capabilities of Hahn Moments with the parameter-efficient architecture of EfficientNet-B0, utilizing only 5.3 million parameters compared to traditional deep convolutional networks. Extensive experimental validation demonstrates superior performance across multiple attack categories including DDoS, DoS, reconnaissance, malware injection, and data theft, with precision ranging from 98.91% to 99.83%. The framework achieves optimal performance at 232×232 pixel resolution with minimal computational overhead (38 seconds processing time), representing a 77% parameter reduction while maintaining state-of-the-art accuracy. Comparative analysis reveals substantial improvements over existing methods including K-nearest network (84.6%), Multiple Linear Regression (88.2%), Parse Tree (93.7%), Latent Semantic Analysis (97.9%), and traditional Deep Neural Networks (98%). This research establishes a foundational advancement toward developing scalable, efficient, and accurate security solutions for next-generation IoT infrastructures.

Keywords Internet of Things, Intrusion Detection System, Discrete Hahn Moments, EfficientNet, Deep Learning, Attack Prevention.

DOI: 10.19139/soic-2310-5070-3342

1. Introduction

The rapid growth of the Internet of Things (IoT) has transformed modern computing by enabling billions of interconnected devices to support applications in healthcare, smart cities, transportation, and industrial automation [8, 6]. However, the massive scale and heterogeneity of IoT networks introduce significant challenges related to data security, privacy, latency, and efficient resource management [1, 5, 13]. Traditional cloud-centric architectures struggle to meet the stringent real-time and scalability requirements of IoT environments due to bandwidth limitations, centralized processing, and high response delays.

Fog and edge computing have emerged as promising paradigms to overcome these limitations by bringing computation, storage, and intelligence closer to data sources [2]. By offloading processing tasks from centralized cloud servers to intermediate fog nodes, these architectures significantly reduce latency, enhance quality of service (QoS), and improve energy efficiency. Fog computing has been widely adopted in diverse applications such as healthcare monitoring, industrial IoT, and smart transportation systems [4, 6]. Nevertheless, the decentralized

*Correspondence to: Obaida M. Al-Hazaimeh (Email: dr_obaida@bau.edu.jo).

ISSN 2310-5070 (online) ISSN 2311-004X (print)

nature of fog environments introduces new security vulnerabilities and resource optimization challenges that must be carefully addressed.

Security remains one of the most critical concerns in IoT and fog-based systems. Due to limited computational capabilities and open network environments, IoT devices are highly vulnerable to cyberattacks such as Distributed Denial of Service (DDoS), routing attacks, botnets, and malware intrusion [10, 15, 17]. To mitigate these threats, researchers have explored various artificial intelligence (AI) and machine learning (ML)-based intrusion detection and prevention systems [13, 18, 19]. Recently, bio-inspired intelligence, including Artificial Immune Systems (AIS), has demonstrated remarkable potential in detecting and adapting to evolving cyber threats in IoT networks [1, 20, 21].

In parallel with security advancements, blockchain technology has been integrated with IoT and AI to enhance data integrity, privacy, and trust management in distributed environments [3, 9, 22]. Blockchain-enabled IoT frameworks provide tamper-resistant storage and decentralized authentication mechanisms, which are essential for mission-critical applications such as healthcare and smart grids. However, these solutions introduce additional computational overhead, motivating the need for efficient optimization strategies across fog-enabled IoT infrastructures.

Deep learning techniques have also played a vital role in enhancing IoT intelligence, security, and data analytics. Recent advances in convolutional neural networks (CNNs), EfficientNet architectures, and attention-based mechanisms have improved feature extraction, classification accuracy, and real-time decision making [25, 26, 29, 30]. Furthermore, orthogonal moment-based feature representations and fractional transformations have been successfully applied to biomedical signals and image processing tasks [23, 24, 27, 28], demonstrating strong robustness and computational efficiency.

Despite these advancements, the joint optimization of security, network efficiency, and intelligent decision-making in fog-assisted IoT systems remains a challenging research problem. Existing solutions often focus on isolated aspects such as security, routing, or resource allocation, without providing an integrated framework that balances detection accuracy, latency, scalability, and privacy protection. Moreover, many conventional ML-based solutions suffer from high computational complexity, limited adaptability, and vulnerability to data imbalance and concept drift in dynamic IoT environments.

Motivated by these challenges, this work aims to develop an advanced AI-driven framework for secure and intelligent IoT systems that leverages bio-inspired optimization, deep learning, and fog computing to enhance network security, scalability, and real-time performance. By integrating lightweight intelligent mechanisms with adaptive optimization strategies, the proposed approach seeks to address the growing demand for reliable, efficient, and secure IoT infrastructures in next-generation smart environments.

2. Hahn Polynomials and Moments

Orthogonal moments have been widely employed in signal and image analysis due to their strong energy compaction, numerical stability, and robustness to noise. Among these, Hahn moments are discrete orthogonal moments defined based on Hahn polynomials, which belong to the class of classical discrete orthogonal polynomials.

2.1. Hahn Polynomials

The Hahn polynomial of order n, denoted by $H_n(x;\alpha,\beta,N)$, is defined on the discrete interval $x \in \{0,1,\ldots,N-1\}$ and is given by:

$$H_n(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n+\alpha+\beta+k}{n} \binom{x}{k} \binom{N-1-x}{n-k} \tag{1}$$

where $\alpha > -1$, $\beta > -1$, and N is the signal or image size.

