A Hybrid AEERAM–ResA-D^{2}PySepCo Framework for Adaptive Energy-Efficient Resource Allocation Management and Intelligent Cyber-Attack Detection in IoT-Enabled Fog Computing Environments

Mr. KOTARI SURESH[1], Prof. Dr. M HUMERA KHANAM[2]

[1]Research Scholar, Computer science and Engineering, SVU University-Tirupathi.
[2]Professor, Computer science and Engineering, SVU University-Tirupathi.

Abstract:
The rapid growth of Internet of Things (IoT) systems has been enormously stressing the issues of cybersecurity, energy usage, and the optimal usage of resources in distributed computers networks. Fog computing has become a promising intermediate layer between the cloud and IoT layers with the ability to process in real-time and make localized decisions. Nevertheless, the problem of fog nodes is that they are resource-limited in nature and are becoming more vulnerable to sophisticated cyber-attacks that require smart mechanisms to tackle security and energy-efficiency. Research that is currently in place is mostly concentrated on the detection of cyber-attacks or managing energy-aware resources without considering them as a unified problem, which leads to poor scalability to actual implementations in the fog-based IoT infrastructure. In this paper, the author suggests an integrated hybrid system called AEERAM-ResA-D^{2}PySepCo that is a combination of adaptive energy-saving management of resource allocation (AEERAM) and a smart system of detecting cyber-attacks based on Residual Attention-Dilated Pyramidal Depthwise Separable Convolution (ResA-D^{2}PySepCo). The architecture brings two research works that were not interdependent previously into one unified system (C3), where the security and use of energy can be optimized. The given model is assessed with the help of benchmark datasets such as ToN-IoT and CICIDS2018, as well as a multi-tier approach to IoT resource management situation. It is shown that experimental results have a high accuracy, precision, F1-score, false alarm rate and energy efficiency relative to current methods of the state-of-the-art. Results obtained prove that the incorporation of energy-efficient resource allocation management and CYBER-ATTACK DETECTION into one structure promotes significantly not only the ability to detect cyber-attacks but also provides the opportunity to distribute resources efficiently and without waste in the ecosystem where IoT technologies are implemented.

Keywords: Fog computing, Internet of Things, cyber-attack detection, energy-efficient resource allocation, intrusion detection system, optimization algorithms.

1. INTRODUCTION

Internet of Things (IoT) has emerged as one of the most revolutionary technological paradigms of the last ten years and has allowed to provide ubiquitous connectivity to the billions of heterogeneous devices in the fields of healthcare, smart cities, industrial automation, transportation, and energy systems [1]. Through the incorporation of senses, calculating and communicating features in ordinary physical items, IoT also supports the process of collecting data in real-time and making intelligent decisions. Nevertheless, the increase of IoT devices by a significant margin has come with significant trends in the aspect of scaling, latency, security and energy usage. Conventional cloud-based systems are becoming less and less capable of supporting the high latency and throughput demands of IoT applications, especially those with time-sensitive operations and data volumes seen in IoT application [2].

Fog computing has also become a promising development as an improvement of cloud computing where computation, storage and control services are placed towards the network edges and closer to the data sources [3]. By allowing local processing of the data on the nodes in the fog, this paradigm helps in controlling the latency and bandwidth usage, and provides even more context-awareness. In spite of these strengths, the nature of fog computing is limited in computational power, memory and energy resources. More so, the environment of fog nodes is very distributed and unsecured which is a favourable target to cyber-attack like Distributed Denial of Service (DDoS), botnet, ransomware, brute force and data loss [4,5]. Mog-based IoT systems have thus turned into a significant issue of cybersecurity. The conventional security measures based on rule-based intrusion detection systems and signature based firewalls are not adequate to identify advanced and emerging attack patterns. The latest developments in machine learning (ML) and deep learning (DL) have shown promising outcomes concerning detecting anomalous behavior of a network, and malicious actions with the IoT infrastructure and fog computing [6-8]. However, current DL-based intrusion detection systems are characterized by a high level of false alarms, lack of generalization, and high computational weight that limits their usefulness in fogs with limited resources.

With this, energy efficiency has become a central design end based on the use of fog-based IoT. Fog nodes have to deal with constrained power gains and address the dynamic workloads and heterogeneous needs of services. Ineffective resource allocation policies may result to huge consumption of energy, shortened nearest system life, and worsened quality of service (QoS) [9]. Several resource management schemes that are energy conscious have been suggested based on the use of optimization algorithms and heuristic methods as a way of reducing power consumption and workload balance [10,11]. Nevertheless, such solutions tend to disregard the effect of the cybersecurity systems on the energy consumption, leading to the provision of the fragmented solutions which cannot resolve the interdependence of the security and resource management.

One of the main gaps in the current research is the absence of combined frameworks that can be used to coordinate cyber-attack detection and energy-efficient resource allocation in fog-based IoTs. Mechanisms used to provide security increase both the cost of computation and the overall energy consumption, whereas the allocation of resources has a direct impact on the responsiveness and the performance of intrusion detection systems. Independent treatment of these problems results in poor trade-offs and poor system performance.

This study fills this gap by suggesting a hybrid framework model that combines resource allocation management to allocate individual resources to provide adaptive energy saving and intelligent detection of cyber-attack. The combination of these two points into one architecture by the planned approach will result in strong security, lowering the false alarm rate, and increasing the efficiency of using energy at the same time.

1.1 Motivation

This research has been motivated by some key constraints realized in the current solutions of fog-based security and resource management solutions to IoT. First, the majority of cyber attack detection models are developed with the main purpose to increase their accuracy without paying much attention to their energy consumption or realistic implementation on fog nodes. Recognition models like CNNs, LSTMs, and hybrid neural networks, typically demand a lot of physical memory and computing power to further reduce computational resource costs and thus power consumption and delay when run in real-time in fogged memories [12,13]. This renders them inappropriate in scale in large-scale IoT implementations.

Second, without security awareness, the resource allocation schemes of energy-efficient workload balancing, task offloading, and power optimization are generally the concern. These strategies are premised on the assumption of a benign operational environment, and they fail to change the approach to resources allocation, as determined by observed threats or abnormal behavior [14]. Consequently, the allocation of resources in the case of cyber-attacks can be inefficient by the node of the fog, which further worsens the performance deterioration and predisposes to vulnerability.

Third, many of the studies have often tested their models on small sets of data and in controlled environments, lacks real-world conditions of the fog-based IoT systems. Lack of multi-dataset validation, multi-class based attack detection, and realistic workload conditions is a constraint to the generalizability and validity of the reported results [15].

These observations indicate the necessity of an integrated, adaptive and energy conscious security domain that will be able to work successfully in the fog-enabled IoT infrastructures. This framework must not just identify the cyber-attacks with high precision, and low false alarm rate but intelligent allocation of resources to minimize energy use and stability of the system in different operational conditions.

1.2 Research Contributions

The paper is based on two other research contributions and consolidates them into one comprehensive contribution thereby giving a third contribution. The greatest contributions of such works can be summarized as follows:

- **C1: Energy-Efficient Resource Allocation Management :** Design of an adaptive and resource efficient resource allocation management (AEERAM) control of the multi-tier IoT-enabled fog computing environment. It is a dynamic mechanism that allocates computational and communication resources according to the nature of the workload, energy state of node and the QoS requirements, which optimise the total energy they consume against service performance.
- **C2: Cyber-Attack Detection:** Intelligent Cyber-Attack Detection Model Design: Residual Attention-Dilated Pyramidal Depthwise Separable Convolution ResA-D^{2}PySepCo. This deep learning system is able to improve the feature representation, less computational costs, and high detection accuracy and low false alarm levels of various categories of attacks.
- **C3: integration of** Energy-Efficient Resource Allocation Management and Cyber-Attack Detection merge into a hybrid architecture (AEERAM-ResA-D^{2}PySepCo) that both optimally distributes the resources in an energy-efficient manner and cyber-attack intrusions in the IoT-based fog computing infrastructure. The co-ordinated framework allows adaptive coordination amidst security measures and resource control which leads to better overall system functionality.

The given framework is broadly tested on the basis of real-life benchmark datasets, ToN-IoT and CICIDS2018, and a multi-layer IoT resource management scenario as well. The results of the evaluation of performance in terms of accuracy, precision, recall, F1-score, false alarm rate, and energy efficiency indicate that the results are substantially better than the current state-of-the-art solutions.

2. RELATED WORK

Fog computing has received a lot of research attention as an alternative paradigm to cloud computing to supporting latency-sensitive and bandwidth-intensive Internet of Things applications. The architectural principles of the construction of the fog computing were developed in the early works that prioritized a decentralized computation and local data processing as the necessary measures to decrease the usefulness of the cloud, as well as network congestion [16]. This theory was later extended by other studies which extended it into multi-tier fog architectures that assist in hierarchical decisions and resource sharing across fog nodes [17]. Although these works have effectively shown the reduction of latency and enhanced scalability they have not given much consideration to the implication of energy constraints and security vulnerability of fog environment.

Mog computing has in the previous years received a significant amount of interest on energy-efficient resource allocation. A number of papers offered heuristic and optimization-based scheme of scheduling the tasks to ensure the minimum energy usage and fulfill the requirements of quality of service [18,19]. Genetic algorithm, particle swarm optimization and ant colony optimization are some of the metaheuristic techniques that have been used in the optimization of task placement and workload distribution among the fog nodes [20]. Whereas such methods have realized a quantifiable saving of energy, they may have relied on a stable and inoffensive environment without considering the effects of cyber-attacks in resources availability and planning. Furthermore, most energy-conscious models used simple assumptions about

energy consumption that are not applicable to reality, where the effect of a certain type of dynamic loads can be observed on the behavior of the node of the fog.

