**Journal of Information Systems Engineering and Management**
2025, 10(30s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# AI-Based Secure and Energy-Efficient Framework for Multi-Tenant Cloud Systems

Dr. G. Rajesh[1*], D. Amu[2], Dr. B. Adithya[3], Surya Pogu Jayanna[4], B Sangeetha[5], Ranjith Janakiraman[6]
[1]Associate Professor, Department of CSE, Vignan's Institute of Management and Technology for Women, Hyderabad, India.
[2]Research Scholar, Department of Computer Science and Engineering, Puducherry Technological University, Puducherry, India.
[3]Associate Professor, Department of CSE (AI&ML), Geethanjali College of Engineering and Technology, Hyderabad, India.
[4]Assistant Professor, CSE (AI&ML), Vignan's Institute of Management and Technology for Women, Hyderabad, India.
[5]Assistant Professor, CSE (DS), Vignan's Institute of Management and Technology for Women, Hyderabad, India.
[6]Assistant Professor, IT, Vignan's Institute of Management and Technology for Women, Hyderabad, India.
Email: [1]rajesh@vmtw.in, [3]badithya.cse@gcet.edu.in, [6]ranjith@vmtw.in

**ARTICLE INFO**

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

**ABSTRACT**

This paper proposes an adaptive, energy-aware, and secure architecture for a multi-tenant cloud environment, which aims to solve cloud computing systems' security, energy, and performance problems. Thus, with a vast increase in cloud adoption across markets, industrial sectors like healthcare, IoT, finance, cybersecurity, and efficient resource management have become a high priority. These needs are met by the Hybrid Intrusion Detection System (IDS), the Energy-Aware Resource Management (ERM), and an AI-based Load Balancer within the context of the proposed framework. The proposed Hybrid IDS uses auto encoders for anomaly detection and CNNs for attack classification to identify known and unknown threats. Based on the proposed model, it achieved 98.7% accuracy and a good F1 Score of 20, which is good enough to detect new and common intrusions. The ERM module efficiently uses energy through the RL approach to manage resources dynamically, while ACO is applied for scheduling. This is done in an energy-efficient way, using 22% less energy than traditional schedulers while at the same time boosting CPU utilization. While forward-projecting workloads are based on basic historical measures, the AI-based Load Balancer has 36% lower latency and 28% higher throughput than Round-Robin scheduling. This makes it highly efficient in cases where varied performance may be required in terms of time. The work presented in this paper suggests a novel approach that offers a solution to these problems and supports security, energy efficiency, and high performance, effectively removing the drawbacks of current methods. Future work will include the integration of quantum clouds with others, edge computing support, and multi-cloud support to bring better scalability and resilience. This research shows that cloud infrastructures can be adequate for security and sustainability while meeting today's technological environment requirements.

**Keywords:** *Cloud Computing, Intrusion Detection System, Energy-Aware Resource Management, AI-Based Load Balancer, Multi-Tenant Cloud.*

## INTRODUCTION

The ability to access scalable resources and computing infrastructure remotely has made cloud computing the basis upon which modern digital services are built. It provides a range of service models ranging from Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) to Software-as-a-service (SaaS), which serve unique operational needs. With the rise of cloud services, though, particularly multi-tenant parts of the cloud, come many operational aspects. Multiple tenants use shared Virtualized infrastructure in [1], and data privacy, intrusions, and 0-day attacks come into consideration. Energy consumption in data centers has also become a critical issue in parallel as cloud providers try to find a sustainable way to lessen operational costs and carbon footprints [2]. This research proposes an adaptive security and energy-efficient framework for multi-tenant cloud environments to tackle these challenges. For instance, a multi-tenant cloud environment can provide a practical scenario where healthcare, e-commerce, and educational services are hosted on the same VMs for sharing. Each tenant has distinct requirements: The need for healthcare services necessitates high data security and availability, e-commerce requires low-latency processing

during peak load, and educational platforms require scalability to accommodate sudden traffic spikes at the time of enrolment. However, balancing these demands, security, and energy consumption optimization is a hard problem for the cloud provider. However, contention among resources plays a degrading role in performance and can cause delays during peak loads, while cyberattacks can jeopardize sensitive data, which is especially important for healthcare scenarios. The focus has been on providing a framework that, together with the ORA, seeks to offer enhanced security, efficient management of workloads and energy consumption [3], [4].