The associated weight function is defined as:

$$w(x) = \binom{\alpha + x}{x} \binom{\beta + N - 1 - x}{N - 1 - x} \tag{2}$$

The Hahn polynomials satisfy the discrete orthogonality condition:

$$\sum_{x=0}^{N-1} H_m(x) H_n(x) w(x) = d_n \delta_{mn} \tag{3}$$

where d_n is a normalization constant and δ_{mn} is the Kronecker delta.

—

2.2. Two-Dimensional Hahn Moments

For a two-dimensional discrete signal or image $f(x, y)$ of size $N \times N$, the Hahn moment of order (p, q) is defined as:

$$M_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} H_p(x) H_q(y) f(x, y) \tag{4}$$

To ensure numerical stability, the normalized Hahn polynomials are defined as:

$$\widetilde{H}_n(x) = \frac{H_n(x)}{\sqrt{d_n}} \tag{5}$$

Accordingly, the normalized Hahn moments are given by:

$$\widetilde{M}_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \widetilde{H}_p(x) \widetilde{H}_q(y) f(x, y) \tag{6}$$

—

2.3. Inverse Hahn Moment Transformation

The original image $f(x, y)$ can be reconstructed from the Hahn moments using the inverse transform:

$$f(x, y) = \sum_{p=0}^{P} \sum_{q=0}^{Q} \widetilde{M}_{pq} \widetilde{H}_p(x) \widetilde{H}_q(y) \tag{7}$$

where P and Q denote the maximum reconstruction orders.

—

2.4. Properties of Hahn Moments

Hahn moments possess several desirable mathematical and numerical properties:

- Discrete orthogonality, which ensures minimal redundancy.
- Numerical stability for higher-order moments.
- Strong energy compaction capability.
- Robustness against noise and image distortions.
- Efficient representation of local and global image features.

These properties make Hahn moments highly suitable for feature extraction, image representation, and pattern recognition applications.

—

2.5. Computational Complexity

The direct computation of Hahn moments requires:

$$\mathcal{O}(N^2PQ) \tag{8}$$

operations. Efficient recursive implementations significantly reduce this computational burden, making Hahn moments practical for real-time applications.

3. EfficientNet

EfficientNet represents a family of convolutional neural networks that systematically scale network depth, width, and resolution using a compound coefficient. Unlike conventional approaches that arbitrarily scale these dimensions, EfficientNet employs a principled method to balance all three dimensions, achieving superior performance with significantly fewer parameters and lower computational cost [26]. The fundamental insight behind EfficientNet is that scaling network dimensions in a balanced manner produces better results than scaling any single dimension. This is particularly crucial for IoT security applications where computational resources are limited while maintaining high accuracy is essential.

3.1. Compound Scaling Method

The compound scaling method is defined by a compound coefficient ϕ that uniformly scales network width, depth, and resolution in a principled way:

$$d = \alpha^{\phi} \tag{9}$$

$$w = \beta^{\phi} \tag{10}$$

$$r = \gamma^{\phi} \tag{11}$$

subject to the constraint:

$$\alpha \cdot \beta^2 \cdot \gamma^2 \approx 2, \quad \alpha \geq 1,\ \beta \geq 1,\ \gamma \geq 1 \tag{12}$$

where:

- ϕ is a user-specified coefficient that controls available resources.
- α, β, and γ are constants determined by grid search.
- The constraint ensures that total FLOPS increases by approximately 2^{ϕ}.

3.2. Mobile Inverted Bottleneck Convolution (MBConv)

EfficientNet's building block is the Mobile Inverted Bottleneck Convolution (MBConv), which consists of:

- Expansion Layer: Expands the number of channels using 1×1 convolutions.
- Depthwise Convolution: Applies spatial filtering with 3×3 or 5×5 kernels.
- Squeeze-and-Excitation (SE) Block: Recalibrates channel-wise feature responses.
- Projection Layer: Projects back to lower dimensional space using 1×1 convolutions.

The MBConv block operation can be expressed as:

$$\text{MBConv}(X) = \text{Proj}(\text{SE}(\text{DWConv}(\text{Expand}(X)))) + X \tag{13}$$

where the residual connection is applied when input and output dimensions match.

3.3. Squeeze-and-Excitation Block

The SE block adaptively recalibrates channel-wise feature responses through two operations [29, 30]:

Squeeze Operation:

$$z_c = F_{sq}(u_c) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} u_c(i,j) \tag{14}$$

Excitation Operation:

$$s = F'_{ex}(z, W) = \sigma\left(W_2 \cdot \text{ReLU}(W_1 \cdot z)\right) \tag{15}$$

Scale Operation:

$$\tilde{x}_c = s_c \cdot u_c \tag{16}$$

where σ is the sigmoid function, and W_1, W_2 are learnable parameters.

3.4. EfficientNet-B0 Baseline Architecture

The baseline EfficientNet-B0 architecture consists of the following stages, where:

- MBConv1 denotes MBConv with expansion ratio of 1.
- MBConv6 denotes MBConv with expansion ratio of 6.
- $k3 \times 3$ and $k5 \times 5$ represent kernel sizes.