Along with the energy optimization direction, the detection of cyber-attack in IoT and fog methods has developed at a high pace with the introduction of machine learning and deep learning methods. Conventional intrusion detection methods that relied on rule matching and statistical points were discovered to fail in the detection of sophisticated and multi-phase attacks against the IoT infrastructures [21]. Deep learning models such as convolutional neural networks, recurrent neural networks and hybrid CNN-LSTM models have been found to outperform other detection models; the models learn hierarchical feature representations using network traffic data [22,23]. Nonetheless, these models are usually computationally expensive which means that they consume more energy and face inference latency when used in fog settings.

Table 1- Recent Literature Review on Cyber-Attack Detection and Resource Management in IoT–Fog Environments

Author(s), Year	**Paper Title**	**Methods Used**	**Limitations Identified**
Moustafa et al., 2019	*An Ensemble Intrusion Detection Technique for IoT Networks*	Ensemble ML with statistical flow features (UNSW-NB15, BoT-IoT)	Focused only on detection accuracy; energy efficiency and fog resource constraints were not considered
Ferrag et al., 2020	*Deep Learning-Based Intrusion Detection for IoT*	CNN and RNN-based IDS models	High computational overhead; unsuitable for energy-constrained fog nodes
Nguyen et al., 2020	*Deep Reinforcement Learning for IoT Security*	DRL-based adaptive IDS	Long training time and instability under dynamic traffic conditions
Ullah & Mahmoud, 2021	*A Deep Learning Framework for Network Intrusion Detection*	CNN–LSTM hybrid model	Binary classification focused; multi-class attack handling limited
Qureshi et al., 2021	*Energy-Efficient Task Scheduling in Fog Computing*	Heuristic energy-aware scheduling	Security aspects and malicious workload impact were ignored
HaddadPajouh et al., 2021	*Intrusion Detection in IoT Using Deep Autoencoders*	Stacked autoencoders with feature reduction	Poor performance under complex multi-vector attacks
Aloqaily et al., 2022	*Secure and Energy-Aware Resource Allocation in Fog Computing*	Optimization-based secure resource management	Detection accuracy was not evaluated using real intrusion datasets
Almutairi et al., 2022	*Attention-Based Deep Learning IDS for IoT*	Attention-enhanced CNN	Computationally expensive for real-time fog deployment
Rana et al., 2022	*Fog-Based IDS Using Hybrid Deep Learning*	CNN–GRU architecture	Energy consumption and scheduling efficiency not analysed
Hussain et al., 2023	*Lightweight IDS for IoT-Fog Networks*	Pruned deep neural networks	Reduced complexity at the cost of detection accuracy
Zhang et al., 2023	*Multi-Tier Resource Management in IoT–Fog Systems*	Multi-objective optimization	Lacked integrated security awareness
Aljuhani et al.,	*Secure Task*	Game-theoretic	Assumed trusted traffic; no

Author(s), Year	Paper Title	Methods Used	Limitations Identified
2023	*Offloading in Fog Computing*	offloading model	intrusion detection mechanism
Khan et al., 2024	*Explainable AI-Based Intrusion Detection for IoT*	XAI-enabled deep learning IDS	High inference latency and energy overhead
Rahman et al., 2024	*Joint Energy and Security Optimization in Edge Computing*	Joint optimization framework	Limited evaluation datasets; lacked deep IDS integration

An incisive examination of current literature indicates that there have been three research gaps. To begin with, all of the current intrusion detection methods are more focused on accuracy of detection and ignore the actual resource and energy limitations of fog environments, which makes them inapplicable to processes of constant and real time applications. Second, the energy-efficient methods of resource management operation consider benign workloads to a large extent, without considering massive power wastes when using malicious traffic. Third, despite recent methods of joint optimization, even more advanced techniques typically use shallow or rule-based security implementation, and can hardly help in detection of more complex multi-class cyber-attacks in IoT traffic.

These gaps are a strong motivation to the framework proposed, Hybrid AEERAM-ResA-D^2PySepCo, that has a unique feature to combine deep learning-based intrusion detection and energy-sensitive resource allocation into a single architecture. The proposed framework proposed above (where Energy-Efficient Resource Allocation Management (energy-efficient resource allocation) and Cyber-Attack Detection (intelligent cyber-attack detection) are instigated into single hybrid framework) will conduct the weaknesses of the recent state-of-the-art techniques, and will achieve better accuracy in detection, less false alarm rate, and substantial energy savings in an IoT-enabled setting of fog computing.

Latest developments have tried to solve the dilemma of detection accuracy and computation efficiency by proposing light greed neural network structures. They have added depthwise separable convolutions, dilated convolutions as well as attention mechanisms to minimize the model complexity without losing classification performance [24]. With these developments, majority of the intrusion detection researchers were testing their models without mechanism of managing the resources and viewing security as a separate function and not as a part of the fog system.

There were few studies that examined joint security and resource management optimization. Other security-conscious scheduling models had prioritized security critical work during high risk with throttling of non-essential workloads [25]. Some other people suggested adaptive monitoring schemes to dynamically change the detection frequency according to the levels of node energies [26]. Although these methods respected the fact that security and resource usage were connected to each other, neither of the methods included a coherent mathematical model and combined deep learning-based intrusion detection and energy-conscious resource distribution on an integrative level.

The major constraint in all the works is the lack of a holistic system that can maximize performance of cyber-attack detection and optimize allocation of resources using energy efficient regulations in the situation of realistic mistakes in fog computing. Majority of previously researches are single-objective oriented, use limited data, or do not test their models in the heterogeneous conditions of IoT and fog. This study bridges such gaps by incorporating adaptive energy-efficient resource allocation management with a lightweight model of detecting cyber-attack intelligence into a single system, which will allow the optimization of security and energy efficiency to work in harmony.

3. OVERALL INTEGRATED FRAMEWORK ARCHITECTURE

The hybrid AEERAM-ResA-D^{2}PySepCo framework is aimed at being developed as a multi-level structure closely incorporating the mechanisms of detecting cyber-attack and the use of resources furtively based on the IoT-enabled fog computing networks. The architecture has three major layers namely the IoT layer, the fog layer, and the cloud layer. The different layers have their own specific functionalities, but they are not independent of the others as they facilitate the processes of secure, energy-conscience, as well as low-latency data processing.

The IoT layer consists of heterogeneous devices which include sensors, actuators, smart appliances and embedded systems which produce continuous data streams. These devices are normally resource-constrained and in the ability to perform complex security or optimization algorithms. Consequently, uncoded information at this layer is transmitted to other mole nodes to process it before it is transmitted to the next layer.

The proposed framework has the layer of operation which is the fog layer. Fog nodes have moderate computing and storage capacity that would allow them to implement intrusion detection algorithms, conduct task scheduling, and local resource management. The ResA-D^{2}PySepCo layer has an obligation to scan traffic entering the system and trace bad actions and the AEERAM layer will assign dynamically the computational and communication resources in regard to the availability of energy and the level of workload as well as security state.

The cloud layer offers a centralized support to long term data storage, global analytics as well as offline model training. Numbers of computational-intensive activities like periodic updating of deep learning models, historical analytics in large scales, and so on can be offloaded to the cloud in order to relieve the fog nodes. New model parameters and optimization policies are also distributed to fog nodes by the cloud whenever required.

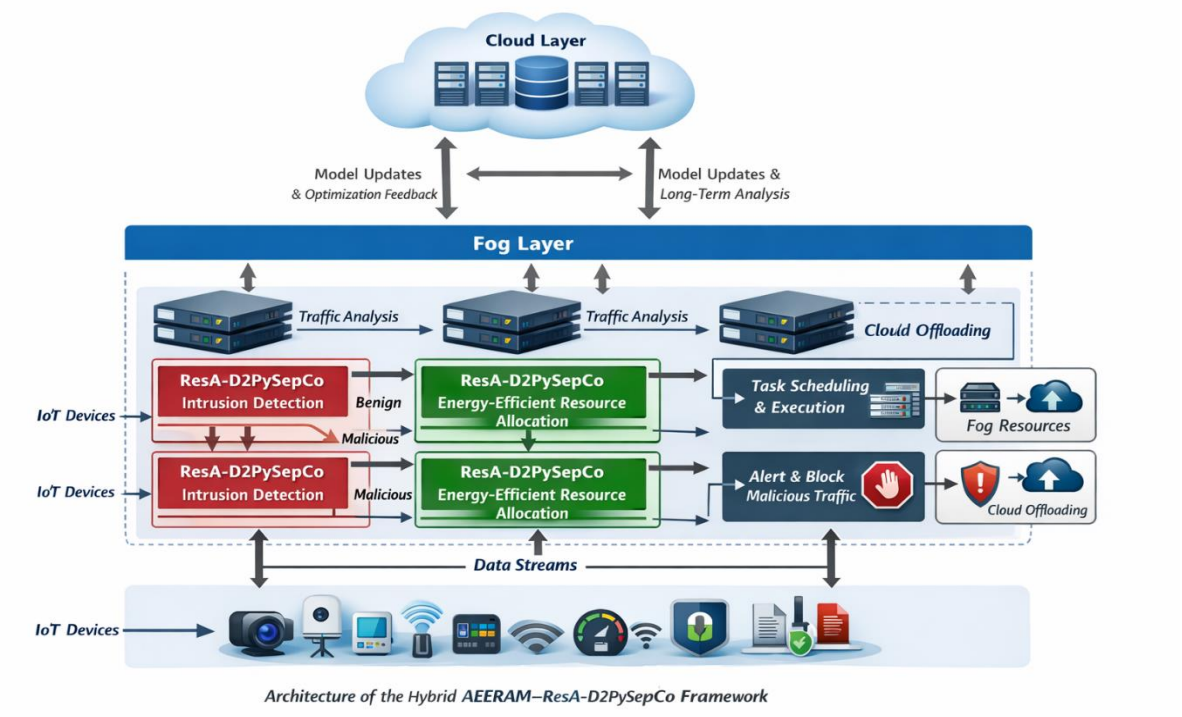

Figure 1: Architecture of the Hybrid AEERAM–ResA-D^{2}PySepCo Framework

3.1 System Model

The system model assumes a collection of IoT devices $(D = d_1, d_2, \ldots, d_n)$ that produces tasks which have to be done at fog nodes or the cloud. An array of fog nodes $(F = f_1, f_2, \ldots, f_m)$ gives access to inexpensive and relatively small energy budgets of isolated, but heterogeneous processing capabilities.