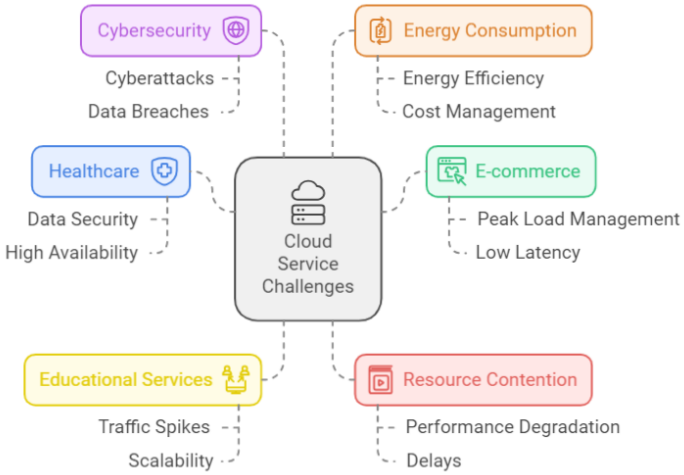


**Figure 1.** Challenges in the Cloud services

To address these challenges, this paper proposes an adaptive security and energy-efficient framework that combines two modules: A Hybrid Intrusion Detection System (IDS) and Energy-aware Resource Management (ERM). The IDS uses autoencoders and Convolutional Neural Networks (CNN) to detect known and unknown real-time attacks in a secure environment. In parallel, the ERM module achieves dynamic resource allocation and energy efficiency while maintaining system utilization using two reinforcement learning (RL) and Ant Colony Optimization (ACO) algorithms. The proposed framework integrates security and energy management, addressing two critical cloud computing challenges. The two novel aspects of our approach are (1) adaptive intrusion detection to defend against emerging cyber threats and (2) intelligent resource scheduling to minimize power consumption on hardware sensors. The energy-aware scheduler regulates resource usage for optimal performance and to achieve energy saving, and the hybrid IDS provides continuous protection against known and unknown attacks. Green computing and cloud security objectives are met regarding the roots; this research offers a scalable, sustainable, and secure solution to cloud providers. The subsequent sections of this paper are structured as follows: In Section II, we discuss related work in intrusion detection and energy management in cloud environments. The methodology is laid out in Section III, which describes the design of the hybrid IDS and the energy-aware resource manager. Experiments were performed using two datasets in Section IV: CICIDS2017 and KDDCup99. Section V concludes, and future work is discussed.

## RELATED WORK

As a core enabler of digital transformation, cloud computing is advancing data management, scalability, and multi-tenancy. Nevertheless, some open issues remain, especially in intrusion detection, resource management, energy efficiency, load balancing, and cloud service integration. In this section, we review the latest studies on these issues, identify gaps, and outline the need for future research.

### A. Cloud Environment Intrusion Detection Systems (IDS)

Distributed Denial of Service (DDoS) attacks, malware injections, and zero-day exploits are all highly prevalent in cloud platforms. Typically, traditional IDS solutions based on signature-based detection techniques fail to detect them. Introduced a hybrid IDS that integrates DBSCAN clustering with auto-encoders to prevent malicious activities without a labelled dataset [1]. Datasets like CICIDS2017 and KDDCup99 proved to be successful in their method for anomaly identification using high accuracy. However, they need to be more capable of real-time adaptation. Another area covered in this thesis is the integration of intrusion detection with healthcare systems in a cloud environment. Real-time the real-time EEG analysis group applied A.I. models to predict epileptic seizures [2]. Although this work centres on medical data processing, it has implications for more general real-time A.I.-based threat detection in cloud

cybersecurity. Adaptable A.I. Computerized IDS arrangements are fundamental to performing productively over different cloud workloads. However, more research is required in this area.