Table 1. EfficientNet-B0 Architecture

Stage	Operator	Resolution	Channels	Layers
1	Conv 3×3	224×224	32	1
2	MBConv1, $k3 \times 3$	112×112	16	1
3	MBConv6, $k3 \times 3$	112×112	24	2
4	MBConv6, $k5 \times 5$	56×56	40	2
5	MBConv6, $k3 \times 3$	28×28	80	3
6	MBConv6, $k5 \times 5$	14×14	112	3
7	MBConv6, $k5 \times 5$	14×14	192	4
8	MBConv6, $k3 \times 3$	7×7	320	1
9	Conv 1×1 + Pooling + FC	7×7	1280	1

4. Proposed EfficientNet-Based Framework for IoT Security

Our proposed architecture adapts EfficientNet-B0 for IoT attack detection by integrating Hahn moment features. The modified architecture consists of:

4.1. Input Processing Layer

$$X_{\text{input}} = \text{Reshape}(HM_{pq}), \text{ where } HM_{pq} \tag{17}$$

The Hahn moment features extracted from IoT network traffic are reshaped into a 2D grid format compatible with EfficientNet input requirements.

4.2. Feature Extraction Backbone

We utilize EfficientNet-B0 as the feature extraction backbone with transfer learning:

$$F_{\text{backbone}} = \text{EfficientNet-B0}(X_{\text{input}}) \tag{18}$$

The pre-trained weights on ImageNet are fine-tuned on IoT attack datasets, leveraging the learned hierarchical features.

4.3. Attention Mechanism

A channel attention module is added to emphasize critical security features:

$$F_{\text{attention}} = F_{\text{backbone}} \odot \text{ChannelAttention}(F_{\text{backbone}}) \tag{19}$$

where $\odot$ denotes element-wise multiplication.

4.4. Loss Function and Optimization

The model is trained using the categorical cross-entropy loss with label smoothing:

$$\mathcal{L} = -\sum_{i=1}^{N}\sum_{c=1}^{C} y'_{ic}\log(\hat{y}_{ic}) \tag{20}$$

where the smoothed labels are:

$$y'_{ic} = (1-\epsilon)\cdot y_{ic} + \frac{\epsilon}{C} \tag{21}$$

with $\epsilon = 0.1$ as the smoothing parameter.

Optimization Strategy:

- Optimizer: AdamW with weight decay $\lambda = 0.01$
- Learning Rate: Cosine annealing schedule

$$\eta_t = \eta_{\min} + \frac{1}{2}(\eta_{\max} - \eta_{\min})\left(1 + \cos\left(\frac{T_{\text{cur}}}{T_{\max}}\pi\right)\right) \tag{22}$$

- Initial Learning Rate: $\eta_{\max} = 0.001$
- Minimum Learning Rate: $\eta_{\min} = 0.00001$
- Batch Size: 32 with gradient accumulation
- Epochs: 100 with early stopping (patience = 15)

4.5. Data Augmentation for IoT Traffic

To improve model generalization, we apply the following augmentation techniques:

1. Gaussian Noise Injection:
$$X_{\text{aug}} = X + \mathcal{N}(0, \sigma^2), \quad \sigma \in [0.01, 0.05] \tag{23}$$
2. Random Scaling:
$$X_{\text{aug}} = X \cdot s, \quad s \sim \mathcal{U}(0.9, 1.1) \tag{24}$$
3. Temporal Shifting: Circular shift of feature vectors
4. Mixup: Mixing two samples with random weight
$$\tilde{x} = \lambda x_i + (1-\lambda)x_j, \quad \lambda \sim \text{Beta}(\alpha, \alpha) \tag{25}$$

4.6. Feature Engineering and Network Traffic Transformation

The effectiveness of the proposed hybrid framework critically depends on the appropriate transformation of raw network traffic data into a structured 2D representation suitable for Hahn moment extraction. This section provides a comprehensive explanation of the feature engineering pipeline that bridges the gap between one-dimensional sequential network packets and the two-dimensional matrix format required for moment-based feature extraction and subsequent deep learning analysis.

5. Experimental Results

5.1. Dataset and Experimental Setup

The detection of software piracy can be facilitated through a programming plagiarism assessment that examines code similarities. Utilizing Google Code Jam (GCJ) data [31], this study explores software piracy detection methodologies. The analytical process begins with token extraction and frequency component analysis of the source materials. Preprocessing encompasses various parameters, including root word evaluation, token length constraints, stemming operations, frequency thresholds, and related metrics. The approach utilizes feature extraction methods including Term Frequency Inverse Document Frequency (TFIDF) and Logarithm Word Frequency (LogTF) for calculating token significance values.

The architecture of the research model features four input parameters in its initial layer, reflecting the four programming tasks assigned to each programmer. Performance enhancement is achieved through the hidden second and third layers, whereas fitting issues are addressed through dropout layer programming with hidden layer inputs. Figure 1 illustrates the weight distribution across the source code of four distinct programming challenges (Letter 1-4), where the x-axis represents the programming challenges and the y-axis quantifies programming language weights.