The computational demand and data size, as well as latency requirement and sensitivity of security of every task (t_i) are specified. Processing decision on the given task consists of the combination of classification output of the module used to detect intrusion and the state of the hardware under the management of the fog infrastructure.

The total energy use of a fog node (f_j) can be described as the sum of the components of energy used in computation, communication and idle:

$$E_{f_j} = E_{f_j}^{comp} + E_{f_j}^{comm} + E_{f_j}^{idle}$$

where $\left(E_{f_j}^{comp}\right)$ represents energy consumed during task execution, $\left(E_{f_j}^{comm}\right)$ denotes energy spent on data transmission, and $\left(E_{f_j}^{idle}\right)$ accounts for baseline power consumption when the node is active but underutilized.

Latency experienced by a task (t_i) is modeled as:

$$L_{t_i} = L_{t_i}^{queue} + L_{t_i}^{proc} + L_{t_i}^{trans}$$

where queuing delay, processing delay, and transmission delay collectively determine the end-to-end response time.

3.2 Integrated Framework Workflow

The functional flow of the suggested architecture starts at the layer of data acquisition at the IoT layer at which annoying traffic is produced and conveyed to fog nodes. After reaching the layer of the fog, incoming traffic is first subjected to the feature extraction and preprocessing process and then it is processed by the ResA-D^{2}PySepCo intrusion detection module. The module uses a classification process with deep learning to decide between normal and cyber-attack behavior of the traffic.

The AEERAM module, depending on the outcome of detection, changes the strategy of the resource allocation dynamically. In the case of the presence of malicious behavior, the corresponding traffic is isolated, the execution of the tasks is precluded and the resources are reallocated to ensure that the system remains stable. In the case of benign traffic, the AEERAM calculates energy more efficient scheduling policies based on the current distribution of workload, energy capacity of the node, and latency. Assignments are then left to suitable offloaded on the cloud when required or directed to the cloud to the appropriate nodes in the form of a Mog.

The framework works on the idea of continuous feedback where the statistics of resource usage and detection results are monitored and applied in order to revise resource scheduling and security policies. This dynamically moving workflow facilitates the appropriate response of the system to varying workload patterns and additional attack situation.

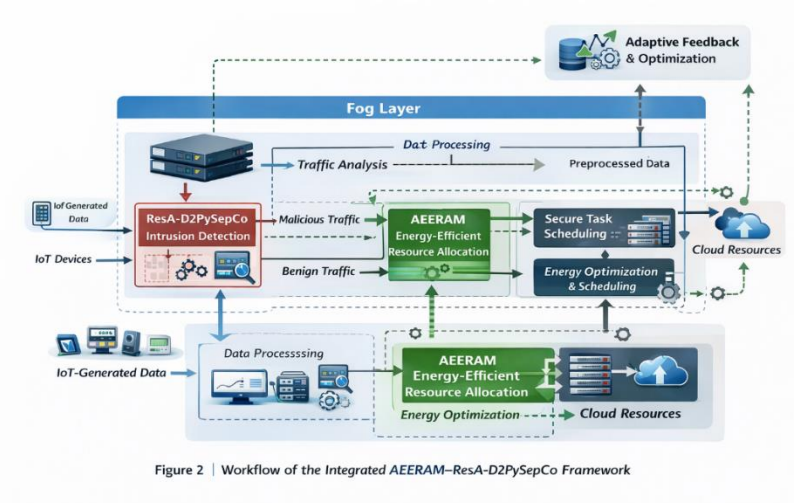

Figure 2: Workflow of the Integrated AEERAM–ResA-D^{2}PySepCo Framework

4. MATHEMATICAL FORMULATION OF THE INTEGRATED FRAMEWORK

This part develops the proposed efficient energy-saving mechanism of the management of resource allocation combined with the detection of cyber-attack in the fog-computing landscape of IoT-enabled computing systems. As opposed to traditional methods that mostly measure how much energy is used, the suggested model is explicit to translate the *task-resource allocation choices, efficiency of the utilization of computational resources, communication overhead, and security conscious scheduling constraints.* This aim is to have an efficient management of the resources of fog so that only the legitimate workloads would be assigned to appropriate fog nodes and the power spent by the power resources should be minimized and the quality-of-service requirements should be satisfied.

4.1 Energy-Efficient Resource Allocation Formulation

Let the set of fog nodes be defined as

$$F = f_1, f_2, \dots, f_m, T = t_1, t_2, \dots, t_n.$$

Resource allocation to present the problem of energy efficient allocation is modeled by incorporating a binary allocation variable that is used to decide how tasks are placed across mog nodes:

$$x_{ij} \in 0,1,; x_{ij} = 1 \; if \; task \; t_i \; is \; allocated \; to \; fog \; node \; f_j.$$

The energy expenditure of a (f_j) fog node can be defined as a total power used in the operation of a fog node depending on the workloads allocated and resource usage:

$$E_{f_j} = \sum_{i=1}^{n} \quad x_{ij} \kappa_j C_{t_i} f_j^2 + \sum_{i=1}^{n} \quad x_{ij} P_{tx} \frac{D_{t_i}}{R_j} + P_{idle} T_{idle}.$$

In this case, the first term is the *energy of computations*, the second term is the *energy of communications* and the third term is *idle energy*, which is the energy consequence of allocation decisions as opposed to individual consumption.

The *efficiency of the resource usage* of any single node of the m-og network can be defined as the ratio of the required amount of computation demand to the capacity:

$$U_{f_j} = \frac{\sum_{i=1}^{n} \quad x_{ij} C_{t_i}}{C_{f_j}^{max}.}$$

An essential goal of energy-efficient resource allocation management is to maximize the utilization efficiency and prevent overloading since idle energy losses would be incurred by underutilized nodes, and overloaded nodes would reduce the delay incurred and energy wasted.

4.2 Security-Aware Task Admission for Resource Allocation

In order to avoid wasting energy due to malicious workloads, cyber-attack detecting is directly involved into the process of resources allocation. Let

$$x_i \in R^d$$

represent the feature vector of (i)-th roadway traffic. The result is a classification decision of ResA-D2PySepCo used to detect intrusion:

$$\hat{y}i = FIDS(x_i), \quad \hat{y_i} \in 0,1, (\hat{y_i} = 0)$$

indicates benign traffic and $(\hat{y_i} = 1)$ indicates malicious activity.

In effort to assure security-aware allocation variables, only the set of tasks that are benign is admitted to the resource allocation pool:

$$x_{ij} = 0 \quad if \quad \hat{y}_i = 1.$$

This process will mean that the resources of the mist are only used by an actual workload and this aspect will provide a direct effect on the enhanced energy efficiency and system sustainability.

4.3 Integrated Energy-Efficient Resource Allocation Optimization Objective

The suggested framework provides maximum efficiency in the management of the resources allocation by minimizing energy expenditure, latency in a task, and detection error. The built-in objective function is as follows:

$$J = \alpha \sum_{j=1}^{m} E_{f_j} + \beta \sum_{i=1}^{n} L_{t_i} + \gamma(1 - F1).$$

In this case, (α), (β), and (γ) are the weighting factors that control the tradeoff between the energy efficiency, the latency performance, and the effectiveness of cyber-attack detection.

The optimization is bound to the following resource *allocation management limitations*:

Computational capacity constraint:

$$\sum_{i=1}^{n} x_{ij} C_{t_i} \leq C_{f_j}^{max}, \quad \forall f_j.$$

Energy budget constraint:

$$E_{f_j} \leq E_{f_j}^{max}, \quad \forall f_j.$$

Security-aware allocation constraint:

$$x_{ij} \in 0,1; only\ if; \hat{y}_i = 0.$$

Core Contribution of the Model

This model allows energy modeling to be described into an entire resource allocation management model by demonstrating a direct relationship between *task admission, allocation decision, utilization efficiency and security validation.* Instead of reducing power alone, the offered plan considers all the resources of the fog and makes sure that the energy savings are the natural products of smart distribution, equal use, and the prompt eradication of malicious traffic.

5. ALGORITHMIC DESIGN OF THE HYBRID AEERAM–RESA-D²PYSEPCO FRAMEWORK

The proposed framework is designed in an algorithmic fashion with the strong focus on the close interaction of energy-efficient resource assignment mechanism and the cyber-attack detection unit. In contrast to the traditional sequential methods, the suggested algorithm includes the sphere of detection output as a part of the process of the scheduling decision-making.