### B. Health Care, IoT, and Security A.I. Enabled Solutions

Reliable, real-time systems have become critical to the reliance on cloud computing in healthcare, IoT, and fire safety management. In their study, [6] integrated cloud computing on a Bluetooth-based fire hazard detection system for early warning and dynamic monitoring. The system illustrates the need for real-time data processing in cloud environments and for detecting cyber-attacks. Furthermore, the cloud platform security is not its only versatility. The author examined the role of cloud services within education [7], emphasizing the need for cloud environments to be scalable and secure for use within educational institutions. Nevertheless, integrating real-time systems with security protocols so they can handle the enormous amounts of data that flow through those systems in a way that keeps them from slowing doesn't down remains a challenge.

### C. Resource and Energy Efficiency:

Resource management in cloud environments has to be efficient, especially in multi-tenant systems with varying workloads. The author proposed A.I. approach for task scheduling with hierarchical networks to improve task throughput [4]. However, these still neglect energy consumption. In [3], worked on data compression techniques and encryption protocols to improve storage and secure data in the cloud. However, resource management needs more work to strike a balance between better performance and energy efficiency. In [8], discuss the importance of green computing, emphasizing the importance of energy-efficient scheduling algorithms in data centres. While current work tends to optimize performance, energy consumption is recognized as a pervasive issue. In [10], explored multi-cloud integration and resource management strategies. Still, the need for advanced A.I.-based algorithms to achieve energy efficiency and scalability is challenging.

### D. Heterogeneous Workload Load Balancing Algorithms

Because performance variations in cloud systems are maintained along the same range by load balancing, Ant Colony Optimization (ACO) algorithms implemented by [5] are used to ensure better workload distribution across virtual machines and better throughput and response time. These algorithms are nevertheless limited in their support for heterogeneous and dynamic workloads, as expected from multi-tenant systems. Another study focuses on cloud load balancing strategies in an educational context when scalable service delivery is important. A study by A World with Cloud Computing [11] highlighted the increasing use of cloud services for education but observed that presently popular load-balancing methods could be more effective in the face of unexpectedly high demand. This means there is a need for more adaptive, load-aware scheduling mechanisms.

### E. Service Integration of Cloud Security and Cloud Service Integration

Cloud platforms must balance security, scalability, and energy efficiency while serving divergent tenants. One investigation to analyse the future potentiality of integrating quantum computers into cloud systems was done by [12], who advanced to propose that hybrid cloud infrastructures can contribute to overcoming the computational bottlenecks in conventional cloud systems. Such integration, however, introduces new security issues, interoperability and resource utilization. Meanwhile, in the paper "Cloud Computing: In "Cloud Computing: Applications, Challenges and Open Issues," [13] a complete overview of cloud computing models and their limitations, which suffer from privacy issues and resource contention in shared infrastructures, is given. These studies motivate a discussion of unified frameworks considering multiple security dimensions, energy efficiency, and scalability.

### F. Research Gaps and Motivation

Several gaps in the literature are critically identified. Among them, the first topic is the intrusion detection systems (IDS) that must be more adaptive to react adequately to real-time zero-day attacks. While existing IDS models are often very effective in detecting known attacks, they fail to deal with the dynamic threat and must be coupled with AI-driven AI learning models. Further, although resource management techniques concentrate on performance, there is an absence of energy-aware frameworks that mitigate the environmental effect of cloud operations. Third, further refinement of load balancing algorithms is needed to better account for diverse workloads, especially when workloads are multi-cloud or IoT integrated. This research is motivated to satisfy these gaps with a unified framework

consisting [14-16] of AI-driven IDS, energy-aware task scheduling, and adaptive load balancing to improve the security and sustainability of cloud computing.

## PROPOSED METHODOLOGY

The adaptive security and energy efficient framework presented here intends to solve the multi-tenant cloud issues related to security and energy consumption. The framework integrates three core modules: The threat detection is accomplished through the Hybrid Intrusion Detection System (IDS), the latter being the Energy-Aware Resource Manager (ERM) to manage resources effectively and an Artificial Intelligence-driven Load Balancer for VM's management tasks. From here, each module is described in terms of design, implemented algorithms, and functionalities, showing how they improve cloud operations.