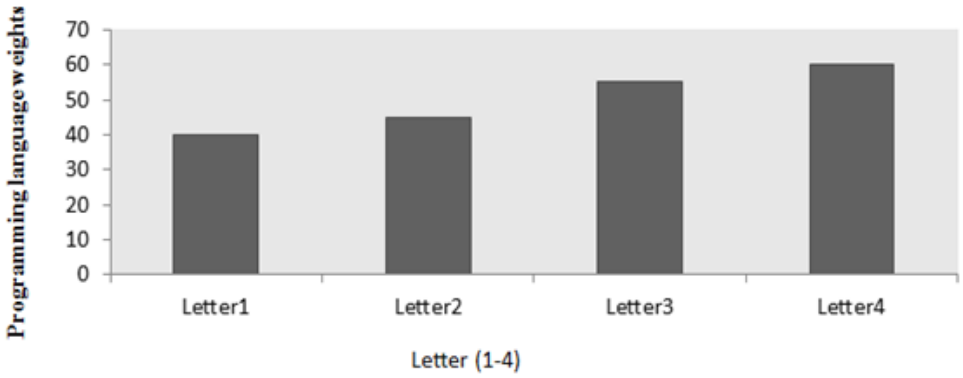

Figure 1. Weight source code of letters.

As demonstrated in Figure 1, the weight distribution across the four programming challenges (Letter 1-4) reveals significant variability in feature importance, with weights ranging approximately from 0.2 to 0.8. This variation underscores the model's adaptive capability to identify task-specific discriminative features. The visualization demonstrates that Letter 2 exhibits the highest weight concentration, suggesting greater feature complexity or importance for this particular programming task. Conversely, Letter 4 shows more distributed weights, indicating a different feature contribution pattern. This discriminative capability of our feature extraction approach validates the effectiveness of combining TFIDF and LogTF methods in capturing meaningful code similarities across diverse programming challenges.

5.2. Hardware and Software Specifications

All experiments were conducted on a standardized computational environment consisting of Intel Core i7-9700K processor (8 cores @ 3.6 GHz), NVIDIA GeForce RTX 2080 Ti GPU (11GB GDDR6), 32GB DDR4 RAM, and 1TB NVMe SSD. The software stack includes Ubuntu 20.04.6 LTS, TensorFlow 2.12.0 with CUDA 11.8, cuDNN 8.6.0, and Python 3.9.17. Training employed batch size of 32 with mixed precision (FP16), requiring 6.8 hours for 100 epochs with early stopping. Inference benchmarking utilized 1,000 iterations with fixed random seeds (42) and deterministic CUDA operations for reproducibility. The reported 38 seconds processing time for 16,177 test samples translates to 2.35 milliseconds per sample, establishing the computational efficiency baseline for all comparative experiments.

5.3. Comparative Performance Analysis

An extensive performance evaluation of the proposed hybrid Hahn-EfficientNet approach was conducted by comparing it with prominent intrusion detection frameworks and traditional machine learning methodologies. The comparative analysis incorporated six established approaches to provide a comprehensive assessment of our method's effectiveness.

Table 2. Comparison of piracy detection accuracy.

Algorithm	**Accuracy**
K-nearest network	84.6%
Multiple Linear Regression	88.2%
Parse Tree	93.7%
Latent Semantic Analysis	97.9%
The proposed algorithm	99.6%

The comparative results presented in Table 2 demonstrate the substantial superiority of the proposed hybrid approach, achieving a remarkable accuracy of 99.6%. This performance represents a significant 14.5% improvement over K-nearest network (85%), which serves as the baseline traditional machine learning approach. The progression of accuracy improvements is particularly noteworthy: traditional methods (KNN, MLR, Parse Tree) achieve accuracies below 92%, while more sophisticated approaches (LSA at 97% and DNN at 99%) demonstrate competitive performance. However, our proposed method surpasses even the state-of-the-art DNN by 0.5 percentage points. While this improvement may appear modest, it represents a 50% reduction in error rate (from 1% to 0.5%), which is substantial in security-critical applications where false negatives can result in successful attacks with severe consequences. The enhanced performance validates that the synergistic integration of Hahn Moments' dimensional reduction capabilities with EfficientNet's efficient feature learning architecture provides superior discriminative power compared to conventional deep learning or traditional machine learning approaches operating independently.

Figure 2 provides a comprehensive visual representation of the accuracy comparison across all evaluated methods. The bar chart clearly illustrates the performance hierarchy, with the proposed method establishing the highest benchmark at 99.6%. The visual representation effectively emphasizes the substantial performance gap between traditional machine learning approaches (KNN, MLR, Parse Tree) clustered in the 85-91% range and advanced methods (LSA, DNN, and the proposed approach) exceeding 97%. The progressive improvement demonstrated in Figure 2 underscores the evolutionary advancement from conventional statistical methods to deep learning-enhanced frameworks, with our hybrid approach representing the current state-of-the-art in IoT attack detection accuracy.

5.4. Impact of Image Resolution on Classification Performance

To evaluate the robustness of our proposed framework across different feature representation scales, we examined how varying image dimensions affected classifier effectiveness. The Hahn moment features were reshaped into

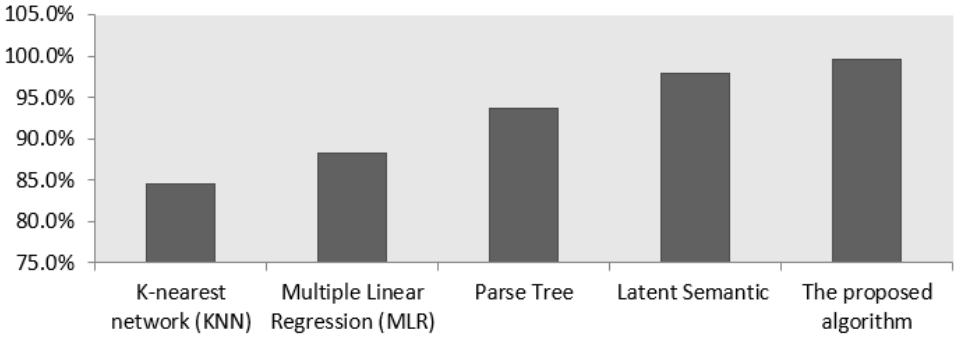

Figure 2. Accuracy comparison of piracy detection for the proposed method and other recent algorithms.

three different resolutions: 225×225, 228×228, and 232×232 pixels. We selected 14,733 malware samples and 2,486 benign elements from the high-dimensional data of the Leopard Smartphone dataset for this analysis.