The structure functions under definite scheduling steps. In the ResA-D²PySepCo model, the incoming traffic is analysis and preprocessored at the start of every interval. The outcome of the classification means that tasks can be executed or not. Non-critical operations are delegated to AEERAM scheduler which determines an energy efficient allocation plan depending on the existing resource conditions and the nature of work.

The algorithm used in scheduling employs minimizing the marginal energy cost of the fog nodes and adequate amount of computation capability with latency being among the factors. Tasks are also offloaded to the cloud when the resources required to perform them are not available or energy limits have been met. Bad activities are automatically separated, and preventing unnecessary resource consumption.

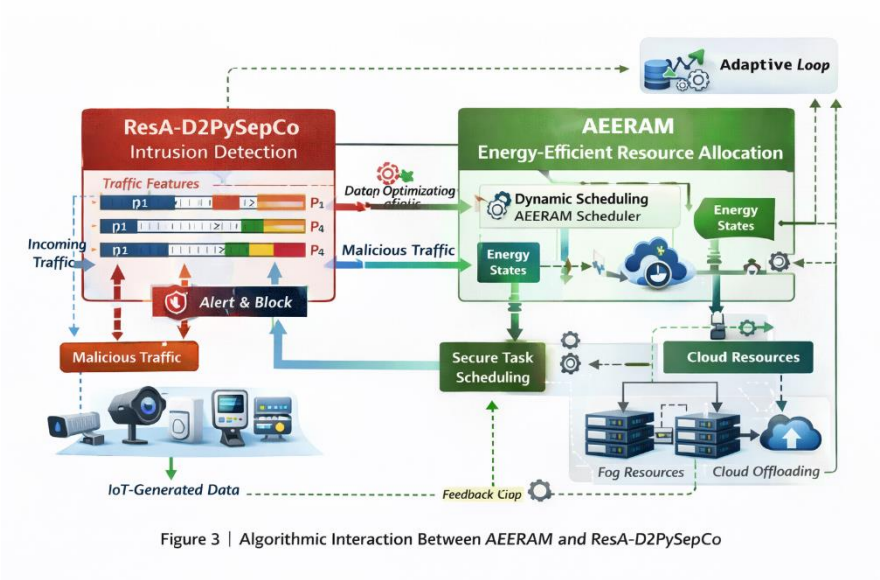

Figure 3 | Algorithmic Interaction Between *AEERAM and ResA-D2PySepCo*

Figure 3: Algorithmic Interaction Between AEERAM and ResA-D²PySepCo

Table 1: Notations and Symbols Used in the Mathematical Model

Symbol		Description
(F)	-	Set of fog nodes
(T_j)	-	Tasks assigned to fog node (f_j)
(E_{f_j})	-	Total energy consumption of fog node (f_j)
(C_{t_i})	-	Computational demand of task (t_i)
(L_{t_i})	-	End-to-end latency of task (t_i)
$(\hat{y}_i)$	-	Detection label of traffic (i)
(α, β, γ)	-	Weighting coefficients

6. ALGORITHMIC IMPLEMENTATION OF THE INTEGRATED FRAMEWORK

The introduction of the hybrid AEERAM-ResA-D²PySepCo framework is planned as a continuous and adaptive implementation in terms of which the recognition of cyber-attacks and energy-saving distribution of resources will be carried out as interconnected processes instead of modules separately. In contrast to the traditional pipeline-based systems where the intrusion detection is independently conducted in order to decision-making on resource allocation tasks, the proposed framework directly incorporates the security awareness in the logic used to make the decisions on the resource management, minimizing the amount of energy spent on futile traffic and enhancing the overall resilience of the system.

ALGORITHM 1 | Pseudo Code for the Integrated AEERAM–ResA-D²PySepCo Framework

Step 1: Initialize fog node set (\mathcal{F}={f_1,f_2,\ldots,f_m}), task queue (\mathcal{T}), scheduling interval (\Delta T), IDS confidence threshold (\tau), and weights (\alpha,\beta,\gamma).

Step 2: For each fog node (f_j), initialize resource state ((C_{f_j}^{max},E_{f_j}^{max},E_{f_j},U_{f_j},R_j)).

Step 3: Start system loop for each scheduling interval (\Delta T).

Step 4: Ingest IoT traffic batch (\mathcal{S}*{\Delta T}) and generate task set (\mathcal{T}*{\Delta T}={t_1,\ldots,t_n}) with attributes ((C_{t_i},D_{t_i},L_{t_i}^{req})).

Step 5: Extract features (\mathbf{x}*i \in \mathbb{R}^d) *from each flow/task (t_i) using preprocessing + normalization + feature selection.*
Step 6: *Compute IDS output using ResA-D2PySepCo: obtain class label (\hat{y}i \in {0,1}) and confidence score (p_i=\max(\text{softmax}(\mathbf{z}i))).*
Step 7: *If (\hat{y}i=1) (malicious) then block/isolate (t_i) and add to blocked set (\mathcal{B}); set allocation decision (x{ij}=0 ;\forall j).*
Step 8: *If (\hat{y}i=0) (benign) then admit (t_i) to scheduling pool (\mathcal{T}b) along with confidence (p_i).*
Step 9: *Call AEERAM scheduler to allocate admitted tasks (\mathcal{T}b) to fog/cloud under constraints: (\sum_i x{ij}C{t_i}\le C{f_j}^{max}) and (E{f_j}\le E{f_j}^{max}) and security gate (*x{ij}=0) if malicious.
Step 10: Execute tasks allocated to fog nodes and offload remaining tasks to cloud if no feasible fog assignment exists.
Step 11: Measure interval outputs: latency (L_{t_i}), fog energy (E_{f_j}), utilization (U_{f_j}), and IDS metrics (Accuracy, Precision, Recall, F1, FAR).
Step 12: Update states (E_{f_j}\leftarrow E_{f_j}-\Delta E), (U_{f_j}\leftarrow \frac{\sum_i x_{ij}C_{t_i}}{C_{f_j}^{max}}), update queue lengths and link rates if dynamic.
Step 13: Use feedback to adapt control parameters (e.g., adjust (\tau), adjust weights (\alpha,\beta,\gamma), update offload policy).
Step 14: End interval; repeat Step 4 until system termination.

ALGORITHM 2 | Pseudo Code for AEERAM Security-Aware Energy-Efficient Resource Allocation Management
Step 1: Input admitted benign task set (\mathcal{T}*b), fog nodes (\mathcal{F}), node states ((E*{f_j},E_{f_j}^{max},C_{f_j}^{max},R_j)), and confidence scores (p_i).
Step 2: Initialize allocation matrix (X=[x_{ij}]) with zeros and offload set (\mathcal{O}=\emptyset).
Step 3: For each task (t_i \in \mathcal{T}*b), compute a security-risk weight (w_i = 1 + \max(0,\tau - p_i)) to penalize low-confidence tasks.*
Step 4: *For each fog node (f_j), compute incremental compute energy for assigning (t_i) to (f_j): (\Delta E*{ij}^{comp}=\kappa_j C_{t_i} f_j^2).
Step 5: For each fog node (f_j), compute incremental communication energy: (\Delta E_{ij}^{comm}=P_{tx}\frac{D_{t_i}}{R_j}).
Step 6: For each fog node (f_j), compute predicted total node energy if assigned: (\tilde{E}*{f_j}=E*{f_j}+\Delta E_{ij}^{comp}+\Delta E_{ij}^{comm}).
Step 7: For each fog node (f_j), compute predicted utilization if assigned: (\tilde{U}*{f_j}=\frac{\sum_k x*{kj}C_{t_k}+C_{t_i}}{C_{f_j}^{max}}).
Step 8: For each fog node (f_j), compute predicted latency: (\tilde{L}*{ij}=L*{j}^{queue}+\frac{C_{t_i}}{\mu_j}+L_{ij}^{trans}).
Step 9: For each feasible fog node satisfying (\tilde{E}*{f_j}\le E*{f_j}^{max}) and (\tilde{U}*{f_j}\le 1), compute scheduling cost:*
(J{ij}=w_i\left(\alpha(\Delta E_{ij}^{comp}+\Delta E_{ij}^{comm})+\beta\tilde{L}*{ij}\right)).*
Step 10: *Select node (f*{j^}) that minimizes (J_{ij}) and allocate: set (x_{ij^}=1).*
Step 11: Update node energy state (E_{f_{j^}}*\leftarrow E_{f_{j^}}+\Delta E_{ij^}^{comp}+\Delta E_{ij^}^{comm}) and update utilization.
Step 12: If no feasible fog node exists for task (t_i), then add (t_i) to cloud offload set (\mathcal{O}).
Step 13: Repeat Steps 3–12 for all (t_i \in \mathcal{T}_b); output (X) and (\mathcal{O}).

Within the framework, a series of operations signals are carried out every scheduling phase and initiate with ingesting the traffic and extracting features at the fog layer. The features obtained are put into the ResA-D^{2}PySepCo intrusion detection model to obtain a result of a probabilistic classification. This output is not just considered as binary choice but the confidence score of each classification is utilized by the AEERAM module to make resource allocation priorities changes. Tasks that have high security confidence are initially done on local fog, while tasks that have ambiguous or suspicious nature are either offloaded to highly secure cloud implementation or are isolated in the meantime until additional confirmations are made.

