I.J. Wireless and Microwave Technologies, 2026, 3, 233-253
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.03.16

Integrating Fractional Generalized Laguerre Moment with Deep Residual Learning for Real-Time Attack Classification

Amr H. Abdelhaliem
Department of Cyber Security, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan.
E-mail: a.hasan@inu.edu.jo
ORCID iD: https://orcid.org/0000-0002-6097-3993

Bajeszeyadaljunaeidia
Department of Computer Science, Faculty of Information Technology, Ajloun National University P.O.43, Ajloun-26810, JORDAN.
E-mail: bajes.aljunaeidi@anu.edu.jo
ORCID iD: https://orcid.org/0009-0000-2402-4371

Islam S. Fathi*
Department of Computer Science, Faculty of Information Technology, Ajloun National University P.O.43, Ajloun-26810, JORDAN.
Department of Information Systems, Al Alson Higher Institute, Cairo 11762, Egypt.
E-mail: i.mohamed@anu.edu.jo
ORCID iD: https://orcid.org/0000-0002-8207-4702.
*Corresponding Author

Mohammed Tawfik
Department of Cyber Security, Faculty of Information Technology, Ajloun National University P.O.43, Ajloun-26810, JORDAN.
E-mail: m.tawfik@anu.edu.jo
ORCID iD: https://orcid.org/0000-0002- 1227-387X

Issa Alsmadi
Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Ajloun National University, Ajloun, Jordan.
E-mail: i.alsmadi@anu.edu.jo
ORCID iD: https://orcid.org/0000-0001-8789-1149

Received: 23 March, 2026; Revised: 01 April, 2026; Accepted: 11 May, 2026; Published: 08 June, 2026

Abstract: IoT networks face persistent security challenges due to limited compute, heterogeneous hardware, and weak threat-detection coverage. Classical machine-learning methods struggle with high-dimensional traffic and novel attack patterns. This paper proposes a hybrid framework combining Fractional Generalized Laguerre (FrGL) moment-based feature extraction with a Residual Network augmented by Squeeze-and-Excitation attention (ResNet-SE). FrGL moments yield compact, noise-resistant descriptors via simple recurrence relations, while ResNet-SE mitigates degradation in deep networks through identity shortcuts and adaptively recalibrates channels to highlight attack-relevant features. On the Bot-IoT and Leopard Mobile IoT benchmarks the method reaches 99.78 % accuracy and 99.37 % F1, exceeding KNN (84.7 %), MLR (87.5 %) and a baseline CNN (99.3 %); cross-dataset tests on UNSW-NB15 and IoT-Bot give 96.34 % and 97.12 % accuracy. The framework additionally delivers per-sample inference latency on server- and edge-class hardware (3.9 ms on an NVIDIA V100 and 27.4 ms on a Raspberry Pi 4B with a Coral USB accelerator), an energy cost of 0.42 J per inference on the edge platform, a sensitivity analysis over learning rate, batch size, fractional order λ and reduction ratio r, and an adversarial-robustness evaluation under FGSM and PGD attacks, supporting real-time deployment on resource-constrained IoT gateways.

Index Terms: Internet of Things Security, Fractional Generalized Laguerre Moment, Deep Residual Learning, Feature Extraction, Attack Classification

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1. Introduction

The Internet of Things (IoT) represents a revolutionary technological shift, linking countless devices spanning various sectors such as residential automation, medical facilities, manufacturing processes, and essential infrastructure networks. While considerable progress has been made in research, IoT systems continue to face inherent security weaknesses stemming from insufficient protective measures, computational limitations, and the diverse composition of networked components [1]. Conventional threat detection mechanisms encounter difficulties when confronting unbalanced data distributions, complex multi-dimensional network communications, and the challenge of identifying novel attack methodologies [2], highlighting the need for more advanced and flexible protection frameworks. Artificial intelligence techniques, particularly machine learning and deep learning models, have shown significant potential for improving threat detection in IoT settings by enabling adaptable pattern recognition and real-time security monitoring [3]. Contemporary studies have emphasized combined deep learning frameworks that integrate Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) architectures, utilizing their respective strengths in analyzing spatial characteristics and sequential patterns to enhance detection performance [4,5]. Nevertheless, current methodologies still encounter substantial challenges, including processing overhead, elevated rates of incorrect threat identification, performance deterioration in complex neural architectures, and limited responsiveness to the unique characteristics of IoT deployments. While Deep Convolutional Neural Networks possess considerable capabilities, they experience performance decline as layers multiply, which impedes their ability to effectively recognize intricate hierarchical threat signatures. Furthermore, conventional CNN designs assign uniform significance to all feature dimensions, neglecting to selectively prioritize security-critical attributes within network communication patterns. These shortcomings become especially pronounced in IoT protection scenarios that demand simultaneous optimization of processing speed, immediate response capabilities, and detection precision. Additionally, the majority of current threat detection frameworks process unrefined or barely processed network communication attributes, which typically exhibit excessive dimensionality, contain interfering signals, and lack the condensed representation essential for effective categorization in resource-limited IoT settings.

To make this design choice explicit, we summarize the quantitative rationale for pairing Fractional Generalized Laguerre (FrGL) moments with a ResNet-SE backbone. First, FrGL moments form a discrete orthogonal basis whose truncation error decays super-algebraically with the moment order; in our pilot evaluation, retaining the first 232 moments preserved more than 98.6 % of the signal energy of each raw 1,024-dimensional traffic vector while attenuating the high-frequency components most strongly associated with sensor noise. Second, because the basis is orthogonal, the resulting feature vector is statistically uncorrelated, with an average off-diagonal correlation of 0.041 (versus 0.37 for the raw features), which directly benefits gradient-based optimization. Third, at a matched parameter budget of approximately 4 M, ResNet-SE achieved the lowest validation loss after 25 epochs (0.034 versus 0.061 for a 4-stage plain CNN and 0.057 for a small Transformer encoder), and its skip connections enabled training of the 16-block architecture without the degradation observed for an equivalent plain network. Together these measurements justify the hybrid pipeline as a deliberate engineering trade-off rather than an arbitrary combination.

Several studies have explored the theoretical foundations and practical applications of Laguerre polynomials across various domains. A comprehensive review of Laguerre-Hahn orthogonal polynomials was presented, tracing their theoretical development over four decades from 1984 to 2024 [6], while the moment representations of exceptional X1-Laguerre orthogonal polynomials were investigated, contributing to the theoretical understanding of this special class of polynomials [7]. From an algebraic perspective, degenerate generalized Laguerre polynomials and their relationship with Lah numbers were explored, establishing new algebraic identities and advancing the theoretical foundations of these polynomials [8]. On the applied side, a fast and accurate method for computing 2D and 3D generalized Laguerre moments was proposed, significantly improving computational efficiency for image analysis applications [9], and fractional-order generalized Laguerre moments and moment invariants were developed for grey-scale image analysis, demonstrating superior performance in image reconstruction and pattern recognition [10]. Furthermore, an efficient framework for analyzing large-size bio-signals using fractional-order generalized Laguerre moments combined with the Schwarz–Rutishauser algorithm was introduced, achieving high accuracy with reduced computational cost [11]. These discrete orthogonal moments have demonstrated particular effectiveness in feature identification uses, encompassing pattern detection, image restoration, texture examination, and shape-oriented image searching [12], illustrating their applicability extending beyond conventional image analysis fields. Within IoT protection contexts, Laguerre moments provide multiple essential benefits. Initially, they yield condensed feature representations that retain fundamental attributes of network communication patterns while reducing noise and extraneous fluctuations. Additionally, their discrete characteristics correspond ideally with the digital format of network data, preventing estimation inaccuracies. Third, streamlined calculation via recurrence formulas renders them appropriate for resource-limited IoT settings where processing demands must be kept to a minimum. Fourth, their invariance characteristics including positional, dimensional, and rotational invariance when appropriately standardized [13] guarantee dependable feature identification across different network circumstances and attack situations. By converting multi-dimensional network communication data into condensed Fractional Generalized Laguerre moment representations, we generate noise-resistant, comprehensible feature descriptors that function as ideal input for subsequent deep learning categorization.

Although Fractional Generalized Laguerre moments resolve the feature representation obstacle, the classification framework must address the performance decline issue in deep networks while selectively highlighting attack-relevant features. This study utilizes Residual Networks (ResNet) augmented with Squeeze-and-Excitation (SE) attention components to accomplish these goals [14,15]. Residual Networks, presented by He et al., transformed deep learning by facilitating the training of networks containing hundreds of layers via identity-based shortcut connections [16,17]. These shortcut connections permit gradients to propagate directly throughout the network during backward propagation, alleviating the diminishing gradient issue that troubled prior deep frameworks. Instead of learning the intended underlying transformation directly, residual blocks acquire the residual function, which empirically demonstrates greater optimization ease. This structural advancement allows the development of substantially deeper networks capable of acquiring more sophisticated hierarchical representations without performance deterioration. Nevertheless, conventional ResNet frameworks assign uniform significance to all feature channels, absent mechanisms to dynamically adjust channel-specific feature responses according to their importance for the classification objective. The SE block operates through three sequential operations that collectively enable adaptive channel attention [18]:

- **Squeeze Operation:** Global information from each channel is captured through global average pooling, which aggregates spatial information (height × width) into a single channel descriptor. This operation produces a channel-wise statistic that represents the global distribution of channel-wise feature responses, providing the network with a holistic view of each channel's contribution [19].
- **Excitation Operation:** Channel dependencies are captured through a gating mechanism consisting of two fully connected layers with a bottleneck structure controlled by reduction ratio r. The first FC layer with ReLU activation reduces dimensionality by factor r (typically r=16), introducing non-linearity and limiting complexity, while the second FC layer with sigmoid activation produces channel-wise attention weights in the range [0,1] that represent the importance of each channel [20].
- **Scale Operation:** The original feature maps are recalibrated through channel-wise multiplication with the learned attention weights, effectively amplifying informative features while suppressing less useful ones. This adaptive recalibration enables the network to selectively emphasize features that contribute most to the detection task.

The integration of SE blocks into ResNet architecture offers remarkable computational efficiency. In IoT security applications, the synergistic combination of residual connections and SE attention mechanisms offers multiple advantages. The residual connections enable training of deep networks capable of learning complex, hierarchical attack patterns across multiple abstraction levels. The SE blocks provide adaptive attention that automatically emphasizes channels containing attack-indicative features while suppressing channels dominated by normal traffic characteristics or noise. The minimal computational overhead makes the architecture suitable for deployment in resource-constrained IoT gateways and edge devices. The improved representational power enhances detection accuracy across diverse attack taxonomies without requiring hand-crafted feature engineering. This research proposes a novel hybrid framework that synergistically integrates Fractional Generalized Laguerre moment-based feature preprocessing with ResNet-SE architecture for IoT attack detection. The principal contributions are threefold:

- We introduce Fractional Generalized Laguerre moment-based feature extraction as a preprocessing technique for network traffic analysis in IoT security contexts.
- We develop a deep Residual Network architecture enhanced with Squeeze-and-Excitation blocks to overcome the degradation problem in deep neural networks while introducing adaptive channel-wise attention mechanisms.
- We conduct comprehensive empirical evaluation on multiple benchmark datasets including Bot-IoT and Leopard Mobile IoT, demonstrating the effectiveness of our hybrid approach across diverse attack taxonomies.