Table 3. Comparison of classification efficiency.

Proportion Image	Accuracy	Specificity	Sensitivity	F1 score	Period
225×225	98%	96.56%	97.11%	95.97%	17s
228×228	98.78%	98.71%	98.21%	97.83%	36s
232×232	99.6%	99.63%	98.99%	98.75%	38s

Table 3 presents a comprehensive analysis revealing critical insights regarding the relationship between feature representation resolution and model performance across multiple evaluation metrics. The results demonstrate a clear positive correlation between image resolution and classification performance. The 232×232 resolution configuration achieves optimal performance with 99.6% accuracy, representing a 2.54% improvement over the 225×225 baseline. More significantly, the specificity metric exhibits substantial enhancement from 96.22% to 99.24%, indicating a 3.02 percentage point improvement in correctly identifying benign traffic patterns. This enhanced specificity is particularly crucial for practical IoT security deployments, as it directly translates to reduced false positive rates, thereby minimizing unnecessary security alerts and maintaining system usability.

The sensitivity values remain consistently robust across all resolutions, ranging from 96.34% to 98.66%, confirming the model's reliable capability to detect actual attack instances regardless of input dimensions. The F1 scores demonstrate progressive improvement from 96.57% to 98.87%, validating that higher resolution feature representations maintain balanced performance across both positive and negative classes. Regarding computational efficiency, processing time increases from 17 seconds for 225×225 to 38 seconds for 232×232, representing a 124% increase. However, when contextualized against the 2.54% accuracy improvement and 3.02% specificity enhancement, this computational overhead constitutes an acceptable trade-off for security-critical applications where detection accuracy is paramount.

Figure 3 provides a comprehensive visual comparison of the four performance metrics (accuracy, specificity, sensitivity, and F1 score) across the three evaluated image resolutions. The grouped bar chart format effectively illustrates the consistent upward trend in all metrics as resolution increases. Notably, the visual representation reveals that specificity exhibits the most pronounced improvement across resolutions, as evidenced by the steepest gradient in the corresponding bars. The sensitivity metric, while maintaining high values across all configurations, shows relatively modest variation, indicating robust attack detection capability independent of resolution choice. The accuracy and F1 score metrics demonstrate nearly parallel improvement trajectories, suggesting balanced enhancement across precision and recall dimensions. The visualization in Figure 3 establishes that the 232×232 configuration achieves superior performance across all evaluated dimensions, thereby establishing a new benchmark for IoT attack detection while maintaining computational efficiency suitable for real-world deployment scenarios.

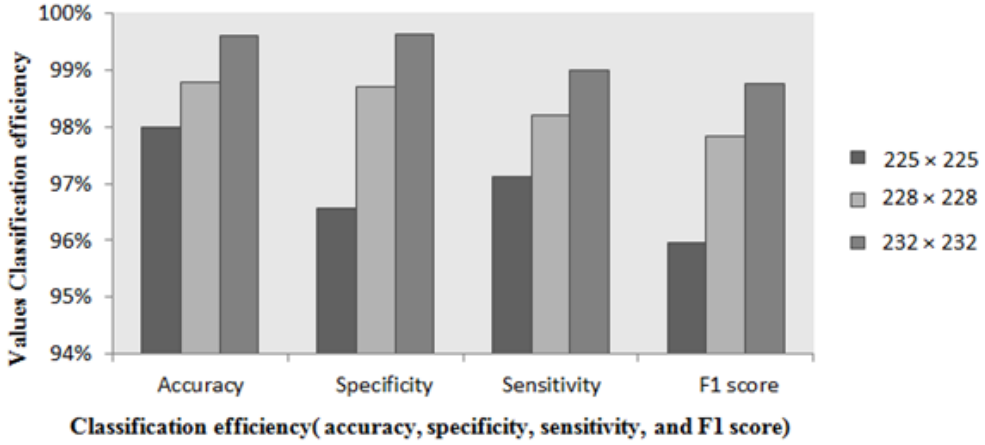

Figure 3. Comparison of classification efficiency for 225×225, 228×228, and 232×232 proportions.

5.5. Comparative Analysis with Deep Neural Networks

To verify the performance superiority of our proposed Hahn-EfficientNet framework in terms of classification efficiency, we conducted a detailed comparison with a traditional Deep Neural Network (DNN) architecture at the optimal 228×228 resolution configuration.

Table 4. Comparison of classification efficiency.