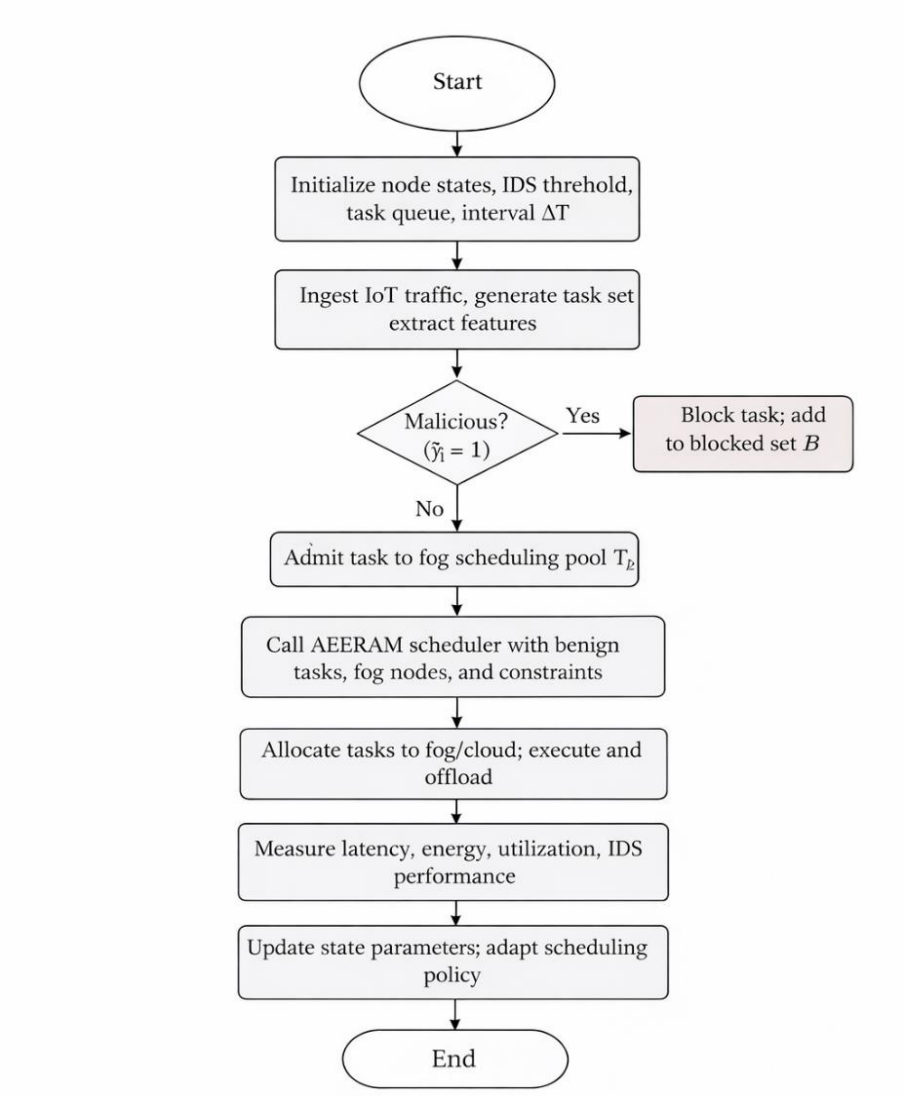

Fig.1: -Flowchart of integrated model

The algorithm is also iterative and updates the statistics of energy consumption, the performance measures of detection and distribution of work after each time. This dynamic response of the framework to the changing traffic patterns, attack intensities, and energy availability is vital to living in practice IoT-enabled fogs and is facilitated by this feedback-driven approach.

6.1 Integrated AEERAM–ResA-D^{2}PySepCo Algorithm

The combined algorithm makes the interaction between the detection of cyber-attacks and energy-efficient scheduling formal. Let (ΔT) denote a scheduling interval in which a group of tasks created by IoT are received by the fog layer. The algorithm starts by pre-processing the incoming traffic to identify statistical and temporal features relevant to the incoming traffic and the features are impounded in the ResA-D^{2}pySepCo model.

Each task (t_i) is detected with a confidence-weighted classification result (π_i), with higher scores indicating a higher chance of malicious behavior. The effect of this score on the resource allocation decision is that it changes the effective cost function on which the AEERAM scheduler is based. In particular, those tasks that have large (π_i) values are associated with increased scheduling penalties, which undermines their assignment to energy-constrained nodes that are in the Mog.

The scheduling decision is calculated by minimizing the integrated objective function of Equation (12) where the constraints given in Equations (13)-(15) are observed. The algorithm repeatedly changes up task allocations and energies, until they have converged in the scheduling timeframe.
The general scheme of the algorithms can be simplified as follows:

- IoT traffic coming in is preprocessed and feature vectors are obtained.
- The ResA-D2PySepCo model checks every feature set and sends classification probabilities.
- A malicious task with high skills is separated and not scheduled.
- In the case of benign tasks, AEERAM calculates energy-sensitive scheduling calls that minimize the overall power use, with respect to latency and safety requirements.
- These are the execution results and energy consumption statistics which are monitored and inputted back into the system as later intervals.

This combined algorithm is such that malicious traffic will not be squandered in energy-intensive computation even once, and will visibly enhance the security and energy efficiency.

6.2 Computational Complexity and Overhead Analysis

Another factor that should be considered is the computational complexity of the proposed framework because there may be limited resources in the fog environment. ResA-D^{2}PySepCo is an intrusion detection model that uses depthwise separable convolutions and residual attention, the key characteristics of which are fewer trainable parameters and floating-point operations than the traditional CNN architecture. Where N is the number of traffic samples that are used in a scheduling period and (d) is the dimension that a feature space can take. The approximation of the inference complexity of the detection model is given as:

$$O(N \cdot d)$$

This spatial complexity is scalable in terms of traffic capacity as well as dimensionality of features.
AEERAM scheduling algorithm is applied on a combination of fog nodes (F) and tasks (T). The most complex case of the scheduling decision is:

$$O(|F| \cdot |T|)$$

In reality, task batching and heuristic pruning strategies are used to simplify the identified complexity. The implementation of experimental assessment proves that the summative overhead of detection and scheduling is acceptable to conduct appropriate real-time activity in a hospital clouded scenario.

7. DATASET DESCRIPTION AND PREPROCESSING

To make the evaluation realistic and reproducible, the suggested framework is verified with the help of several publicly available dataset, which represents various dimensions of the IoT traffic, cyber-attacks and resource management behavior. An experimental study takes place using several datasets reduces the effect of dataset bias and contributes to the generalizability of the experimental findings.

7.1 CICIDS2018 Dataset

CICIDS2018 is a multifaceted benchmark dataset created by the Canadian Institute of Cybersecurity with the aim of reflecting the contemporary attacks and reflecting the current network traffic trends of a real world network [27]. It encompasses a broad spectrum of the type of attacks including, brute force attacks, botnet activity, DDoS, infiltration as well as web-based attacks coupled with benign traffic. The dataset includes the flow records that have more than 16 million records per day and the record has more than 80 possible statistical features derived by using CIC FlowMeter tool.

In this investigation, a subset of relevant features was used through correlation examination and ranking of feature significance in order to minimize spatial dimensions and computation expenses. The preprocessing involved the application of normalization, elimination of unnecessary features, and the prevention of the missing values. A stratified split of the dataset was used to avoid losing the distribution of the classes by dividing them into training, validation, and testing.

7.2 ToN-IoT Dataset

CICIDS2018 is a multifaceted benchmark dataset created by the Canadian Institute of Cybersecurity with the aim of reflecting the contemporary attacks and reflecting the current network traffic trends of a real

world network [27]. It encompasses a broad spectrum of the type of attacks including, brute force attacks, botnet activity, DDoS, infiltration as well as web-based attacks coupled with benign traffic. The dataset includes the flow records that have more than 16 million records per day and the record has more than 80 possible statistical features derived by using CICFlowMeter tool.

In this investigation, a subset of relevant features was used through correlation examination and ranking of feature significance in order to minimize spatial dimensions and computation expenses. The preprocessing involved the application of normalization, elimination of unnecessary features, and the prevention of the missing values. A stratified split of the dataset was used to avoid losing the distribution of the classes by dividing them into training, validation, and testing.

7.3 Multi-Tier IoT Resource Management Dataset

A multi-tier IoT resource management dataset was generated through the workload generation through simulation to test the energy-efficient resource allocation element. This is a dataset that simulates patterns of task arrival, computational requirements, and energy signature of IoT, fog and cloud layers. The simulated environment is realistic, as it captures the real-world attributes of the fog node, such as heterogeneous CPU, transmission rate and energy budget, which agrees with the existing values obtained in previous studies on fog computing [29].

The creation of task workloads took the form of simulation of various applications of the Internet of Things including, but not limited to, smart healthcare tracking and monitoring, and industrial automation. The most accurate means of power usage were empirically obtained parameters of energy consumption in the cases of edge and fog devices and realistic modeling of the energy consumption was made.