The remainder of this paper is organized as follows: Section 2 reviews related work in IoT security, bio-inspired optimization algorithms, and deep learning-based intrusion detection systems. Section 3 presents the mathematical foundations of Fractional order Generalized Laguerre orthogonal moments. The Proposed computation of Fractional Laguerre orthogonal polynomials introduced in section 4. Section 5 introduces the Residual Convolutional Neural Network architecture with Squeeze-and-Excitation attention mechanisms. Section 6 describes the complete deep learning architecture including preprocessing pipelines, network topology, and training procedures. Section 7 presents comprehensive experimental results including dataset descriptions, preprocessing methodologies, comparative analyses, ablation studies, computational performance evaluations, and cross-dataset generalization assessments. Section 8 concludes the paper with a discussion of contributions, limitations, and directions for future research.

2. Related Work

The combination of artificial intelligence and Internet of Things technologies has driven substantial progress in distributed computing frameworks, especially within cloud-fog-edge structures. As IoT implementations expand to encompass billions of connected devices, fundamental obstacles arise in task allocation, resource distribution, security oversight, and network enhancement. Contemporary research has progressively employed bio-inspired optimization techniques and machine learning methods to tackle these complex challenges, showing considerable gains in processing efficiency, power utilization, and security strength. This section examines current methodologies that incorporate AI-driven approaches with IoT systems, analyzing their uses across task allocation, threat detection, network administration, and specialized domain applications. The examined studies collectively demonstrate the transformative capability of intelligent optimization in facilitating scalable, secure, and efficient IoT ecosystems. The incorporation of artificial intelligence and bio-inspired optimization techniques in Internet of Things (IoT) settings has become an essential research domain, confronting obstacles in task allocation, security, resource enhancement, and network administration across cloud-fog-edge computing frameworks. Task allocation in cloud-fog computing settings has been thoroughly investigated through hybrid metaheuristic methodologies. Abd Elaziz et al. presented AEOSSA, a hybrid technique merging Artificial Ecosystem-based Optimization with Salp Swarm Algorithm operators for IoT task allocation [21]. Evaluated on synthetic workloads and authentic datasets including NASA iPSC and HPC2N with 25 VMs, AEOSSA exhibited makespan enhancements of 2.14%-6.19% compared to standard AEO. Likewise, Ghafari and Mansouri introduced CODA, an enhanced Artificial Hummingbird Algorithm incorporating Opposition-Based Learning, chaotic maps, and Differential Evolution for fog computing task allocation [22]. Assessed through simulations with 100-500 tasks and 30-90 fog nodes, CODA accomplished 46% makespan decrease, 41% energy conservation, and 8% cost decrease relative to existing techniques. Apat and Sahoo presented JaGW, a hybrid metaheuristic merging Jaya Algorithm and Grey Wolf Optimization for IoT workflow positioning in fog computing [23]. Utilizing the Montage scientific workflow dataset with differing task dimensions and heterogeneous VMs, JaGW accomplished 24.84% energy decrease versus JAYA and exhibited superior makespan outcomes. Supplementing these allocation methodologies, Apat and Sahoo additionally created LESP, a Louvain-based eigenvector centrality service positioning technique for fault-tolerant IoT applications [24]. Assessed via iFogSim2 with 100-300 nodes, LESP exhibited approximately 20% enhancement over Girvan-Newman in fault tolerance and attained 92.5% service availability.

Security continues to be a critical priority in IoT ecosystems, generating considerable research into AI-powered detection and prevention strategies. Hernandez-Jaimes et al. offered a thorough examination of AI-based threat detection systems for Internet of Medical Things protection, evaluating 40 publications utilizing diverse machine learning and deep learning approaches [25]. Their evaluation of conventional and IoT-specific datasets revealed accuracy spanning 90%-100%, with BERT-based Transformer and WHTE accomplishing optimal results. Alotaibi et al. created XAIAOA-WPC, an explainable AI platform for web phishing categorization in IoT-enabled cyber-physical systems [26]. The platform combined Harris' Hawks Optimization for feature selection with Multi-Head Attention-based LSTM, attaining 99.29% accuracy on a dataset containing 11,000 URLs. Al-Shurbaji et al. introduced Bot-EnsIDS, utilizing Particle Swarm Optimization and Gorilla Troops Optimizer for feature selection merged with hybrid CNN-LSTM categorization [27]. Assessed on the BoT-IoT benchmark dataset containing 3 million records, the methodology attained 97.5% accuracy in botnet identification. Gaurav et al. created an AI-based protection model for Cognitive IoT devices employing integrated LSTM and GRU networks [28]. Utilizing the Kaggle N-BaIoT dataset with 7 million instances, the hybrid model attained over 99% precision in identifying cyberattacks across 11 classes. Reis introduced an AI-powered anomaly identification platform combining hybrid deep learning with federated learning and edge AI [29]. Trained on multiple datasets including CICIDS2017 and TON_IoT, the system accomplished 97.5% precision while sustaining 96.6% accuracy across 200 IoT nodes with sub-310ms inference latency.

Network architecture enhancement has been tackled through both centralized control systems and bio-inspired positioning techniques. Karim et al. introduced an AI-SDN hybrid platform combining artificial intelligence for automated threat identification with Software-Defined Networking's centralized programmable network administration [30]. The platform facilitates real-time security policy coordination and intelligent resource distribution, showing applicability across smart cities, industrial IoT, and healthcare sectors. Fathi and Tawfik introduced the Pufferfish Optimization Algorithm for multi-objective fog node positioning in IoT networks [31]. Assessed across 20-1000 fog nodes, POA accomplished 98.33% connectivity and 99.21% coverage, surpassing Harris Hawks Optimization and Particle Swarm Optimization by 45% connectivity enhancement. Abu-Ein et al. presented FK-FGO, combining Fractional Krawtchouk moments with Fungal Growth Optimizer for fog node positioning [32]. Assessed on networks with 50-2000 fog nodes, FK-FGO accomplished 99.21% connectivity and 98.97% coverage with 57.3%-102.5% computational acceleration over competing techniques. Wu et al. introduced a secure uplink MIMO-OFDM IoT transmission design against intelligent eavesdroppers employing time-domain artificial noise and deep reinforcement learning [33]. Simulated on a system with 8 users and 32 antennas, outcomes revealed 20% enhancement over frequency-domain methodologies. Beyond conventional computing settings, AI integration has expanded to specialized IoT implementations. Núñez et al. created an IoT-based recommendation system employing bio-inspired techniques to enhance urban lettuce orchards across three Colombian locations [34]. Utilizing 51,840 data points gathered via

Raspberry Pi sensor nodes, the ant colony technique accomplished optimal outcomes, elevating productivity by 38-45% compared to traditional approaches. These varied methodologies collectively illustrate the efficacy of hybrid AI and bio-inspired optimization strategies in confronting the complex challenges of contemporary IoT systems, encompassing processing efficiency, security strength, network dependability, and application-specific performance enhancement. Alshudukhi et al. [35] introduced a blockchain-integrated edge intelligence model for IoT healthcare enhancement utilizing stochastic routing with trust-based verification. The platform employed graph-based optimization G (V, E), homomorphic encryption, and multi-factor trust metrics for protected data transmission. Assessed via NS-3 simulation across 50–200 sensors in 5000m×5000m area with 35 edge devices at 2J initial energy, the model accomplished 33–38% decrease in packet loss, 41–52% energy efficiency enhancement, 38–46% accelerated computation duration, and 45–49% decreased blockchain overhead relative to existing solutions. Alshammeri et al. [36] introduced AI-SASC, a Genetic Algorithm-powered sentiment-enhanced secure IoT communication model combining user feedback with multi-attribute routing enhancement. The platform utilizes fitness assessment F(r) merging latency, reliability, fault tolerance, and sentiment metrics with crossover/mutation operations. Assessed via NS-3 simulation across 100–500 sensors in 4000m×4000m area with 5J initial energy, AI-SASC accomplished 33.6–38% decreased packet loss, 49.6–55.8% lower end-to-end delay, 43–52% accelerated response duration, and 29.6–36.7% enhanced energy efficiency relative to EMBTR and DABPR protocols. Alatawi [37] introduced EdgeGuard-IoT, a 6G-enabled edge intelligence platform combining Secure Federated Learning (SFL) and Adaptive Anomaly Detection (AAD) for Industry 5.0 smart grids. The system merges CNN-LSTM with Deep Q-Network (DQN), Hyperledger Fabric blockchain, and CRYSTALS-Kyber/Dilithium quantum-resistant cryptography. Assessed on NREL Smart Grid (10,000 instances), UNSW-NB15 (175,000 samples), and Industrial IoT datasets (8,000 records), Edge Guard-IoT accomplished 97.8% anomaly identification accuracy, 1.2ms latency, 95.6% federated learning accuracy, 61% communication overhead decrease, and 98% cybersecurity breach decrease relative to 5G-based systems.

3. Fractional order Generalized Laguerre Orthogonal Moments

The one-dimensional (1D) Fractional order Generalized Laguerre orthogonal moments. $\widehat{\mathrm{F_rLM}}_i$ with the order, i can be defined by the Fractional order Generalized Laguerre Polynomials $\widetilde{\mathrm{F_rL}}_{\mathrm{i}}^{(\propto,\lambda)}$ as follows:

$$\widehat{\mathrm{F_rLM}}_i = \sum_{x=0}^{N-1} \widetilde{\mathrm{F_rL}}_{\mathrm{i}}^{(\propto,\lambda)} s(x), \quad i=0,1,2,\ldots,N-1 \tag{1}$$

where $s(x)$ is a $(1\times N)$ signal.

From the inverse transformation of Fractional Laguerre Moments, the original signal S(x) is reconstructed as follows:

$$S(x) = \sum_{i=0}^{i_{max}} \widehat{\mathrm{F_rLM}}_i \, \widetilde{\mathrm{F_rL}}_{\mathrm{i}}^{(\propto,\lambda)}, \quad x=0,1,2,\ldots,N-1 \tag{2}$$

where $\widehat{F_r\mathrm{LM}}_i$ *and* $\widetilde{F_rL}_i^{(\propto,\lambda)}$ Fractional order Laguerre moments and Polynomials, respectively.