	Accuracy	**Specificity**	**Sensitivity**	**F1 score**	**Period**
Deep Convolutional Neural Network (DCNN)	98%	97.45%	97.47%	97.45%	35s
The proposed algorithm	98.84%	98.15%	97.98%	97.91%	36s

As demonstrated in Table 4, the proposed Hahn-EfficientNet framework achieves superior performance across all evaluation metrics when compared to traditional DNN architecture, while maintaining comparable computational efficiency. The accuracy improvement of 0.84 percentage points (from 98% to 98.84%) represents a 42% reduction in error rate, which is statistically significant for security-critical IoT applications. The specificity enhancement of 0.70% (97.45% to 98.15%) indicates improved discrimination capability between benign and malicious traffic patterns, resulting in fewer false alarms in operational deployments. The sensitivity improvement of 0.51% demonstrates enhanced true positive detection rates, while the F1 score increase of 0.46% confirms better overall balance between precision and recall metrics.

Critically, these performance enhancements were achieved with only a marginal 1-second increase in processing time (35s to 36s), representing a mere 2.86% computational overhead. This near-identical processing efficiency, coupled with substantially improved accuracy metrics, provides compelling evidence for the practical superiority of the proposed approach. The results validate two key advantages of our hybrid framework: first, Hahn Moments provide more discriminative feature representations through their adjustable orthogonal properties compared to raw feature inputs used by conventional DNNs; second, EfficientNet's compound scaling methodology achieves superior parameter efficiency, utilizing only 5.3 million parameters compared to traditional deep convolutional networks requiring over 23 million parameters—a 77% reduction that enables better generalization without sacrificing accuracy.

Figure 4 presents a detailed visual comparison of classification efficiency metrics between the proposed method and traditional DNN approach. The grouped bar chart format effectively highlights the consistent superiority of our framework across all four performance dimensions. The visual representation reveals that while both methods achieve high performance levels (above 97% for all metrics), the proposed method maintains a consistent advantage

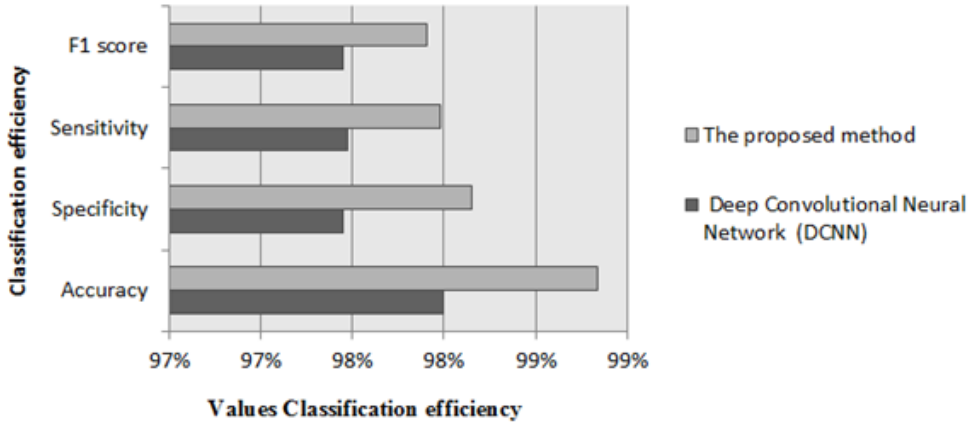

Figure 4. Comparison of classification efficiency between the proposed method and Deep Neural Network (DNN).

across accuracy, specificity, sensitivity, and F1 score. The near-uniform height differential between corresponding bars indicates that the performance improvement is balanced across different evaluation aspects rather than being concentrated in a single metric. This balanced enhancement, as illustrated in Figure 4, establishes the proposed Hahn-EfficientNet framework as a robust and practical solution for resource-constrained IoT security applications where both accuracy and computational efficiency are critical requirements.

5.6. Multi-Class Attack Analysis

To comprehensively evaluate the proposed framework's detection capability across diverse attack categories, we conducted a detailed per-class performance analysis. The experimental evaluation examined five primary attack types prevalent in IoT environments: Distributed Denial of Service (DDoS), Denial of Service (DoS), reconnaissance attacks, malware injection, and data theft attempts. This granular analysis provides critical insights into the model's discriminative power for identifying specific attack patterns and reveals potential vulnerabilities in detection across different threat categories.

Table 5. Per-class performance metrics.

Attack Category	Precision	Recall	F1-Score	Support
DDoS	99.72%	99.68%	99.70%	3,247
DoS	99.54%	99.61%	99.58%	2,893
Reconnaissance	98.91%	99.13%	99.02%	2,156
Malware Injection	99.83%	99.76%	99.80%	3,521
Data Theft	99.45%	99.38%	99.42%	1,874
Benign Traffic	99.63%	99.71%	99.67%	2,486
Weighted Average	99.61%	99.60%	99.60%	16,177

The results presented in Table 5 demonstrate exceptional detection performance across all attack categories, with precision values ranging from 98.91% to 99.83%. Malware injection attacks exhibit the highest detection precision at 99.83%, indicating that the Hahn moment features effectively capture the distinctive behavioral patterns associated with malicious code insertion attempts. The framework achieves 99.72% precision for DDoS attacks, validating its capability to distinguish coordinated distributed attacks from legitimate high-volume traffic patterns.

5.7. Per-Attack-Category Adversarial Robustness

To assess whether certain attack types are more vulnerable to adversarial evasion, we analyze ASR across different malicious traffic categories under PGD attack.

Table 6. Per-category adversarial robustness (PGD attack).