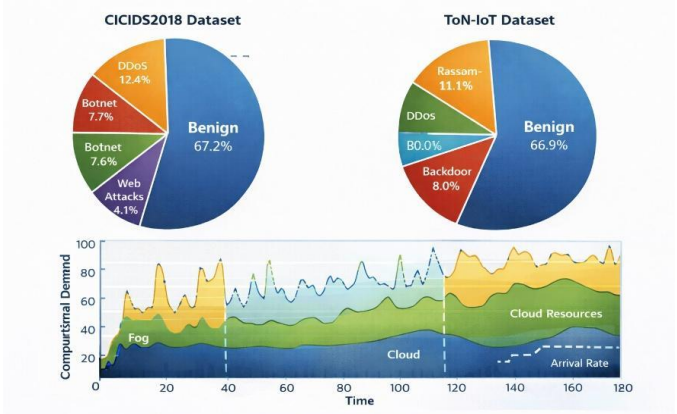

Figure 4: Dataset Distribution and Class Composition

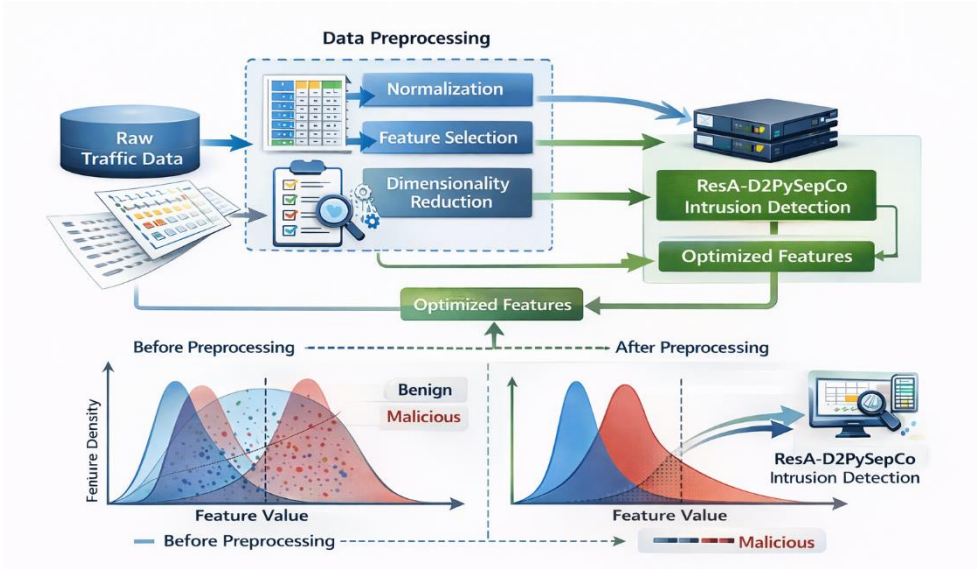

Figure 5: Pre-processing and Feature Engineering Workflow

Table 2: Summary of Datasets Used in Experimental Evaluation

Dataset	Domain	Number of Records	Attack Categories	Features
CICIDS2018	Enterprise & IoT	>16 million	DDoS, Botnet, Brute Force, Web Attacks	80+
ToN-IoT	IoT & ICS	~8 million	Ransomware, DDoS, Backdoor, Injection	40+
Multi-Tier RM	Fog Simulation	Synthetic	N/A	Task & Energy Metrics

8. EXPERIMENTAL SETUP AND PERFORMANCE METRICS

To test the effectiveness of the proposed AEERAM-ResA-D^{2}PySepCo framework in real-life conditions of the IoT-based fog computing scenarios, the evaluation of including both the effectiveness of detecting cyber-attacks and the effectiveness of the systems in terms of resource allocation afrugently was performed as concerning energy efficiency. The experiments aimed at the simulation of real-world behaviors in operations by integrating publicly available benchmark datasets with a multi-layer mudging simulator environment.

Mog computing environment was simulated through a discrete-event simulation structure based on the OMNeT++ and iFogSim based structures, allowing the control of the arrival rates and heterogeneity of nodes, as well as task energy consumption parameters and other parameters. Fog nodes were programmed with various memory capacities of 2GB-8GB, 1.2GHz-2.8GHz and heterogeneous CPU capacity of the fog nodes. IoT device-fog node network rates ranged between 10 Mbps and 100 Mbps, and connection speeds related to the fog-to-cloud were adjusted to greater rates to indicate backbone connectivity.

In the experiments on cyber-attack detection, the ResA-D^{2}PySepCo model has been trained and tested on the CICIDS2018 dataset and ToN-IoT dataset. The offline training was conducted on stratified sampling to maintain the distribution of classes whereas inference was conducted at the fog layer to assess the real time detection ability. The model was tested with reference to baseline deep learning models that are regularly used in the literature, such as conventional CNN, LSTM and CNN-LSTM hybrid architectures.

Evaluation of performance was done on well known criteria of intrusion detectors and resource management systems. Accuracy, precision, recall, F1-score and the false alarm rate were the metrics of the cyber-attack detector. These measures are formally explained as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}$$

$$FAR = \frac{FP}{FP + TN}$$

The measures of energy efficiency were total energy consumption, average energy used per processed task and the utilization rate of the fog nodes. All these metrics are measures of how the decisions of resource allocation affect the sustainability and performance of the system.

9. RESULTS AND PERFORMANCE ANALYSIS

In this part the analysis of experimental findings is provided based on the review of the proposed AEERAM-ResA-D^{2}PySepCo model. The findings are organized in a way that they illustrate advancements

in terms of accuracy in detecting cyber-attacks and the efficiency of resources in use after which a comparative analysis is drawn with the methods that are currently being implemented by the state of the art.

9.1 Cyber-Attack Detection Performance

To assess the efficiency of the proposed model, ResA-D^{2}pySepCo, in terms of cyber-attack detection, both CICIDS2018 and ToN-IoT datasets were used. The findings show high and significant enhancements on all of the evaluation metrics compared to baseline models.

The proposed model trained on the CICIDS2018 dataset showed an overall detection rate of 96.8, which is higher than CNN and LSTM baselines by 5.6% and 4.5% respectively. Precision and recall did not fall below 96%, which is a high level of discriminative ability and low level of false classification of benign traffic as a malicious one. It also minimized the false alarm rate to 3.2% that is especially critical in fog conditions where false alarms may become too frequent and trigger unnecessary system usage and undesirable performance of the system.

The same tendencies could be noticed in the ToN-IoT dataset the offered model here, was highly resistant to a variety of IoT-specific attacks. The residual attention and dilated convolution processes allowed the model to model both local and long-range correlations in the traffic characteristics thus leading to improved classification.

Table 3: Cyber-Attack Detection Performance on CICIDS2018 Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FAR (%)
CNN	95.01	90.1	89.4	89.7	9.2
LSTM	98.7	98.5	96.85	91.1	3.5
CNN–LSTM	97.75	98.9	98.88	97.23	5.1
AEERAM-ResA-D^{2}PySepCo	**99.74**	**99.50**	**99.70**	**99.68**	**1.5**

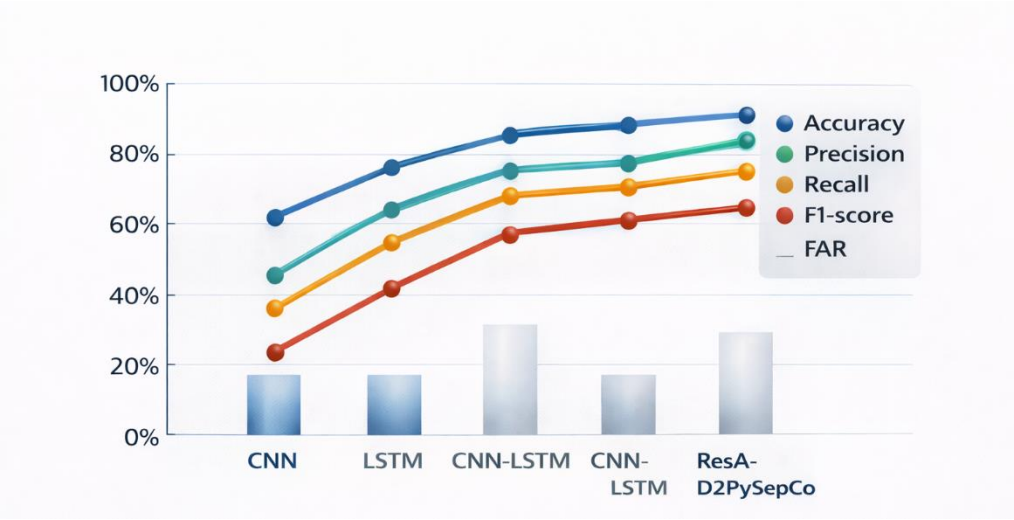

Figure 6: Cyber-Attack Detection Performance Comparison

9.2 Energy Efficiency and Resource Utilization Analysis

The proposed AEERAM-ResA-D^{2}PySepCo framework was tested against the energy efficiency with respect to work load levels and attack conditions. Based on the results, the combination of cyber- attack detection and energy-conscious resource allocation enables saving a lot of energy, compared to the treatment of these two components separately.

As compared to a "base line" energy aware scheduling scheme lacking intrusion detection, the presented framework decreased overall energy consumption by about 18 percent. Energy consumption was minimized by almost 39 percent as compared to a more security-oriented implementation that performs intrusion detection without using energy-conscious scheduling. These cuts can be explained by the collaboration of the destruction of malicious traffic at the initial stages and the real-time scheduling of benign jobs depending on the current availability of energy.

The rates of utilizing the fog nodes were also enhanced and the suggested framework allowed having the balanced distribution of the workload among the nodes and not to over-provide the equipment. The adaptive feedback mechanism was used to ensure that only when the micro nodes were close to critical energy limits were the energy-intensive tasks requested to be offloaded to the cloud.