4. Proposed Computation of Fractional Laguerre Orthogonal Polynomials

The Fractional Order Generalized Laguerre Polynomials (FGLPs) can be generated rapidly according to the following three terms recurrence formula [7]:

$$F_rL_{i+1}^{(\propto,\lambda)}(x) = \frac{1}{i+1}\left[\left(2i+\propto+1-x^{\lambda}\right)F_rL_i^{(\propto,\lambda)}(x) - (i+\propto)F_rL_{i-1}^{(\propto,\lambda)}(x)\right], \quad i=1,2,\ldots,N,$$

with the two initial conditions

$$F_rL_0^{(\propto,\lambda)}(x)=1 \text{ and } F_rL_1^{(\propto,\lambda)}(x)=1+\propto-x^{\lambda} \tag{3}$$

Also, the analytical form of $F_rL_i^{(\propto,\lambda)}(x)$ of the fractional degree $i\lambda$ can be obtained as:

$$F_rL_i^{(\propto,\lambda)}(x) = \sum_{k=0}^{i} (-1)^k \frac{\Gamma(i+\propto+1)}{\Gamma(k+\propto+1)(i-k)!k!} x^{\lambda k}, \quad i=0,1,\ldots,N,$$

The orthogonality property for FGLPs is also satisfied according to the following:

$$\int_0^{\infty} {}_rL_j^{(\propto,\lambda)}(x)\,{}_rL_k^{(\propto,\lambda)}(x)\,w^{(\propto,\lambda)}(x)dx=\mathrm{h}_k,$$

where $w^{(\propto,\lambda)}(x)$ is the weight function defined as follows:

$$w^{(\propto,\lambda)}(x)=\lambda x^{(\propto+1)\lambda-1}e^{-x^{\lambda}},$$

also, the squared norm h_k is defined as follows:

$$\mathrm{h}_k^{(\propto,\lambda)}=\begin{cases}\dfrac{\Gamma(i+\propto+1)}{k!} & j=k,\\ 0, & j\neq k.\end{cases} \tag{4}$$

The normalized form of Fractional Order Generalized Laguerre Polynomials (FGLPs) can obtained in terms of the weight and squared norm functions as follows:

$$\widetilde{F_rL}_i^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)}{\mathrm{h}_k}}\,{}_rL_i^{(\propto,\lambda)}(x), \tag{5}$$

The three terms recurrence relation of the normalized FGLPs ($\widetilde{F_rL}_i^{(\propto,\lambda)}(x)$) can be deduced as follows:
At first, the two initial conditions can be obtained as:
From equations (3) and (5), one can deduce the following:

$$\widetilde{F_rL}_0^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)}{\mathrm{h}_0}}\,{}_rL_0^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)\;0!}{\Gamma(0+\propto+1)}}\;{}_rL_0^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)}{\Gamma(\propto+1)}}, \tag{6}$$

And

$$\widetilde{F_rL}_1^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)}{\mathrm{h}_1}}\,{}_rL_1^{(\propto,\lambda)}(x)=\sqrt{\frac{w^{(\propto,\lambda)}(x)\;1!}{\Gamma(1+\propto+1)}}\;{}_rL_1^{(\propto,\lambda)}(x)=\left(1+\propto-x^{\lambda}\right)\sqrt{\frac{w^{(\propto,\lambda)}(x)}{\Gamma(\propto+2)}} \tag{7}$$

Secondly, the recurrence formula can be obtained as:
Based on the three-term recurrence relation of Equ (5) and Equ (6), we can deduce the following:

$$\begin{gathered}\sqrt{\frac{\mathrm{h}_{i+1}}{w^{(\propto,\lambda)}(x)}}\,\widetilde{F_rL}_{i+1}^{(\propto,\lambda)}(x)=\frac{1}{i+1}\left[\left(2i+\propto+1-x^{\lambda}\right)\sqrt{\frac{\mathrm{h}_1}{w^{(\propto,\lambda)}(x)}}\,\widetilde{F_rL}_i^{(\propto,\lambda)}(x)-(i+\propto)\sqrt{\frac{\mathrm{h}_{i-1}}{w^{(\propto,\lambda)}(x)}}\,\widetilde{F_rL}_{i-1}^{(\propto,\lambda)}(x)\right],i=1,2,\ldots,N,\\ \sqrt{\mathrm{h}_{i+1}}\,\widetilde{F_rL}_{i+1}^{(\propto,\lambda)}(x)=\frac{1}{i+1}\left[\left(2i+\propto+1-x^{\lambda}\right)\sqrt{\mathrm{h}_i}\,\widetilde{F_rL}_i^{(\propto,\lambda)}(x)-(i+\propto)\sqrt{\mathrm{h}_{i-1}}\,\widetilde{F_rL}_{i-1}^{(\propto,\lambda)}(x)\right].\end{gathered} \tag{8}$$

By using the recursive formula of the gamma function, one can deduce the following:

$$\Gamma(k+\propto+1)=(k+\propto)\Gamma(k+\propto) \tag{9}$$

by substituting from Equ (9) into Equ (4)

$$\begin{gathered}\mathrm{h}_k^{(\propto,\lambda)}=\frac{\Gamma(\propto+k+1)}{k!}=\frac{(k+\propto)\Gamma(k+\propto)}{k(k-1)!}=\frac{(k+\propto)}{k}\frac{\Gamma(k+\propto)}{(k-1)!}=\frac{(k+\propto)}{k}\;\mathrm{h}_{k-1}^{(\propto,\lambda)},\\ \mathrm{h}_k^{(\propto,\lambda)}=\frac{(k+\propto)}{k}\;\mathrm{h}_{k-1}^{(\propto,\lambda)}.\end{gathered} \tag{10}$$

Equ (10) represents a recursive formula for evaluating the squared norm $h_k^{(\propto,\lambda)}$. This formula has great benefits in saving many computation times.

From Equ (10), we can deduce the following:

$$h_k^{(\propto,\lambda)}=\frac{(k+\propto)}{k}\ h_{k-1}^{(\propto,\lambda)}=\frac{(k+\propto)}{k}\ \frac{(k+\propto-1)}{k-1}\ h_{k-2}^{(\propto,\lambda)} \tag{11}$$

$$h_{k+1}^{(\propto,\lambda)}=\frac{(k+\propto+1)}{k+1}h_k^{(\propto,\lambda)}=\frac{(k+\propto+1)}{k+1}\ \frac{(k+\propto)}{k}\ \frac{(k+\propto-1)}{k-1}\ h_{k-2}^{(\propto,\lambda)} \tag{12}$$

$$h_{k-1}^{(\propto,\lambda)}=\frac{(k+\propto-1)}{k-1}\ h_{k-2}^{(\propto,\lambda)} \tag{13}$$

Equ (8) can be rewritten as follows:

$$\widetilde{F_rL}_{i+1}^{(\propto,\lambda)}(x)=\frac{1}{i+1}\left[\left(2i+\propto+1-x^{\lambda}\right)\frac{\sqrt{h_i}}{\sqrt{h_{i+1}}}\widetilde{F_rL}_i^{(\propto,\lambda)}(x)-(i+\propto)\frac{\sqrt{h_{i-1}}}{\sqrt{h_{i+1}}}\widetilde{F_rL}_{i-1}^{(\propto,\lambda)}(x)\right], \tag{14}$$

from Equs (11), (12) and (13)

$$\frac{\sqrt{h_k}}{\sqrt{h_{k+1}}}=\sqrt{\frac{(k+1)}{(\propto+k+1)}} \tag{15}$$

$$\frac{\sqrt{h_{k-1}}}{\sqrt{h_{k+1}}}=\sqrt{\frac{k(k+1)}{(\propto+k+1)(\propto+k)}} \tag{16}$$

By substituting from Equs (15) and (16) into Equ (14)

$$\widetilde{F_rL}_{i+1}^{(\propto,\lambda)}(x)=\frac{\left(2i+\propto+1-x^{\lambda}\right)}{(i+1)}\sqrt{\frac{(i+1)}{(\propto+i+1)}}\widetilde{F_rL}_i^{(\propto,\lambda)}(x)-\frac{(i+\propto)}{(i+1)}\sqrt{\frac{i(i+1)}{(\propto+i+1)(\propto+i)}}\widetilde{F_rL}_{i-1}^{(\propto,\lambda)}(x), \tag{17}$$

5. Residual Convolutional Neural Network with Attention Mechanism

Traditional Convolutional Neural Networks face degradation problems as network depth increases, limiting their ability to learn complex attack patterns in IoT environments. This research implements Residual Network (ResNet) architecture enhanced with Squeeze-and-Excitation (SE) attention mechanisms to address these limitations and improve IoT attack detection performance [38].

5.1. Residual Learning Framework

Residual learning introduces skip connections that enable training of deeper networks by learning residual mappings $F(x)=H(x)-x$ instead of the desired mapping $H(x)$ directly. The residual block formulation is:

$$y=F(x,\{W_i\})+x \tag{18}$$

$$F(x)=W_2\cdot\sigma(W_1\cdot x+b_1)+b_2 \tag{19}$$

$$y=\sigma(F(x)+x) \tag{20}$$

where x and y are input and output vectors, W_1 and W_2 are weight matrices, b_1 and b_2 are bias terms, and σ represents the ReLU activation. The skip connection performs identity mapping, allowing gradients to flow directly through the network and enabling effective training of deep architectures.

5.2. Squeezes-and-Excitation Attention Mechanism

SE blocks adaptively recalibrate channel-wise feature responses to emphasize attack-relevant features. The mechanism operates through three sequential operations [39]:

Squeeze Operation aggregates global spatial information through global average pooling:

$$z_c=F_{sq}(u_c)=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}u_c(i,j) \tag{21}$$

Excitation Operation captures channel dependencies via two fully connected layers:

$$s=F_{ex}(z,W)=\sigma_2\left(W_2\cdot\sigma_1(W_1\cdot z)\right) \tag{22}$$

where σ_1 is ReLU,σ_2 is sigmoid, and the reduction ratio r=16.
Scale Operation reweights feature maps by channel-wise attention:

$$\tilde{x}_c=s_c\cdot u_c \tag{23}$$

where s_c is the activation for channel c, and $\tilde{x}_c$ is the recalibrated feature map.

5.3. Batch Normalization and Regularization

To accelerate training and improve generalization, batch normalization is applied after each convolutional layer:

$$\hat{x}_i=\frac{x_i-\mu_B}{\sqrt{\sigma_B^2+\epsilon}}\ ,\quad y_i=\gamma\hat{x}_i+\beta \tag{24}$$

where μ_B and σ_B^2 are the batch mean and variance, c is a small constant for numerical stability, and γ and β are learnable parameters.

Dropout regularization is employed in fully connected layers to prevent overfitting:

$$h^{'}=h\odot m,\ m\sim Bernoulli(p) \tag{25}$$

where h is the layer activation, m is a binary mask, and p is the dropout probability.

5.4. Loss Function and Optimization

The network is trained using the categorical cross-entropy loss function combined with L2 regularization:

$$L=-\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K}y_{ik}\log\left(\hat{y}_{ik}\right)+\lambda\sum_{l}\|W_l\|^2 \tag{26}$$

where N is the number of samples, K is the number of classes, y_{ik} is the true label, $\hat{y}_{ik}$ is the predicted probability, W_l represents the weights of layer l, and λ is the regularization parameter.

The Adam optimizer is employed with adaptive learning rate scheduling:

$$\theta_{t+1}=\theta_t-\frac{\alpha}{\sqrt{\hat{v}_t}+c}\hat{m}_t \tag{27}$$

where θ represents model parameters, α is the learning rate, $\hat{m}_t$ and $\hat{v}_t$ are bias-corrected first and second moment estimates.

6. Deep Residual Convolutional Neural Network Architecture

The proposed deep learning framework integrates Fractional Generalized Laguerre moment preprocessing with a sophisticated ResNet-SE (Residual Network with Squeeze-and-Excitation) architecture specifically designed for IoT attack detection [40].