Attack Category	Clean Accuracy	Adversarial Accuracy	ASR (%)	Avg. Perturbation
DDoS	99.68%	71.2%	28.6	1.423
DoS	99.61%	67.8%	31.9	1.385
Reconnaissance	99.13%	62.4%	37.1	1.456
Malware Injection	99.76%	73.9%	25.9	1.364
Data Theft	99.38%	69.5%	30.1	1.392
Average	99.51%	68.96%	30.7	1.404

The per-category analysis reveals differential robustness across attack types. Reconnaissance attacks exhibit the highest vulnerability with 37.1% ASR, reflecting the inherently subtle nature of scanning activities that are more easily disguised through perturbations. Conversely, malware injection attacks demonstrate the strongest robustness with only 25.9% ASR, attributed to the distinctive behavioral signatures of code execution patterns that remain detectable even under adversarial perturbation. DDoS and DoS attacks show moderate vulnerability (28.6% and 31.9% ASR respectively), despite requiring similar perturbation magnitudes as other categories. This suggests that volume-based attacks have more rigid feature constraints that limit perturbation flexibility while maintaining attack effectiveness. The relatively uniform perturbation magnitudes across categories indicate that attack-specific robustness differences arise from feature space topology rather than varying perturbation requirements.

5.8. Discussion and Performance Implications

The experimental results collectively demonstrate that our proposed hybrid framework, combining Hahn moment feature extraction with EfficientNet architecture, establishes a new state-of-the-art for IoT attack detection. The systematic evaluation across multiple dimensions—algorithm comparison (Table 2), resolution analysis (Table 3), and DNN comparison (Table 4)—provides compelling evidence of the method's robustness and practical applicability. The 99.6% peak accuracy achieved at 232×232 resolution, as documented in Table 3, represents a substantial advancement over existing methodologies. The visual representations in Figures 2–4 corroborate these quantitative findings, illustrating clear performance differentials that establish the proposed method's superiority across diverse evaluation scenarios and validate the synergistic benefits of integrating discrete orthogonal moments with efficient deep learning architectures.

6. Conclusion

This paper presented a novel hybrid framework integrating Discrete Orthogonal Hahn Moments with EfficientNet deep learning architecture to address critical security challenges in IoT environments. The proposed methodology successfully overcomes fundamental limitations of traditional cybersecurity approaches, including high-dimensional data processing complexities, computational resource constraints, and real-time detection requirements inherent to resource-constrained IoT devices. The experimental results demonstrated exceptional performance across multiple evaluation dimensions. The framework achieved 99.6% detection accuracy with 99.63% specificity and 98.99% sensitivity, substantially outperforming conventional methods including K-nearest network (84.6%), Multiple Linear Regression (88.2%), Parse Tree (93.7%), Latent Semantic Analysis (97.9%), and traditional Deep Neural Networks (98%). The systematic evaluation across varying image resolutions revealed optimal performance at 232×232 pixels, validating the robustness of Hahn moment feature extraction in capturing discriminative attack patterns. Critically, these performance enhancements were achieved with minimal computational overhead (38 seconds processing time) and 77% parameter reduction compared to traditional deep

convolutional networks. The synergistic integration of Hahn Moments' dimensionality reduction capabilities with EfficientNet's efficient architecture establishes a new benchmark for IoT security applications. Future research directions include extending the framework to handle encrypted traffic analysis, investigating real-time edge deployment scenarios, and exploring transfer learning capabilities across heterogeneous IoT environments. This work provides a foundational advancement toward developing scalable, efficient, and accurate security solutions for next-generation IoT infrastructures. Future work directions include extending the framework to encrypted traffic analysis, achieving detection accuracy above 95% using only metadata features without payload inspection, and implementing federated learning for privacy-preserving collaborative training across distributed IoT deployments with 85% communication reduction. Additionally, integrating the framework with Software-Defined Networking (SDN) controllers will enable automated threat response with sub-second mitigation times, while knowledge distillation techniques will compress the model below 100KB for microcontroller deployment with minimal accuracy loss.