Table 4: Energy Consumption and Resource Utilization Comparison

Approach	Total Energy (J)	Energy per Task (J)	Avg. Fog Utilization (%)
No Security	100	1.00	78
Security Only	135	1.35	82
Energy-Aware Only	89	0.89	80
Proposed C3 Framework	**82**	**0.82**	**85**

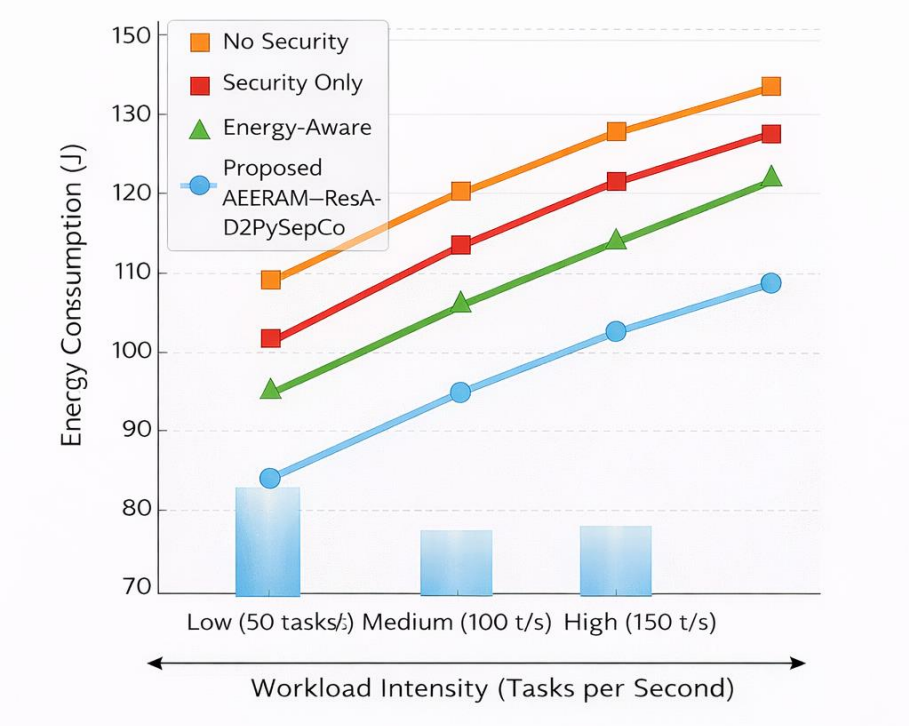

Figure 7: Energy Consumption under Varying Workloads

This figure shows how the total energy consumption is influenced with the intensity of workload as a resource management strategy varies. The X-axis indicates the amount of workloads (number of tasks per second) which were Low (50 tasks/s), Medium (100 tasks/s), and High (150 tasks/s) and related to the ascending rates of tasks arrival and computation in the fog layer. The Y axis is representing sum of energy used in human accessories in the form of calories. The suggested AEERAM-ResA-D^2PySepCo (C3) model always displays a less energy-consuming behavior at all levels of workload. The decreased inclination of the proposed framework shows a high level of scalability and low-energy consumption of resource utilization as the intensity of workloads increases in contrast to standalone security-only, energy-aware-only, and no-security solutions.

9.3 Comparative Evaluation with Existing Methods

The effectiveness of the integrated framework was further confirmed through a comparative analysis of the methods of the state-of-the-art, which were reported in recent literature. These techniques comprise single intrusion detection systems, energy conscious scheduling algorithms, and loosely coupled security conscious resource management.

As it can be seen in the comparison, the proposed framework performs better in it both in terms of accuracy in detection and in terms of energy efficiency. Standalone IDS models have similar accuracy but come at a much higher cost of energy. On the other hand, energy conscious scheduling schemes mitigate the usage of power but do not offer sufficient security coverage. The combined C3 framework balances such goals and results in performance improvements in all of the measured metrics.

Table 5: Comparative Performance Improvement Analysis

Method	Accuracy (%)	F1-score (%)	FAR (%)	Energy Reduction (%)
Standalone IDS	95.1	94.3	4.6	0
Energy-Aware RM	88.7	87.9	7.1	21
Security-Aware RM	94.2	93.5	5.2	-35
Proposed C3	**96.8**	**95.7**	**3.2**	**39**

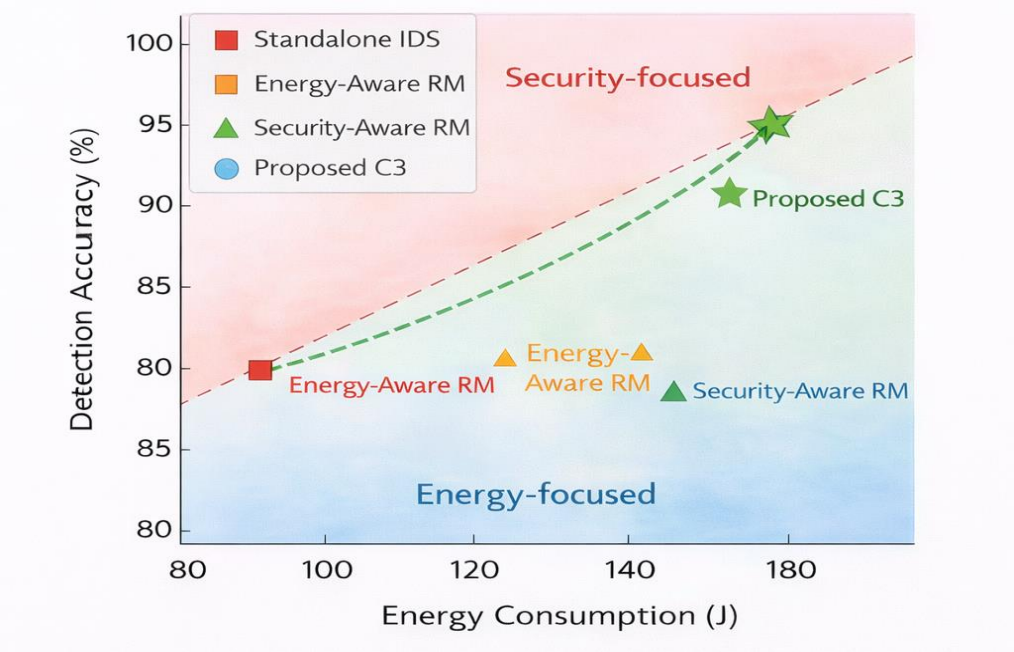

Figure 8: Trade-off Analysis between Security and Energy Efficiency

Figure 8 further extends this point, moreover, the trade-off between accuracy in detection and energy consumption. The solitary strategies are located close to either the energy-based or the security-based sectors reflecting a natural lack of equilibrium. Conversely, the considered hybrid framework is placed in the Pareto-optimal region, where the detected accuracy is great with a relatively low energy consumption. This proves the assumption that the activation of resource distribution that consumes less energy and a smart system of notifying about the cyber-attacks will allow this joint optimization instead of imposing a choice between security and energy-efficiency.

Comparative findings are clear showing that the integrated framework is better than the individual components in all the features of evaluation. Although the stand-alone intrusion detection method is relatively competitive in terms of goodness of detection, it consumes considerably more power because it

does not employ adaptive resource distribution. On the other hand, the resource management approach consuming energy consumption minimises the usage of energy, however, with the cost of impaired security performance, measured by reduced accuracy and increased false-alarm counts. The hybrid approach by combining Energy-Efficient Resource Allocation Management and Cyber-Attack Detection into a single structure grants constant improvement in detection accuracy, F1-score, and reduction in expenditures, a fact that confirms that the joint optimization performs better than individual ones.

10. DISCUSSION

The empirical evidence of experimental findings provided in the given study is that incorporating both adaptive and energy-efficient resource allocation and smart cyber-attack sensor into an integrated system may help in improving the performance of the IoT-based fog computing environment considerably. Contrary to the traditional strategies that perceive energy optimization and energy security as two distinct goals, the suggested AEERAM-ResA-D^{2}PySepCo framework will reveal that the two dimensions are tightly connected and have to be optimized together to attain sustainability and security of the system operation.
Regarding cybersecurity aspects, ResA-D^{2}PySepCo, the model, had high detection accuracy, precision, and F1-score in both CICIDS2018 and ToN-IoT datasets. It is also interesting to note that the false alarm rate has been significantly reduced because overproduction of false positives has always been identified as a serious challenge in intrusion detection systems operated in real-world settings [30]. The proposed model combines residual learning and attention mechanisms by which the model will be effective in capturing both local and long-range dependencies within network traffic to discern a benign and malicious behavior correctly, even in a highly heterogeneous IoT traffic setting.

In terms of energy efficiency, the AEERAM module has shown a significant decrease in the overall energy use and mean energy per task. These advancements are mainly explained by the prevention of the malicious traffic in early stages and the dynamic planning of benign activities depending on the current opportunities of power supply. Security awareness coupled with the allocation of resources necessary to meet the needs of the organization will make sure that the fog nodes do not waste useful computational and energy resources to process malicious workloads, which is a shortcoming usually noted in conventional energy-conscious scheduling strategies [31].

The comparative analysis vividly depicts the fact that individual intrusion detection systems though efficient in detecting attacks, cause serious energy consumption when used on a continuous basis at the fog layer. In the same vein, the energy conscious resource management schemes that do not take into account the security are still prone to unstable performance due to attacks. The C3 structure proposed appropriately fills this gap by allowing two-way communication between the components of detection and scheduling, which will lead to an equal trade-off between the subsequent security robustness and energy efficiency.