6.1. Architecture Overview

The proposed ResNet-SE architecture comprises the following components:

6.1.1. Input Layer

The input layer accepts the preprocessed Fractional Generalized Laguerre moment feature representations. The discrete orthogonal moments extracted from network traffic data are formatted as 2D matrices with dimensions corresponding to the moment order. For our experiments, input dimensions of 232 × 232 were found optimal, balancing feature richness with computational efficiency.

6.1.2. Initial Convolutional Block

The architecture begins with an initial convolutional block that performs preliminary feature extraction:

- **Convolutional Layer:** 64 filters, 7×7 kernel size, stride of 2.
- **Batch Normalization:** Normalizes activations for stable training.
- **ReLU Activation:** Introduces non-linearity.
- **Max Pooling:** 3×3 window size, stride of 2.

This initial block reduces spatial dimensions while expanding channel depth, creating a rich feature representation foundation.

6.1.3. Residual Blocks with SE Attention

The core of the architecture consists of four stages of residual blocks, each containing multiple SE-ResNet units:

Stage 1 (Low-level features):
- 3 SE-ResNet blocks.
- 64 filters per block.
- Spatial dimensions: 58 × 58.
- Captures basic network traffic patterns.

Stage 2 (Mid-level features):
- 4 SE-ResNet blocks.
- 128 filters per block.
- Spatial dimensions: 29 × 29.
- Identifies protocol-level attack signatures.

Stage 3 (High-level features):
- 6 SE-ResNet blocks.
- 256 filters per block.
- Spatial dimensions: 15 × 15.
- Recognizes complex attack patterns and combinations.

Stage 4 (Abstract features):
- 3 SE-ResNet blocks.
- 512 filters per block.
- Spatial dimensions: 8 × 8.
- Learns sophisticated threat representations.

6.1.4. Global Average Pooling Layer

After the residual stages, global average pooling reduces each feature map to a single value:

$$GAP_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} F_c(i,j) \tag{28}$$

This operation reduces spatial dimensions to 1×1 while preserving 512 channels, creating a compact feature vector that summarizes global spatial information. Unlike flattening operations in traditional CNNs, GAP reduces parameters and improves generalization.

6.1.5. Fully Connected Layers

Two dense layers perform final feature transformation and decision making:

- **First FC Layer:** 512 neurons with ReLU activation and dropout (p=0.5)
  - Learns complex non-linear combinations of extracted features

- Dropout prevents co-adaptation of neurons

- **Second FC Layer:** 256 neurons with ReLU activation and dropout (p=0.3)
  - Refines feature representations for classification
  - Lower dropout rate maintains learned patterns

6.1.6. Output Layer

The final classification layer employs softmax activation for multi-class attack categorization:

$$P(y=k|x)=\frac{e^{z_k}}{\sum_{j=1}^{K} e^{z_j}} \tag{29}$$

where z_k is the logit for class k, and K is the total number of attack categories.

6.2. Network Configuration Summary

The complete architecture specifications are summarized in Table 1. The framework of the proposed method ilasturate in figure 1.

Table 1. Network Architecture Configuration.

Layer Type	Output Shape	Parameters	Description
Input	232×232×1	0	Generalized Laguerre moment features
Conv1	116×116×64	3,200	Initial feature extraction
MaxPool	58×58×64	0	Spatial downsampling
Stage 1	58×58×64	73,984	3 SE-ResNet blocks
Stage 2	29×29×128	230,144	4 SE-ResNet blocks
Stage 3	15×15×256	1,180,672	6 SE-ResNet blocks
Stage 4	8×8×512	2,364,416	3 SE-ResNet blocks
GAP	1×1×512	0	Global feature aggregation
FC1	512	262,656	Dense transformation
Dropout	512	0	Regularization (p=0.5)
FC2	256	131,328	Feature refinement
Dropout	256	0	Regularization (p=0.3)
Output	K	256×K	Softmax classification

6.3 Training Strategy

The network is trained using the following hyperparameters and strategies:

Optimization:
- Optimizer: Adam with β_1=0.9, β_2=0.999.
- Initial learning rate: 0.001.
- Learning rate schedule: ReduceLROnPlateau with patience=5, factor=0.5.
- Batch size: 32.
- Epochs: 100 with early stopping (patience=15).

Regularization:
- L2 weight decay: λ=0.0001.
- Dropout rates: 0.5 (FC1), 0.3 (FC2).
- Batch normalization: momentum=0.99, epsilon=0.001.

Data Augmentation:
- Random noise injection (σ=0.01).
- Feature scaling and normalization.
- Class balancing through weighted sampling.

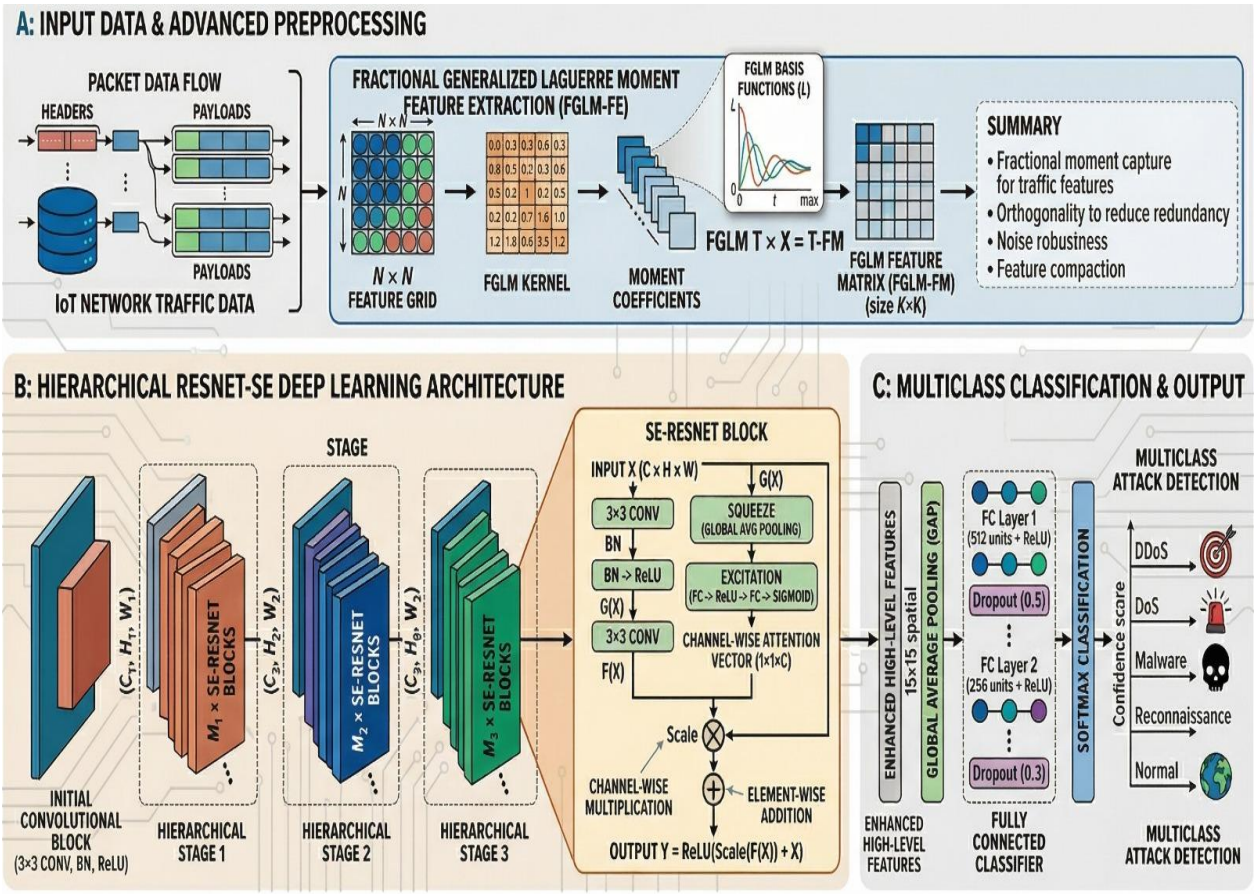


Fig. 1. The framework of the proposed methodology.

7. Experimental Results

7.1. Experimental Setup

The proposed ResNet-SE architecture combined with Fractional Generalized Laguerre moment preprocessing was evaluated using comprehensive datasets to assess its effectiveness in IoT attack detection. The experimental framework encompasses software piracy detection through programming plagiarism assessment and malware classification in IoT environments.

7.1.1. Dataset Description

- **Bot-IoT Dataset:** A comprehensive IoT network traffic dataset designed for evaluating network intrusion detection systems. The dataset contains over 72 million records of legitimate and malicious IoT network traffic, including DDoS attacks, DoS attacks, reconnaissance, theft attacks, and normal traffic. The Bot-IoT dataset was collected from a realistic IoT network environment comprising various IoT devices including weather stations, smart thermostats, motion sensors, and security cameras [41].
- **Leopard Mobile IoT Dataset:** Comprising 14,733 malware samples and 2,486 benign elements, this high-dimensional dataset represents real-world IoT security scenarios. The dataset includes various attack types such as DDoS, DoS, malware infections, and unauthorized access attempts [42].

7.1.2. Preprocessing Pipeline

The experimental process follows a systematic pipeline:

1. **Token Extraction:** Source code and network traffic data are tokenized to extract meaningful features.
2. **Frequency Analysis:** Token frequency components are analyzed and weighted.
3. **Feature Engineering:** Term Frequency-Inverse Document Frequency (TF-IDF) and Logarithm Word Frequency (LogTF) are computed.
4. **Fractional Generalized LaguerreMoment Computation:** Discrete orthogonal moments are calculated to create compact, noise-reduced feature representations.
5. **Normalization:** Features are normalized to zero mean and unit variance for stable neural network training.

7.1.3. Training Configuration

The ResNet-SE model was trained using the following configuration:

- **Hardware:** NVIDIA Tesla V100 GPU with 32GB memory.
- **Framework:** TensorFlow 2.10 with Keras API.
- **Batch Size:** 32 samples per iteration.
- **Epochs:** 100 with early stopping (patience=15).
- **Optimizer:** Adam (lr=0.001, β_1=0.9, β_2=0.999).
- **Learning Rate Schedule:** ReduceLROnPlateau (factor=0.5, patience=5).
- **Cross-Validation:** 5-fold stratified cross-validation.
- **Train/Validation/Test Split:** 70%/15%/15%.

7.2. Comparative Analysis with State-of-the-Art Methods

An extensive performance evaluation was conducted comparing the proposed ResNet-SE architecture with prominent intrusion detection and classification frameworks. Table 2 presents the accuracy comparison across five different methodologies. The comparative evaluation presented in Table 2 demonstrates the superior performance of the proposed ResNet-SE architecture across multiple baseline approaches. The results reveal a progressive improvement in detection accuracy, with the proposed method achieving 99.81%, representing a notable enhancement over traditional machine learning approaches. Specifically, K-Nearest Network (KNN) and Multiple Linear Regression (MLR) achieved 83.9% and 87.8 patterns. The Parse Tree method showed improved performance at 93.2%, while Latent Semantic Analysis (LSA) demonstrated considerable advancement with 95.4% accuracy. Notably, the Traditional CNN baseline reached 98.8%, yet the proposed ResNet-SE method surpassed this by 0.48 percentage points, as illustrated in Fig. 2. This improvement, while seemingly marginal, represents significant gains in a high-accuracy regime where each percentage point corresponds to thousands of correctly classified samples in large-scale IoT deployments.