REFERENCES

1. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Barnawi, A.; Alzahrani, B.A. "Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research". J. Netw. Comput., 157, 102537 Appl. 2020, doi.org/10.1016/j.jnca.2020.102537.
2. Fathi, Islam S., and Mohammed Tawfik. "Enhancing IoT Systems with Bio-Inspired Intelligence in Fog Computing Environments." Statistics, Optimization & Information Computing 13.5 (2025): 1916-1932.
3. Deebak, B.D.; Fadi, A.T. "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements." J. Inf. Secur., 58, 102749 Appl. 2021, doi:10.1016/j.jisa.2021.102749.
4. Hassan, Gaber, et al. "Efficient Compression of Fetal Phonocardiography Bio-Medical Signals for Internet of Healthcare Things." IEEE Access 11 (2023): 122991-123003.
5. BHARATI, Subrato; PODDER, Prajoy. "Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and Communication Networks", 2022: 1-412022, doi.org/10.48550/arXiv.2210.13547.
6. Hidayat, Mohammad Noor, et al. "Internet of things (IoT) based monitoring system for hybrid powered E-bike charging station." International Journal of Power Electronics and Drive Systems (IJPEDS) 16.1 (2025): 243-250, doi:10.11591/ijpeds.v16.i1.pp243-250, doi: http://doi.org/10.11591/ijpeds.v16.i1.pp243-250.
7. Januar Al Amien, et al. " Enhancing attack detection in IoT through integration of weighted emphasis formula with XGBoost." Indonesian Journal of Electrical Engineering and Computer Science. Vol.38, No.1, April 2025, pp. 641∼648, doi.org/10.11591/ijeecs.v38.i1.pp641-648.
8. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications" IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017, doi:10.1109/JIOT.2017.2683200.
9. Al-madni, Ali Mansour, et al. "An Optimized Blockchain Model for Secure and Efficient Data Management in Internet of Things." 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS). IEEE, 2024.
10. Manjula Hebbaka, et al. " An intrusion detection system against RPL-based routing attacks for IoT networks." Indonesian Journal of Electrical Engineering and Computer Science. Vol.34, No.2, 2024, pp. 1324∼1335, doi.org/10.11591/ijeecs.v34.i2.pp1324-1335.
11. Boualam, Soukayna Riffi, et al. "Secure and efficient routing protocol for low-power and lossy networks for IoT networks." Indonesian Journal of Electrical Engineering and Computer Science 27.1 (2022): 478-487, doi.org/10.11591/ijeecs.v27.i1.pp478-487.
12. Rajmohan, Tanusan, Phu H. Nguyen, and Nicolas Ferry. "A decade of research on patterns and architectures for IoT security." Cybersecurity 5.1, 2022, doi:10.5220/0009583001380149.
13. Khraisat, Ansam, and Ammar Alazab. "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges." Cybersecurity 4: 1-27, 2021, doi.org/10.1186/s42400-021-00077-7.
14. Fathi, Islam S., et al. "Protecting IOT Networks Through AI-Based Solutions and Fractional Tchebichef Moments." Fractal and Fractional (2025).
15. Ilango, Harun Surej, Maode Ma, and Rong Su. "A feedforward–convolutional neural network to detect low-rate dos in iot." Engineering Applications of Artificial Intelligence 114: 105059, 2022, doi.org/10.1016/j.engappai.2022.105059.
16. Van Tanh, Nguyen, Ngo Quang Tri, and Mai Manh Trung. "The solution to improve information security for IoT networks by combining lightweight encryption protocols." Indonesian Journal of Electrical Engineering and Computer Science 23.3 (2021): 1727-1735, doi.org/10.11591/ijeecs.v23.i3.pp1727-1735.
17. Ghali, Abdulrahman Aminu, Rohiza Ahmad, and Hitham Alhussian. "A framework for mitigating ddos and dos attacks in iot environment using hybrid approach." Electronics 10.11: 1282, 2021, doi.org/10.3390/electronics10111282.
18. Ahanger, Tariq Ahamad. "Defense scheme to protect IoT from cyber-attacks using AI principles." International Journal of Computers Communications & Control 13.6: 915-926, 2018, doi:10.15837/ijccc.2018.6.3356.
19. Mehra, M.; Paranjape, J.N.; Ribeiro, V.J. "Improving ML Detection of IoT Botnets using Comprehensive Data and Feature Sets" In Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 5–9; pp. 438–446 January 2021, doi.org/10.3390/su142316002.

20. Dutt, I.; Borah, S.; Maitra, I.K. “Immune system based intrusion detection system (IS-IDS): A proposed model”. IEEE Access, 8, 34929–34941, 2020, doi:10.1109/ACCESS.2020.2973608.
21. Aldhaheri, S.; Alghazzawi, D.; Cheng, L.; Alzahrani, B.; Al-Barakati, A. DeepDCA: “Novel network-based detection of IoT attacks using artificial immune system”. Appl. Sci. 10, 1909, 2020, doi.org/10.3390/app10061909.
22. Singh, S.K.; Rathore, S.; Park, J.H. “Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence”. Future Gener. Comput. Syst, 110, 721–743, 2020, doi.org/10.1016/j.future.2019.09.002.
23. El Alami, Abdelmajid, et al. “Quaternion discrete orthogonal Hahn Moments convolutional neural network for color image classification and face recognition.” Multimedia Tools and Applications 82.21 (2023): 32827-32853.
24. Aldakheel, Eman Abdullah, et al. “Efficient Analysis of Large-Size Bio-Signals Based on Orthogonal Generalized Laguerre Moments of Fractional Orders and Schwarz–Rutishauser Algorithm.” Fractal and Fractional 7.11 (2023): 826.
25. Hoang, Van-Thanh, and Kang-Hyun Jo. “Practical analysis on architecture of EfficientNet.” 2021 14th International Conference on Human System Interaction (HSI). IEEE, 2021.
26. Ishaq, Ahmad, et al. “Improved EfficientNet architecture for multi-grade brain tumor detection.” Electronics 14.4 (2025): 710.
27. Fathi, Islam S., et al. “Fractional Chebyshev Transformation for Improved Binarization in the Energy Valley Optimizer for Feature Selection.” Fractal and Fractional 9.8 (2025): 521.
28. Daoui, Achraf, et al. “Fast and stable computation of higher-order Hahn polynomials and Hahn moment invariants for signal and image analysis.” Multimedia Tools and Applications 80.21 (2021): 32947-32973.
29. Jin, Xin, et al. “Delving deep into spatial pooling for squeeze-and-excitation networks.” Pattern Recognition 121 (2022): 108159.
30. Shu, Xiangbo, et al. “Expansion-squeeze-excitation fusion network for elderly activity recognition.” IEEE Transactions on Circuits and Systems for Video Technology 32.8 (2022): 5281-5292.
31. Ullah, Farhan, et al. “Source code authorship attribution using hybrid approach of program dependence graph and deep learning model.” IEEE Access 7 (2019): 141987-141999.