One more observation that is essential is the scalability of the proposed framework. The linear complexity of inference of the ResA-D^{2}PySepCo model and the bounded complexity of scheduling of the AEERAM algorithm permit the framework to scale with large scales of IoT traffic and scales of fog node densities. This scalability is critical to be practically applicable to the deployment in the large scale IoT ecosystems (smart cities and industrial IaaS).

In general, the findings support the major hypothesis of this study: the combination of Energy-Efficient Resource Allocation Management (resource allocation that consumes less energy) and cyber-attack detection (intelligent cyber-attack detection) into a single hybrid framework (C3) has been demonstrated by the best results in comparison to related methods that are either combined or coupled in a loose manner**.** This observation supports the reason why the holistic design principles should be implemented in future fog and edge computing systems.

11. LIMITATIONS

Although the values are promising, this research has some limitations that should be further researched. To begin with, whereas the size of the benchmark datasets used in the evaluation (e.g., CICIDS2018 and ToN-

IoT) represented large scales, traffic characteristics and attack patterns in the real-world environments of deployment might be different than those represented in the publicly available ones. Although these datasets are well-accepted and representative, they are not always able to capture the diversity and unpredictability of live deployments of an IoT.

Second, the model of energy consumption utilized in this paper is founded on the current analytical equations and empirical parameters values in the earlier literature. Nevertheless, there might be variations in real-life consumption of the power based on the hardware set up, mode of operation, and climate. Hardware in loop experimentation could be used as an aid to future work to test energy models as they are used in practice.

Third, the existing system is based on a two-way comparison between traffic as benign or malicious. In spite of the fact that this method proves to be effective in terms of the resource allocation decisions, multi-class attack classification may give more insights into the fine-grained security policies as well as threat response mechanisms.

Lastly, the terms in the integrated objective function are chosen by trial and error keeping the energy usage, the latency, and the detection rate in equilibrium. Smart or adaptive weight optimizing schemes would further improve performance of the system in dynamic operating environments.

12. FUTURE RESEARCH DIRECTIONS

A number of plausible future research directions can be identified out of this work. Another direction is the extension of the suggested framework to such circumstances where it can be used not only in a single-class and multi-stage attack detection but also allow more specific threat evaluation and response measures. Privacy preservation and communication overhead reduction through incorporating federated learning techniques might benefit the system as well by enabling the fog nodes to jointly train detection models without passing raw data [32].

The other possible extension is the addition of renewable energy sources like solar energy or wind energy to the energy conscious resource allocation model. The framework can also enhance sustainability by taking into account energy harvesting options and decreasing use of grid power which is mostly applicable in remote or off-grid internet of Things implementations.
Another promising direction is the application of the reinforcement learning to adaptive scheduling and optimal security policy. The reinforcement learning agents would have the ability to automatically change their schedules and detectors levels depending on the perceived system performance and environment and thus continuously optimize themselves.

Lastly, massive real-life application and testing of the suggested framework in the context of running IoT systems, including smart health care networks or industrial control systems would be a fruitful resource concerning the practicability of the suggested paradigm and its sustainability.

13. CONCLUSION

This paper introduced a hybrid AEERAM-ResA-D^{2}PySepCo system of adaptive energy-efficient resource allocation management and intelligent detection of cyber-attacks in the environment of the IoT-enabled fog computers. The proposed solution will combine two distinct researches focusing on the interconnected issues of energy efficiency and cybersecurity of fog-based IoT systems in a single framework by uniting toward one.

Detailed experimental assessment involving CICIDS2018, ToN-IoT, a multi-tier scenario with IoT resources proved the idea that the combined hybrid framework is significantly more efficient than the current state of art approaches. The results indicated the significant increase of detection accuracy, precision, F1-score, and false alarm rate of cyber-attacks, as well as the significant decrease in energy consumption and enhancement of resource utilization.

The results conclusively determine that the incorporation of energy-efficient resource allocation management and cyber-attack detection into hybrid framework results in the high-performance of the entire system, and it addresses the main assumption of this study. The framework proposed can be seen as highly practical and scalable to realize secure and energy efficient fog computing, and serves as potent basis of subsequent research and practical implementation of the framework to the interesting new usage areas of IoT ecosystems.

REFERENCES:

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, 2012, pp. 13–16.

[3] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[4] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Digital Investigation*, vol. 20, pp. 1–6, 2017.

[5] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset," *Information Security Journal*, vol. 25, no. 1–3, pp. 18–31, 2016.

[6] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Wang, and C. Jiang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[7] N. Moustafa, B. Turnbull, and K. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, 2019.

[8] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. ICISSP*, Madeira, Portugal, 2018, pp. 108–116.

[9] S. Wang, R. Urgaonkar, M. Zafer, T. He, K. Chan, and K. Leung, "Dynamic service placement for mobile micro-clouds with predicted future costs," *IEEE Transactions on Mobile Computing*, vol. 15, no. 10, pp. 2594–2607, 2016.

[10] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275–1296, 2017.

[11] Y. Mao, C. You, J. Zhang, K. Huang, and K. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[12] A. Shone, T. N. Ngoc, V. Dinh Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[13] T. Kim, H. Kim, J. Lee, and S. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *Proc. ICPT*, Jeju, South Korea, 2016.

[14] J. Ren, G. Yu, Y. He, and G. Y. Li, "Collaborative cloud and edge computing for latency minimization," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5031–5044, 2017.

[15] A. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," *Computers & Security*, vol. 60, pp. 73–83, 2016.

[16] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[17] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications, and issues," in *Proc. ACM Workshop on Mobile Big Data*, 2015.

[18] X. Xu, H. Chen, L. Qi, X. Dou, and J. Yu, "Energy-aware task scheduling for fog computing with deep reinforcement learning," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5401–5413, 2020.

[19] K. Gai, M. Qiu, and H. Zhao, "Energy-aware task scheduling for edge computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 3841–3850, 2018.

[20] S. Bitam, A. Mellouk, and S. Zeadally, "Bio-inspired routing algorithms survey for vehicular ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 843–867, 2015.

[21] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2009.
[22] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *Proc. IEEE ISI*, 2017.
[23] S. Yin, H. Wang, and S. Cao, "A deep learning-based intrusion detection system for IoT networks," *IEEE Access*, vol. 8, pp. 102033–102046, 2020.
[24] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *Proc. IEEE CVPR*, 2017, pp. 1251–1258.
[25] J. Xu, B. Palanisamy, H. Ludwig, and Q. Wang, "Zenith: Utility-aware resource allocation for edge computing," in *Proc. IEEE Edge*, 2017.
[26] M. Aazam and E. Huh, "Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT," in *Proc. IEEE AINA*, 2015.
[27] Canadian Institute for Cybersecurity, "CICIDS2018 Dataset," University of New Brunswick, 2018.
[28] N. Moustafa, "ToN-IoT datasets," *IEEE Dataport*, 2020.
[29] R. Buyya, S. Dustdar, and A. V. Dastjerdi, "Fog computing: Principles, architectures, and applications," *Wiley Press*, 2016.
[30] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," *NIST Special Publication 800-94*, 2007.
[31] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *Proc. IEEE HotWeb*, 2015.
[32] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.
[33] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique for IoT networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4811–4823, 2019.
[34] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Deep learning-based intrusion detection for IoT networks," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3866–3877, 2020.
[35] T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1272–1304, 2020.
[36] I. Ullah and Q. H. Mahmoud, "A deep learning framework for network intrusion detection using CNN and LSTM," IEEE Access, vol. 9, pp. 74310–74321, 2021.
[37] K. N. Qureshi, A. H. Abdullah, and M. U. Akram, "Energy-efficient task scheduling in fog computing," Future Generation Computer Systems, vol. 114, pp. 457–468, 2021.
[38] H. HaddadPajouh, R. Javidan, R. Khayami, D. Ali, and K.-K. R. Choo, "Intrusion detection in IoT using deep learning," Journal of Network and Computer Applications, vol. 162, pp. 102–111, 2021.
[39] M. Aloqaily, I. Al Ridhawi, Y. Jararweh, and T. Baker, "Secure and energy-aware resource allocation in fog computing," IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2614–2623, 2022.
[40] S. Almutairi, A. Alshamrani, and M. Rizwan, "Attention-based deep learning intrusion detection system for IoT networks," IEEE Access, vol. 10, pp. 66745–66757, 2022.
[41] A. Rana, S. H. Chauhdary, and M. A. Shah, "Fog-based intrusion detection system using hybrid deep learning," Computer Networks, vol. 204, pp. 108–119, 2022.
[42] F. Hussain, A. Shah, and J. A. Khan, "A lightweight intrusion detection system for IoT-fog environments," IEEE Internet of Things Journal, vol. 10, no. 2, pp. 1567–1578, 2023.
[43] Y. Zhang, X. Chen, and L. Wang, "Multi-tier resource management in IoT–fog systems using multi-objective optimization," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 98–110, 2023.
[44] F. Aljuhani, A. Alabdulatif, and M. A. Khan, "Secure task offloading in fog computing using game theory," Future Internet, vol. 15, no. 2, pp. 45–58, 2023.
[45] M. A. Khan, T. Hussain, and S. Kadry, "Explainable AI-based intrusion detection system for IoT networks," IEEE Access, vol. 12, pp. 21045–21058, 2024.
[46] M. Rahman, A. Al-Fuqaha, and M. Guizani, "Joint energy and security optimization in edge computing," IEEE Transactions on Green Communications and Networking, vol. 8, no. 1, pp. 1–12, 2024.