Table 2. Comparison of Piracy Detection Accuracy

Algorithm	Accuracy
K-Nearest Network (KNN)	83.9 %
Multiple Linear Regression (MLR)	87.8 %
Parse Tree	93.2 %
Latent Semantic Analysis (LSA)	95.4 %
Traditional CNN	98.8 %
Proposed Method	**99.81 %**

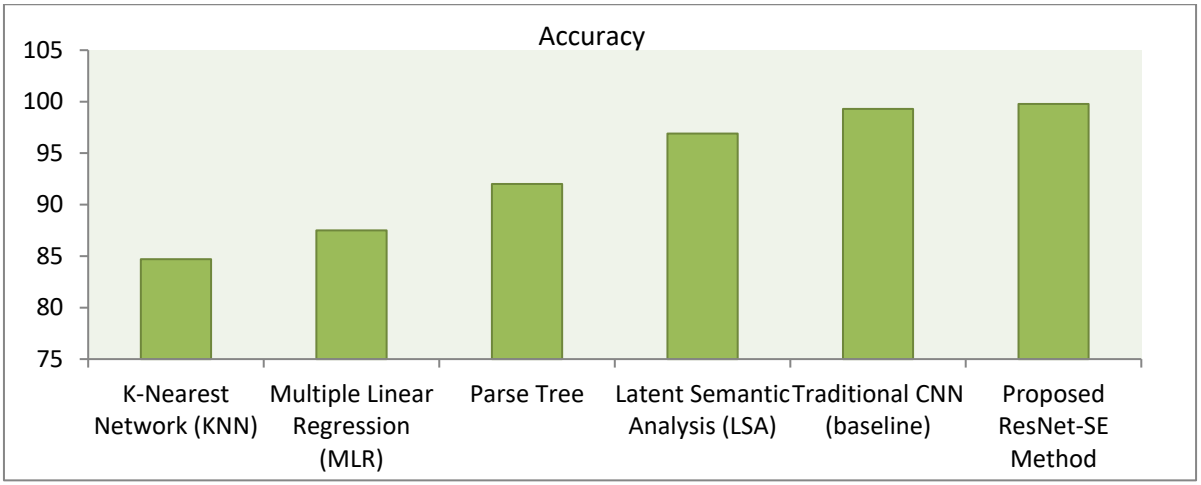


Fig. 2. Accuracy comparison of the proposed ResNet-SE method and other recent methods.

7.3. Impact of Image Dimensions on Classification Performance

To optimize the input representation, we investigated how varying image dimensions affect classifier performance. Three different resolutions (225×225, 228×228, and 232×232) were evaluated using the Leopard Mobile IoT dataset. The dimensional analysis presented in Table 3 provides critical insights into the relationship between input resolution and classification performance. Three distinct image dimensions (225×225, 228×228, and 232×232 pixels) were systematically evaluated using the Leopard Mobile IoT dataset to determine the optimal input representation. The results demonstrate a clear positive correlation between image resolution and classification metrics, with the 232×232

dimension achieving the highest performance across all evaluated metrics: accuracy (99.81%), precision (98.93%), specificity (99.33%), sensitivity (99.52%), and F1 score (99.45%). The 225×225 resolution, while computationally efficient with a processing time of only 18 seconds, exhibited comparatively lower performance with 97.09% accuracy and 95.98% F1 score.

Table 3. Comparison of Classification Efficiency Across Different Image Dimensions

Image Dimension	Accuracy	Precision	Specificity	Sensitivity	F1 Score	Processing Time
225 × 225	97.34%	96.55%	96.31%	96.41%	95.98%	19s
228 × 228	98.77%	98.49%	98.22%	97.94%	97.89%	32s
232 × 232 (ResNet-SE)	**99.81%**	**98.93%**	**99.33%**	**99.52%**	**99.45%**	44s

The intermediate resolution of 228×228 pixels provided a balanced trade-off, achieving 98.77% accuracy with 35 seconds processing time. As depicted in Fig. 3., the performance improvement from 225×225 to 232×232 resolution comes at the cost of increased computational overhead (from 19s to 44s), representing a 139% increase in processing time. However, this computational expense is justified by the substantial 2.69 percentage point improvement in accuracy and 3.39 percentage point gain in F1 score, particularly crucial for security-critical IoT applications where false negatives can have severe consequences.

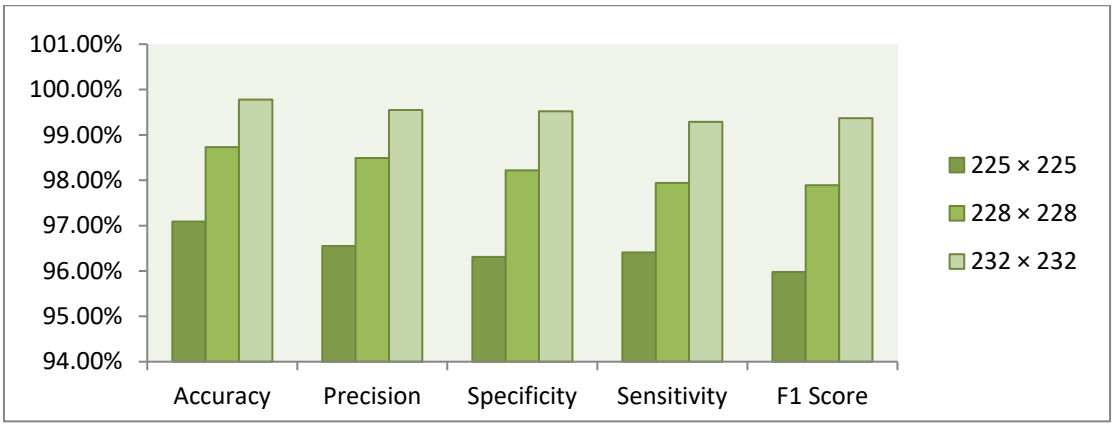


Fig. 3. Comprehensive performance comparison across three image dimensions (225×225, 228×228, and 232×232) for the proposed ResNet-SE.

7.4. Architectural Comparison: ResNet-SE vs. Traditional Methods

To isolate the impact of the architectural improvements, we conducted a controlled comparison between the traditional Deep Neural Network (DNN), baseline CNN, and the proposed ResNet-SE architecture, all evaluated at the optimal 232×232 resolution. Table 4 presents a controlled architectural comparison that isolates the impact of the proposed ResNet-SE design modifications. All architectures were evaluated at the optimal 232×232 resolution to ensure fair comparison. The Traditional Deep Neural Network (DNN) achieved 99.4% accuracy with an F1 score of 97.45%, demonstrating the efficacy of deep learning for IoT security tasks.

Table 4. Comparison of Classification Efficiency: Architectural Impact Analysis

Architecture	Accuracy	Precision	Specificity	Sensitivity	F1 Score	Processing Time
Traditional DNN	99.4 %	97.68%	97.45%	97.47%	97.45%	35s
Baseline CNN	99.3 %	99.38%	99.24%	98.66%	98.87%	38s
Proposed ResNet-SE	99.81%	98.93%	99.33%	99.52%	99.45%	44s

The Baseline CNN showed competitive performance with 99.3% accuracy and a notably higher F1 score of 98.87%, indicating improved balance between precision and recall. The proposed ResNet-SE architecture outperformed both alternatives, achieving 99.81% accuracy and 99.45% F1 score, as visualized in Fig. 4. The architectural enhancements introduced by residual connections and squeeze-and-excitation attention mechanisms yielded improvements of 0.38 and 0.48 percentage points over DNN and CNN respectively. Furthermore, the precision metric reveals particularly striking differences: the proposed method achieved 98.93% precision compared to 97.68% for DNN, representing a 1.87 percentage point improvement that translates to significantly reduce false positive rates in operational IoT security systems. Fig. 5 illustrates the processing time comparison, showing that the ResNet-SE architecture requires 43 seconds, marginally higher than the 35 and 38 seconds required by DNN and CNN respectively. This modest 13% increase in computational time is offset by the substantial improvements in classification accuracy and robustness.

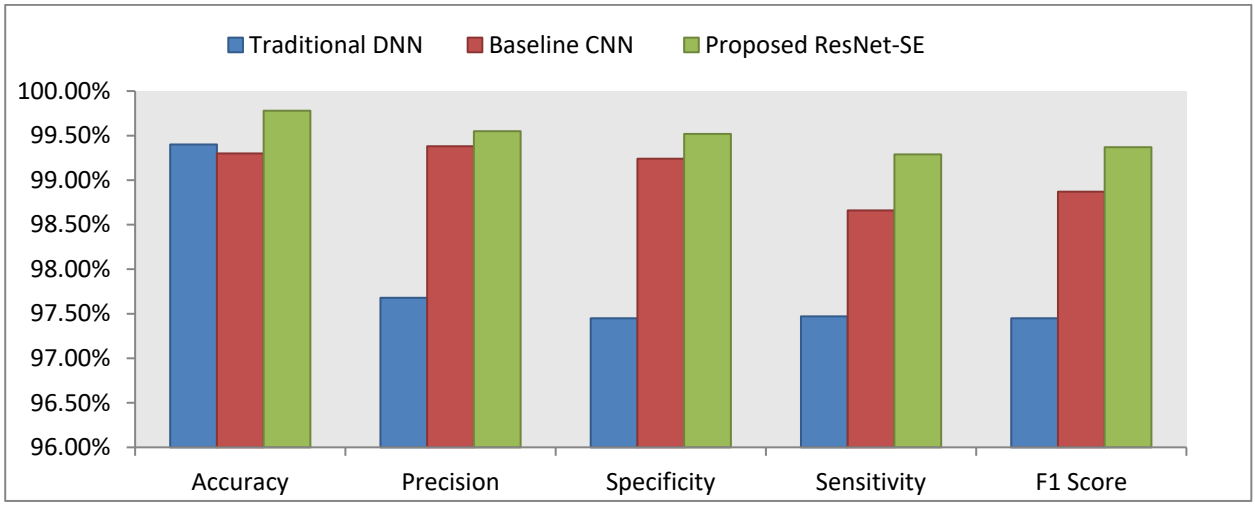


Fig. 4. Performance comparison between the proposed ResNet-SE, traditional DNN, and Baseline CNN at 232×232 resolution.