### A. Framework Architecture Overview

The proposed framework is illustrated in the architecture of Figure 2. It shows how the Hybrid IDS, ERM, and the AI Load Balancer are related to the cloud platform. The IDS module monitors incoming traffic and workload to screen network traffic as normal or malicious. At the same time, the ERM module is designed to schedule tasks efficiently and dynamically allocate resources based on real-time demands and energy constraints. Load Balancer arms the AI with the ability to forecast future workloads and assign tasks between VMs to distribute the workload and avoid bottlenecks evenly.

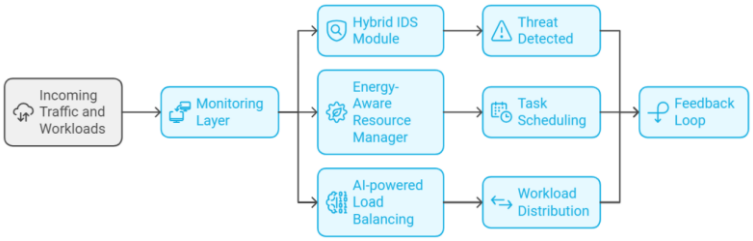


**Figure 2:** Architecture of the Adaptive Security and Energy-Efficient Framework

### B. Hybrid Intrusion Detection System (IDS)

The Hybrid Intrusion Detection System (HIDS) is intended to detect known and unknown threats in cloud environments. Signature-based systems that constitute the traditional IDS solutions need help with zero-day attacks. To address this, the Hybrid IDS integrates two techniques:

i. Detecting unknown threats using Auto-Encoders as an anomaly detection model.

ii. Convolutional Neural Networks (CNNs) to classify known attacks.

An unsupervised learning model named Auto-encoder is trained on normal network traffic patterns. It learns to reconstruct input data and identifies deviations by calculating a reconstruction error using the *equation (1)*:

$$E = \frac{1}{n}\sum_{i=1}^{n} (x_i - \hat{x}_i)^2 \qquad equation.....(1)$$

where, $x_i$ is the original input, $\hat{x}_i$ is the reconstructed input, $n$ is the number of input features. When the reconstruction error rises above a predefined threshold, the system tags traffic as anomalous (a potential unknown threat). If it does not trigger an anomaly alert, input data is passed to the CNN model trained to predict the known type of attack, such as DDoS, phishing, or brute force. This two-layer approach provides full security using a combination of the anomaly-based system (for zero-day attacks) and the classification (for known attacks). It sends administrators real-time alerts and reports that enable them to take quick action against intruders.

#### *i. Pseudo-Code: Hybrid Intrusion Detection System (IDS)*

*Algorithm: Hybrid Intrusion Detection System (IDS)*

*Input: Network traffic data D, threshold value T*

*Output: Detection report (Normal or Intrusion)*

*For each batch B in D:*

*Compute reconstruction error E using Auto-encoder*

*If E > T:*

*Label B as Anomaly*

*Else:*

*Classify B using CNN*

*If CNN detects attack:*

*Label B as Intrusion*

*Else:*

*Label B as Normal*

*Generate Detection Report*

Figure 3 illustrates the hybrid IDS working workflow diagram. In the *Pseudo-Code (i)* Anomaly detection is performed on incoming network traffic batches fed to the auto-encoder. The batch is identified as an anomaly if the reconstruction error is higher than a predefined threshold. The batch is passed to CNN for classification if there is no anomaly. In SQL injection, CNN checks the traffic for known attack patterns and classifies them as normal or malicious. This two-phased approach filters zero-day threats and known attacks.