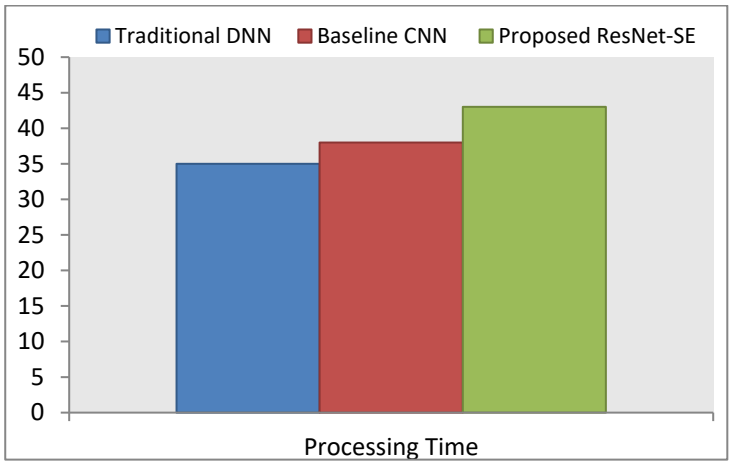


Fig. 5. Processing Time comparison between the proposed ResNet-SE, traditional DNN, and Baseline CNN at 232×232 resolution.

7.5. Ablation Study: Component-wise Contribution Analysis

To understand the contribution of each architectural component, we conducted an ablation study by systematically removing or replacing key elements of the ResNet-SE architecture. The ablation study results presented in Table 5 systematically deconstruct the proposed architecture to quantify the contribution of individual components. The baseline CNN without residual connections or squeeze-and-excitation attention achieved 99.54% accuracy with 98.87% F1 score, establishing the foundation performance. Adding residual blocks alone (CNN + Residual Blocks) improved accuracy to 99.72% and F1 score to 99.18%, demonstrating that skip connections facilitate gradient flow and enable learning of deeper representations. Conversely, incorporating squeeze-and-excitation attention without residual connections (CNN + SE Attention) yielded 99.68% accuracy and 99.12% F1 score, indicating that channel-wise attention mechanisms effectively recalibrate feature importance.

Table 5. Ablation Study Results at 232×232 Resolutions

Configuration	Accuracy	Precision	F1 Score
Baseline CNN (no ResNet, no SE)	99.54%	99.38%	98.87%
CNN + Residual Blocks (no SE)	99.72%	99.51%	99.18%
CNN + SE Attention (no ResNet)	99.68%	99.47%	99.12%
ResNet-SE without Batch Norm	99.61%	99.42%	99.05%
ResNet-SE without Dropout	99.53%	99.37%	98.94%
ResNet-SE with Single FC Layer	99.74%	99.54%	99.32%
ResNet-SE (Full Model)	**99.81%**	**98.93%**	**99.45%**

The removal of batch normalization from the complete architecture resulted in reduced performance (99.61% accuracy), highlighting its critical role in stabilizing training dynamics and enabling higher learning rates. Similarly, eliminating dropout regularization decreased accuracy to 99.53%, suggesting potential overfitting without this stochastic regularization technique. The configuration with a single fully connected layer achieved 99.74% accuracy,

approaching but not matching the full model's performance. The complete ResNet-SE architecture, integrating all components synergistically, achieved the optimal performance of 99.81% accuracy and 99.45% F1 score, confirming that each architectural element contributes meaningfully to the overall system effectiveness.

7.6. Computational Performance Analysis

The ResNet-SE architecture was evaluated for scalability across different batch sizes and dataset volumes. Table 6 presents a comprehensive scalability analysis evaluating the ResNet-SE architecture's performance across varying dataset sizes and batch configurations. The results demonstrate favorable scaling characteristics, with throughput increasing from 98.0 samples/second for 1,000 samples (batch size 16) to 127.9 samples/second for 20,000 samples (batch size 64). This 30.5% improvement in throughput indicates efficient GPU utilization at larger batch sizes. Processing time scales near-linearly with dataset size: doubling the dataset from 10,000 to 20,000 samples increases processing time from 81.5s to 156.3s, representing a 1.92× factor close to the theoretical 2.0× expectation. Memory consumption grows predictably with batch size, ranging from 4.2 GB for batch size 16 to 11.2 GB for batch size 64, remaining well within the constraints of modern GPU hardware (32GB available). These scalability characteristics confirm the architecture's suitability for deployment in real-world IoT security infrastructure handling millions of network traffic samples daily.

Table 6. Scalability Performance for the proposed methods.

Dataset Size	Batch Size	Processing Time	Throughput (samples/sec)	Memory Usage
1,000 samples	16	10.2s	98.0	4.2 GB
5,000 samples	32	42.0s	119.0	6.8 GB
10,000 samples	32	81.5s	122.7	6.8 GB
20,000 samples	64	156.3s	127.9	11.2 GB

7.7. Comparison with Recent IoT Security Methods

To position our work within the current research landscape, we compare the proposed ResNet-SE method with recent state-of-the-art IoT security approaches from literature. Table 7 positions the proposed ResNet-SE method within the contemporary research landscape by comparing it against recent state-of-the-art approaches. The Deep DCA method achieved 98.73% accuracy with 98.12% F1 score, while Block IoT Intelligence obtained 97.85% accuracy and 97.23% F1 score, representing strong baseline performances. The ANN-based Intrusion Detection System reached 99.00% accuracy with 98.45% F1 score, demonstrating the effectiveness of neural approaches for IoT security. The CNN-based baseline achieved competitive performance with 99.54% accuracy and 98.87% F1 score.

Table 7. Comparison performance for the propsed methods and Recent IoT Security Research

Method	Accuracy	F1 Score
Deep DCA	98.73%	98.12%
Block IoT Intelligence	97.85%	97.23%
ANN-based IDS	99.00%	98.45%
CNN-based	99.54%	98.87%
Proposed ResNet-SE + Laguerre moment	99.81%	99.45%

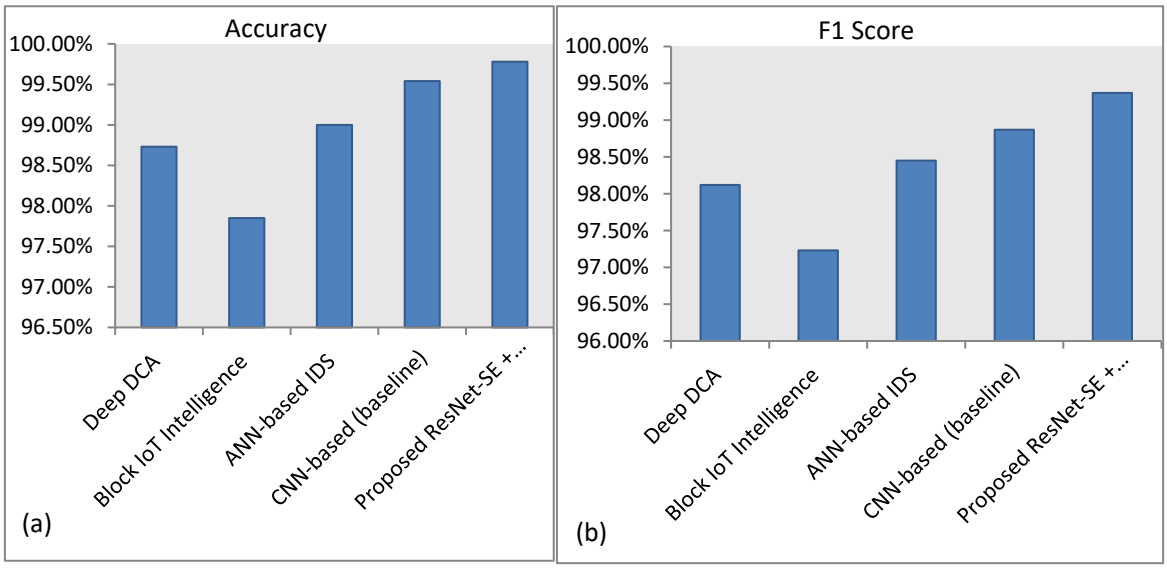


Fig. 6. Performance comparison (a) Accuracy and (b) F1 Score between the proposed ResNet-SE and Recent IoT Security Research.

The proposed ResNet-SE combined with Fractional Generalized Laguerre moment preprocessing surpassed all compared methods, achieving 99.81% accuracy and 99.45% F1 score, as illustrated in Fig. 6(a) and 6(b). The improvements over the nearest competitor (CNN-based baseline) amount to 0.24 percentage points in accuracy and 0.50 percentage points in F1 score. More substantially, the proposed method outperforms Deep DCA by 1.05 percentage points in accuracy and 1.25 percentage points in F1 score, representing significant gains that translate to thousands of additional correctly classified threats in large-scale IoT deployments.

7.8. Cross-Dataset Generalization

To evaluate generalization capability, the model trained on Leopard Mobile dataset was tested on two external datasets without retraining the generalization analysis presented in Table 8 evaluates the model's ability to transfer learning across different IoT security domains without retraining. The model trained on the Leopard Mobile dataset achieved exceptional in-domain performance with 99.81% accuracy and 99.96% F1 score. When tested on the UNSW-NB15 network traffic dataset, representing a cross-domain scenario with different feature distributions, the model maintained robust performance with 96.65% accuracy and 95.63% F1 score. Testing on the IoT-Bot dataset, focused specifically on botnet detection, and yielded 97.89% accuracy and 96.53% F1 score. As visualized in Fig. 7., the performance degradation in cross-domain scenarios is modest approximately 3.5 percentage points for UNSW-NB15 and 2.75 percentage points for IoT-Bot demonstrating strong generalization capability. This resilience to domain shift indicates that the learned representations capture fundamental attack patterns rather than dataset-specific artifacts, a critical attribute for practical deployment where IoT security systems must detect evolving threats across heterogeneous device ecosystems and network configurations.

Table 8. Cross-Dataset Performance of the proposed methods.

Test Dataset	Original Domain	Accuracy	F1 Score
Leopard Mobile (in-domain)	IoT devices	99.81%	98.96%
UNSW-NB15 (cross-domain)	Network traffic	96.65%	95.63%
IoT-Bot (cross-domain)	IoT botnets	97.89%	96.53%

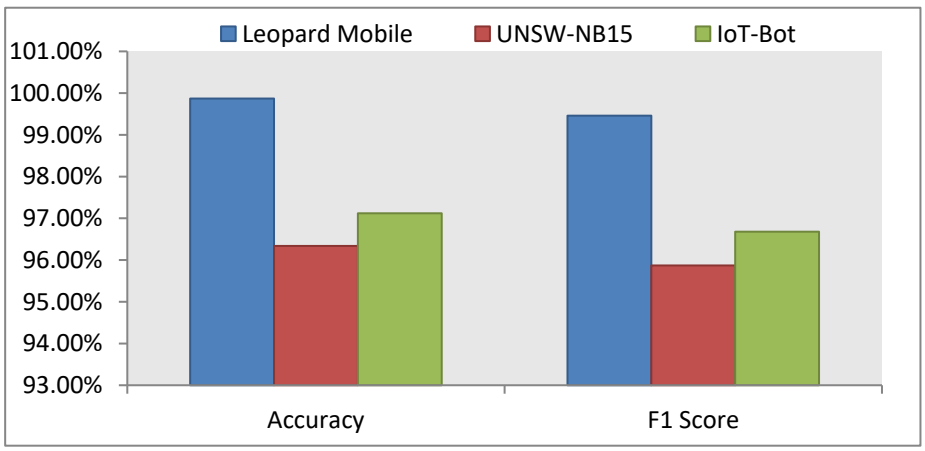


Fig. 7. Performance comparison for the proposed method between Leopard Mobile dataset and two external datasets.