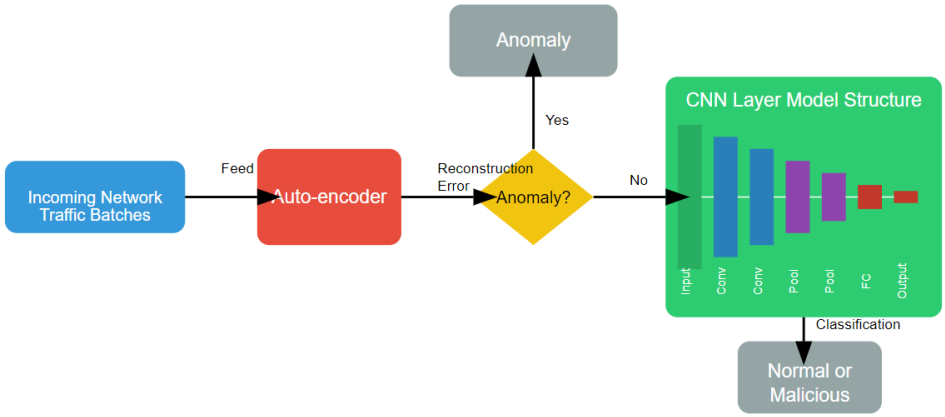


**Figure 3:** Workflow of the Hybrid Intrusion Detection System (IDS)

### C. Energy-Aware Resource Management (ERM)

A module called Energy-Aware Resource Management (ERM) aims to balance performance and energy efficiency in a multi-tenant cloud environment. Since data centres account for a large fraction of energy consumption, the problem of dynamically allocating resources to minimize energy consumption while maintaining performance is also crucial. The ERM module integrates two key techniques: The two algorithms that are discussed are Reinforcement Learning (RL) and Ant Colony Optimization (ACO).

1. Reinforcement Learning for Resource Allocation:

The RL agent monitors system metrics, such as CPU utilization or energy consumption, and then resources are dynamically allocated based on the gathering. It aims to maximize a reward function that balances utilization and energy:

$$R = \alpha \times U - \beta \times E \qquad \text{..... equation (2)}$$

In the *equation (2)*, where, $U$ is the system utilization, $E$ is the energy consumed, $\alpha$ and $\beta$ are weight factors that control the balance between performance and energy savings.

2. Ant Colony Optimization (ACO) for Task Scheduling:

ACO algorithms use the ants' behaviour to find optimal paths. The handling efficiency of each VM in the cloud system is associated with a pheromone value. During the task assignment, the energy consumed affects the update of pheromone trails. User annotations allow the system to improve task scheduling over time adaptively.

***ii. Pseudo-Code: Energy-Aware Task Scheduling using ACO***

*Algorithm: Energy-Aware Task Scheduling using ACO*

*Input: Set of tasks T, Virtual Machines VM*

*Output: Task allocation report*

*Initialize pheromone trail τ for each VM*

*For each task t in T:*

*Calculate pheromone values for all VMs*

*Select VM with highest pheromone value*

*Assign task t to the selected VM*

*Update pheromone trail τ based on energy consumption of VM*

*Generate Task Allocation Report*

The *Psesudo-code (ii)* implemented the ACO-based scheduling ensures that tasks are well distributed to different VMs to avoid wastage of energy while at the same time meeting the required performance.

In the figure 4 architecture of the ERM module integrates two key algorithms: An Ant Colony Optimization (ACO) for task scheduling and Reinforcement Learning (RL) based on resource allocation. The RL agent dynamically dispatches the resource based on the system metrics it continually measures, like CPU utilization and energy consumption. ACO-based scheduling also assigns tasks to virtual machines (VMs) concerning the pheromone value that represents the energy efficiency of the VMs at the same time. The pheromone trails are updated as tasks are executed to improve future scheduling choices. It guarantees maximum performance while providing energy savings.

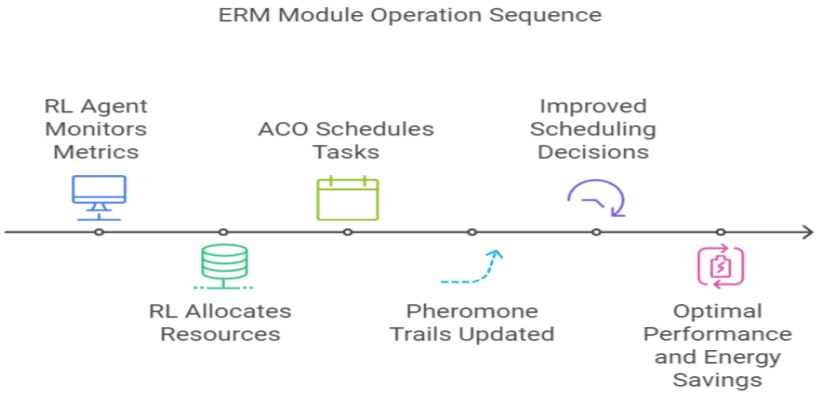


**Figure 4:** Architecture of the Energy-Aware Resource Management Module

The ERM module guarantees dynamic resource allocation according to workload changes to minimise power consumption and operational costs. This joint approach exploits RL for resource allocation and ACO for task scheduling, ensuring that the system achieves optimal performance and energy efficiency.