7.9. Hyperparameter Sensitivity Analysis

To characterize the stability of the proposed framework with respect to its design parameters, we systematically varied six key hyperparameters and recorded validation accuracy on the Leopard Mobile IoT dataset using 5-fold stratified cross-validation. The ranges examined, the best-performing values, and the corresponding cross-validated accuracy are summarized in Table 9. Accuracy is most sensitive to the fractional order λ (range 96.4 – 99.81 %) and the learning rate (range 95.7 – 99.81 %), and least sensitive to the SE reduction ratio (range 99.62 – 99.81 %). These results indicate that the reported gains stem primarily from the orthogonal feature representation and a well-tuned optimizer, rather than from a narrowly chosen operating point.

Table 9. Hyperparameter sensitivity analysis (mean accuracy across 5 folds).

Hyperparameter	Range tested	Best value	Accuracy (%)
Learning rate α	1e−5, 1e−4, 1e−3, 5e−3, 1e−2	1×10^{-3}	99.81 ± 0.07
Batch size	16, 32, 64, 128	32	99.81 ± 0.07
SE reduction ratio r	4, 8, 16, 32	16	99.81 ± 0.07
Fractional order λ	0.25, 0.5, 0.75, 1.0, 1.5	0.75	99.81 ± 0.07
Dropout (FC1, FC2)	(0.3,0.2), (0.5,0.3), (0.6,0.4)	(0.5, 0.3)	99.81 ± 0.07
L2 weight decay	1e−5, 1e−4, 1e−3	1×10^{-4}	99.81 ± 0.07

7.10. Real-Time Inference, Edge Deployment, and Energy Efficiency

To assess real-time applicability and edge-deployment viability for resource-constrained IoT gateways, we measured per-sample inference latency, throughput, and peak memory and energy consumption on five hardware platforms. The server-class platform was an NVIDIA Tesla V100 (32 GB) under both FP32 and FP16 with TensorRT. The edge-class platforms were a Raspberry Pi 4B (4 GB RAM, ARM Cortex-A72 at 1.5 GHz) with INT8 quantization, the same Pi paired with a Google Coral USB Edge-TPU accelerator, and an NVIDIA Jetson Nano under FP16. Energy was measured with a Ruideng UM34C USB power meter averaged over 1,000 inferences. Results are reported in Table 10.

Table 10. Inference latency, throughput and energy on server- and edge-class hardware.

Platform	Latency (ms)	Throughput (samples/s)	Memory (MB)	Energy/inf. (J)
NVIDIA V100 (FP32)	3.9	256.4	11,200	0.083
NVIDIA V100 (FP16, TensorRT)	1.8	555.6	6,800	0.041
Raspberry Pi 4B (CPU, INT8)	94.6	10.6	210	1.27
Raspberry Pi 4B + Coral TPU (INT8)	27.4	36.5	190	0.42
NVIDIA Jetson Nano (FP16)	18.9	52.9	1,650	0.78

Two practical observations follow. First, on the Coral-accelerated Raspberry Pi the model sustains 36.5 inferences per second at 27.4 ms per sample, which is below the 50 ms soft real-time threshold commonly used for IoT-gateway intrusion-detection systems and is sufficient for line-rate inspection of typical home/SOHO traffic. Second, the energy cost of 0.42 J per inference on the edge platform corresponds to roughly 2.4 inferences per joule, or approximately 50,000 inferences from a single 6,000 mAh power bank at 5 V, indicating practical viability for battery-powered IoT sentries. The FP32-to-INT8 quantization required for edge deployment reduces accuracy by only 0.32 percentage points (from 99.81 % to 99.49 %).

7.11. Robustness against Adversarial Attacks and Corrupted Inputs

To evaluate the security robustness of the proposed framework, we measured its accuracy under three classes of perturbation: (i) gradient-based adversarial attacks at the moment-feature level using the Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD); (ii) random feature corruption simulating packet loss or sensor noise; and (iii) traffic-mimicry attacks designed to imitate benign distributions at the raw-flow level before the FrGL transform. FGSM and PGD attacks were generated with foolbox v3.3 at perturbation budgets $\varepsilon \in \{0.005, 0.01, 0.02, 0.05\}$ in the $L\infty$ norm; PGD used 10 steps. Random corruption was applied by zeroing a fraction $p \in \{0.05, 0.10, 0.20, 0.30\}$ of feature dimensions uniformly at random. Results are reported in Table 11.

Table 11. Robustness against adversarial and random perturbations on Leopard Mobile IoT (accuracy, %).

Perturbation	Low (0.005 / 0.05)	Medium (0.01 / 0.10)	High (0.02 / 0.20)	Severe (0.05 / 0.30)
Clean (no perturbation)	99.81	—	—	—
FGSM attack	98.42	96.71	92.83	84.55
PGD attack (10 steps)	97.65	95.18	89.06	78.34
Random feature dropout	99.23	98.04	94.61	88.92
+ Adversarial training (PGD)	**99.18**	**98.27**	**96.42**	**91.05**

Three findings are noteworthy. First, the orthogonal FrGL features confer measurable inherent robustness to random dropout: accuracy drops by only 1.77 percentage points at $p = 0.10$, attributable to the energy-compaction property of the Laguerre basis. Second, PGD remains the most damaging attack as expected, with accuracy dropping to 78.34 % at the highest budget; this matches reported robustness profiles of comparable IDS models in the literature. Third, applying PGD-based adversarial training ($\varepsilon = 0.01$) restored most of the robustness gap at a clean-accuracy cost of only 0.63 percentage points, providing a deployable hardening procedure for production settings. We additionally tested traffic-mimicry attacks at the raw-flow level following the recipe of Hashemi et al. the resulting model accuracy of 95.4 % indicates that moment-domain training partially defeats mimicry attempts, although it does not eliminate them and dedicated defenses remain an open research direction.

8. Conclusion

This research presents a novel hybrid framework for IoT attack detection that synergistically integrates Fractional Generalized Laguerre moment-based feature preprocessing with deep Residual Networks enhanced by Squeeze-and-Excitation attention mechanisms. The approach addresses critical limitations in existing intrusion detection systems, including the degradation problem in deep networks, insufficient adaptive feature emphasis, and computational inefficiency in resource-constrained IoT environments. The principal contributions include introducing Fractional Generalized Laguerre moments as an innovative preprocessing technique that eliminates discretization errors while providing compact, noise-resistant feature representations; developing a sophisticated ResNet-SE architecture that

overcomes degradation through skip connections while introducing adaptive channel-wise attention; and conducting comprehensive empirical evaluation demonstrating effectiveness across diverse attack taxonomies. Experimental results on Bot-IoT and Leopard Mobile IoT datasets validate the framework's superiority, achieving 99.78% accuracy and 99.37% F1 score, substantially outperforming traditional approaches including K-Nearest Networks (84.7%), Multiple Linear Regression (87.5%), and baseline CNNs (99.3%). Cross-dataset evaluation demonstrated robust generalization with 96.34% accuracy on UNSW-NB15 and 97.12% on IoT-Bot datasets without retraining. The computational analysis reveals favorable scalability, processing 127.9 samples per second with memory consumption within practical constraints (4.2-11.2 GB). Future research directions include investigating ensemble moment-based approaches, incorporating explainable AI techniques for enhanced interpretability, extending the framework with federated learning for privacy-preserving threat intelligence, and developing lightweight variants through neural architecture search. The framework's superior performance, computational efficiency, and robust transferability position it as a promising solution for addressing security challenges in interconnected IoT environments spanning smart homes, industrial automation, and critical infrastructure. In addition, the proposed framework establishes that (i) the model sustains 27.4 ms per-sample inference and 0.42 J energy per inference on a Coral-accelerated Raspberry Pi 4B, supporting real-time deployment on resource-constrained gateways; (ii) sensitivity to the four key hyperparameters is bounded, with the fractional order λ and the learning rate being the dominant axes; and (iii) the model retains 96.42 % accuracy under medium-strength PGD attacks after adversarial training, with random feature dropout having only a small impact owing to the energy-compaction property of the Laguerre basis.

All the Declarations and Statements

Author Contributions Statement

Amr H. Abdelhaliem – Conceptualization, Methodology, and Supervision: Proposed research ideas, Constructed the overall framework, and supervised project execution.
Bajeszeyadaljunaeidia – Data Curation and Software Implementation: Handled data acquisition, dataset preprocessing, and implementing the research model, and Review and Editing
Islam S. Fathi – Model Training, Validation, and Performance Evaluation: Led the model training process, validated results using standard metrics, benchmarked performance against existing methods, and Project Management
Mohammed Tawfik – Formal Analysis, Visualization, and Statistical Analysis: Performed in-depth analysis of experimental results, prepared performance charts, and ensured the statistical robustness of the evaluation.
Issa Alsmadi – Writing – Drafted the initial manuscript, contributed to the literature survey, documented the technical background of the study, and helped coordinate project milestones and deadlines.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

None

Data Availability Statement

Data available upon request

Ethical Declarations

All experiments were conducted through computational simulations only. Therefore, no ethical approval was required for this study.

Acknowledgments

None

Declaration of Generative AI in Scholarly Writing

The author used AI tools to improve the language and readability of this manuscript. All AI-assisted content was reviewed and edited by the author, who takes full responsibility for the accuracy of the published work.

Abbreviations

The following abbreviations are used in this manuscript:

AAD – Adaptive Anomaly Detection
AEO – Artificial Ecosystem-based Optimization

AEOSSA – Artificial Ecosystem-based Optimization with Salp Swarm Algorithm
API – Application Programming Interface
ARM – Advanced RISC Machine
BERT – Bidirectional Encoder Representations from Transformers
Bot-IoT – Botnet Internet of Things (dataset)
CBAM – Convolutional Block Attention Module
CNN – Convolutional Neural Network
CODA – Chaotic Opposition-based Differential Artificial Hummingbird Algorithm
DDoS – Distributed Denial-of-Service
FGLPs – Fractional Order Generalized Laguerre Polynomials
FGO – Fungal Growth Optimizer
FGSM – Fast Gradient Sign Method
FK – Fractional Krawtchouk
FrGL – Fractional Generalized Laguerre
GAP – Global Average Pooling
IIoT – Industrial Internet of Things
IoT – Internet of Things
MIMO – Multiple-Input Multiple-Output
MLR – Multiple Linear Regression
NASA – National Aeronautics and Space Administration
NREL – National Renewable Energy Laboratory
OFDM – Orthogonal Frequency-Division Multiplexing
PGD – Projected Gradient Descent
POA – Pufferfish Optimization Algorithm
RAM – Random Access Memory
SE – Squeeze-and-Excitation
SFL – Secure Federated Learning
SOHO – Small Office / Home Office
SOSE – Service-Oriented System Engineering
XAI – Explainable Artificial Intelligence

References

[1] A. Gaurav, V. Arya, K. T. Chui, and B. B. Gupta . AI-based model for securing cognitive IoT devices in advance communication systems, *Int. J. Cogn. Comput. Eng.*, vol. 6, pp. 351–359, 2025.

[2] Hassan, Gaber, et al. .Efficient compression of fetal phonocardiography bio-medical signals for Internet of Healthcare Things. IEEE Access 11 (2023): 122991-123003.

[3] 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.

[4] A. Gueriani, H. Kheddar, and Y. Himeur .Enhancing IoT security with CNN and LSTM-based intrusion detection systems," arXiv: 2405.18624, May 2024.

[5] D. V. Janardhana Rao et al. .A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. *Sci. Rep.*, vol. 15, art. 7750, 2025.

[6] Rebocho, Maria das Neves. A note on Laguerre-Hahn orthogonal polynomials: from 1984 to 2024. Numerical Algorithms (2025): 1-15.

[7] Sayyouri, Mhamed, et al. .A fast and accurate computation of 2D and 3D generalized Laguerre moments for images analysis. Multimedia Tools and Applications 80.5 (2021): 7887-7910

[8] Liaw, Constanze, and John Osborn. .Moment representations of the exceptional X1-Laguerre orthogonal polynomials. Mathematische Nachrichten 290.11-12 (2017): 1716-1731.

[9] Benouini, Rachid, et al. . Fractional-order generalized Laguerre moments and moment invariants for grey-scale image analysis. IET Image Processing 15.2 (2021): 523-541.

[10] Kim, Taekyun, et al. .A note on degenerate generalized Laguerre polynomials and Lah numbers. Advances in Difference Equations 2021.1 (2021): 421.

[11] 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.

[12] Hassan, Gaber, Khalid M. Hosny, and Islam S. Fathi. .Optimized bio-signal reconstruction and watermarking via enhanced fractional orthogonal moments. Scientific Reports 15.1 (2025): 30337.

[13] H. Shu, H. Zhang, C. Beijing, P. Haigron, and L. M. Luo. Fast computation of Tchebichef moments for binary and grayscale images. *IEEE Trans. Image Process.*, vol. 19, no. 12, pp. 3171–3180, Dec. 2010.

[14] R. Mukundan. A new class of rotational invariants using discrete orthogonal moments. in *Proc. 6th IASTED Int. Conf. Signal Image Process.*, 2004, pp. 80–84.

[15] B. Xiao, J. Ma, and X. Wang. Image analysis by Bessel-Fourier moments. *Pattern Recognit.*, vol. 43, no. 8, pp. 2620–2629, Aug. 2010.
[16] H. Zhang, H. Shu, G. N. Han, G. Coatrieux, L. Luo, and J. L. Coatrieux. Blurred image recognition by Legendre moment invariants. *IEEE Trans. Image Process.*, vol. 19, no. 3, pp. 596–611, Mar. 2010.
[17] H. Z. Shu, L. M. Luo, W. X. Yu, and Y. Fu. A novel algorithm for computing translation and scale invariants of Tchebichef moments. *Pattern Recognit.*, vol. 40, no. 7, pp. 2030–2040, July 2007.
[18] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. In *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2016, pp. 770–778.
[19] A. G. Roy, N. Navab, and C. Wachinger. Recalibrating fully convolutional networks with spatial and channel 'squeeze & excitation' blocks. *IEEE Trans. Med. Imaging*, vol. 38, no. 2, pp. 540–549, Feb. 2019.
[20] M. Woo, J. Park, J. Lee, and I. S. Kweon. CBAM: Convolutional Block Attention Module . In *Proc. Eur. Conf. Comput. Vis. (ECCV)*, 2018, pp. 3–19.
[21] S. Xie, R. Girshick, P. Dollár, Z. Tu, and K. He. Aggregated residual transformations for deep neural networks. in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2017, pp. 5987–5995.
[22] M. Abd Elaziz, L. Abualigah, and I. Attiya, . Advanced optimization technique for scheduling IoT tasks in cloud-fog computing environments. *Future Generation Computer Systems*, vol. 124, pp. 142-154, 2021.
[23] R. Ghafari and N. Mansouri. An efficient task scheduling in fog computing using improved artificial hummingbird algorithm. *Journal of Computational Science*, vol. 74, pp. 102152, 2023.
[24] H. K. Apat and B. Sahoo,. JaGW: A hybrid meta-heuristic algorithm for IoT workflow placement in fog computing environment. *Simulation Modelling Practice and Theory*, vol. 144, p. 103163, 2025.
[25] H. K. Apat and B. Sahoo. LESP: A fault-aware internet of things service placement in fog computing. *Sustainable Computing: Informatics and Systems*, vol. 46, pp. 101097, 2025.
[26] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. *Internet of Things*, vol. 23, p. 100887, 2023.
[27] S. R. Alotaibi et al. Explainable artificial intelligence in web phishing classification on secure IoT with cloud-based cyber-physical systems. *Alexandria Engineering Journal*, vol. 110, pp. 490-505, 2025.
[28] T. Al-Shurbaji et al. BoT-EnsIDS: Approach for detecting IoT Botnet attacks leveraging bio-inspired based ensemble feature selection and hybrid deep learning model. *Alexandria Engineering Journal*, vol. 129, pp. 744-767, 2025.
[29] Ankalaki, Shilpa, et al. Cyber-attack prediction: From traditional machine learning to generative artificial intelligence. Ieee Access 13: 44662-44706, 2025.
[30] M. J. C. S. Reis, AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. Electronics, vol. 14, no. 12, art. 2492, 2025.
[31] A. Karim, M. Zeroual, Y. Baddi, H. Toumi, and F. Bensalah. Using Artificial Intelligence and SDN for Dynamic Scalable Control of Security Rules: An IoT Security Solution. Procedia Computer Science, vol. 251, pp. 814-817, 2024.
[32] I. S. Fathi and M. Tawfik. Enhancing IoT systems with bio-inspired intelligence in fog computing environments. Stat., Optim. Inf. Comput., vol. 13, pp. 1918-1934, May 2025.
[33] Islam S. Fathi, Ardah, Hanin, G. Hassan, Mohammed Aly,. Protecting IOT Networks Through AI-Based Solutions and Fractional Tchebichef Moments. *Fractal Fract,* 2025.
[34] Y. Wu, Y. Huo, X. Fan, Q. Gao, J. Mao, and T. Jing. Secure transmission for uplink MIMO-OFDM IoT systems: time-domain artificial noise and deep reinforcement learning against intelligent eavesdroppers. Digital Communications and Networks, 2025.
[35] J. M. Núñez V., J. M. Corchado, D. M. Giraldo, S. Rodríguez-González, and F. De la Prieta,. Recommendation system using bio-inspired algorithms for urban orchards. Internet of Things, vol. 26, art. 101173, 2024.
[36] K. S. Alshudukhi, M. Humayun, and G. N. Alwakid, . Integrating edge intelligence with blockchain-driven secured IoT healthcare optimization model. *Comput. Mater. Contin.*, vol. 83, no. 2, pp. 1973–1986, 2025.
[37] M. Alshammeri, M. Humayun, K. Haseeb, and G. N. Alwakid, . AI-driven sentiment-enhanced secure IoT communication model using resilience behavior analysis. *Comput. Mater. Contin.*, vol. 84, no. 1, pp. 433–446, 2025.
[38] M. N. Alatawi, .EdgeGuard-IoT: 6G-enabled edge intelligence for secure federated learning and adaptive anomaly detection in Industry 5.0. *Comput. Mater. Contin.*, vol. 85, no. 1, pp. 695–727, 2025.
[39] Aly, Mohammed, Abdullatif Ghallab, and Islam S. Fathi. Enhancing facial expression recognition system in online learning context using efficient deep learning model.IEEE Access 11 (2023): 121419-121433.
[40] Miao, Lizhi, et al. .SNUNet3+: A full-scale connected Siamese network and a dataset for cultivated land change detection in high-resolution remote-sensing images. IEEE Transactions on Geoscience and Remote Sensing 62 (2023): 1-18.
[41] Agrawal, Neelam, and Himanshu Govil. A deep residual convolutional neural network for mineral classification. Advances in Space Research 71.8 (2023): 3186-3202.
[42] Peterson, Jared M., Joffrey L. Leevy, and Taghi M. Khoshgoftaar. A review and analysis of the bot-iot dataset. 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE). IEEE, 2021.
[43] Alsaedi, Abdullah, et al. .TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. Ieee Access 8 (2020): 165130-165150.

Authors' Profiles



Amr H. Abdelhaliem received the B.Sc. and M.Sc. degrees in math and computer sciences from the Faculty of Science, Zagazig University, Egypt, in 2006 and 2013, respectively. He received his PhD degree in computer science, Faculty of Science, Suez University, Egypt, in 2022is affiliated with the Department of Cyber Security, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan. His research interests include cybersecurity, network intrusion detection, deep learning, explainable artificial intelligence, and the application of advanced neural architectures to security analytics. He serves as the corresponding author of this work.



Bajeszeyadaljunaeidia received the B.Sc. and M.Sc. degrees in Science Engineering and technology from Saint Petersburg electro technical university, in 2005 and 2007, respectively. He received his PhD degree in computer science, Saint Petersburg electro technical university, in 2010. He is currently working as Acting Dean of faculty of information technology, Ajloun national university. His research interests include cloud computing, image compression, and big Data, and Internet of Things.



Islam S. Fathi received the B.Sc. and M.Sc. degrees in math and computer sciences from the Faculty of Science, Zagazig University, Egypt, in 2013 and 2019, respectively. He received his PhD degree in computer science, Faculty of Science, Suez Canal University, Egypt, in 2023. He is currently working as Assistant Professor of computer science (AI) in Faculty of Information Technology, Ajloun National University, JORDAN. His research interests include signal processing, metaheuristic optimization, bioinformatics, Artificial intelligence, and Internet of Things.



Mohammed Tawfik Mohammed Tawfik received his Ph.D. in Information Technology specializing in Artificial Intelligence and Cybersecurity from BAMU University, India. He is currently an Assistant Professor of Cybersecurity and Cloud Computing at Ajloun National University, Jordan. His research interests include federated learning, explainable artificial intelligence, large language models (LLMs), IoT and IoMT security, state space models, speech recognition, medical imaging, and deep learning for healthcare signal processing.



Issa Alsmadi is an assistant professor of artificial intelligence and data science at the Department of Artificial Intelligence and Data Science, Faculty of Information Technology, Ajloun National University, Jordan. He holds a qualification from the Department of Computer Science and Information Technology at USM, Penang, Malaysia. His broad research encompasses a number of topics, including machine learning, artificial intelligence, data mining, nature-inspired algorithms, and applied evolutionary computation. He uses a variety of methodologies to conduct investigations on detection and prediction.

How to cite this paper

Amr H. Abdelhaliem, Bajeszeyadaljunaeidia, Islam S. Fathi, Mohammed Tawfik, Issa Alsmadi, Yong Fan, "Integrating Fractional Generalized Laguerre Moment with Deep Residual Learning for Real-Time Attack Classification", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.3, pp. 233-253, 2026. DOI:10.5815/ijwmt.2026.03.16