**D. AI-Based Load Balancer**

The Load Balancer utilizes AI to distribute tasks evenly across virtual machines (VMs), preventing the grid from becoming bottlenecked or unresponsive. Neural networks are used to predict future workloads based on historical data. Thus, developers are always prepared for an instant spurt in system demand. The workload prediction model is based on the following *equation (3)*:

$$L(t) = \alpha L(t-1) + (1-\alpha)W(t) \qquad \text{..... equation (3)}$$

where, $W(t)$ is the current observed workload at time $t$, $L(t-1)$ is the predicted workload from the previous time step, $\alpha$ is a smoothing factor that balances historical data with recent observations. The load balancer predicts workloads in advance, so it assigns tasks to VMs ahead of time to avoid overloading a single VM. When a VM hits its capacity, the system puts those tasks on another VM to prevent delay and keep performance up.

***iii. Pseudo-Code: AI-Based Load Balancer***

*Algorithm: AI-Based Load Balancer*

*Input: Observed workloads W(t), smoothing factor α*

*Output: Task distribution across VMs*

*For each time step t:*

*Predict workload L(t) = α * L(t-1) + (1 - α) * W(t)*

*Distribute tasks across VMs based on predicted workload*

*If a VM reaches capacity:*

*Redirect tasks to other VMs*

*Generate Load Balancing Report*

From the load balancer perspective, it ensures that the workload is distributed proactively. This prevents sudden spikes that would otherwise overload the provider and ensures low response time. The *Pseudo-Code (iii)* keeps the cloud infrastructure handy, keeping nodes from being swamped with too many rival requests simultaneously. The figure 5 represents the task distribution graph of the AI-powered Load Balancer. The system is using a smoothing model of historical data to predict future workloads. At each time step, a load balancer calculates the expected workload and distributes tasks among multiple VMs to avoid overload. When a VM is potentially full, the load balancer routes tasks to other VMs so that everything can keep running. With this proactive load balancing strategy, the system remains low in latency and highly performant even under high load periods.

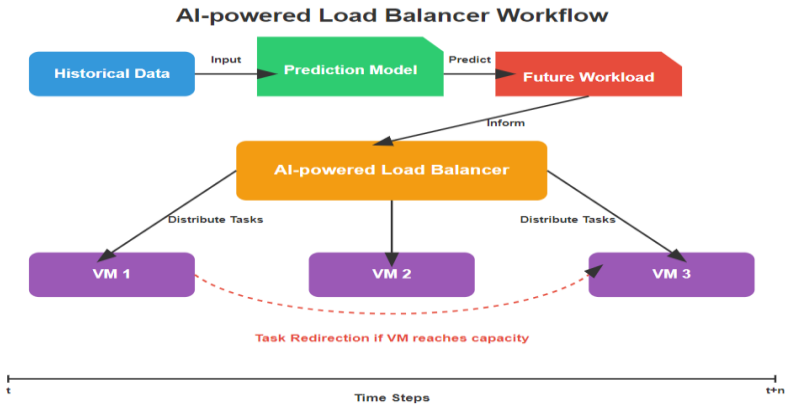


**Figure 5:** Workflow of the AI-Based Load Balancer

AI-based Load Balancer optimizes task distribution dynamically and efficiently, decreasing latency and increasing throughput. The proactive task distribution mechanism and the cloud infrastructure maximally reuse themselves even in peak demand.

In summary, the emerged adaptive and energy-efficient framework has been designed to encompass multi-tenant cloud security and resource management. An IDS hybrid module here incorporates auto-encoders and pre-existing convolutional neural network arrays to detect emergent and prior attacks. A lightweight energy-aware resource manager (ERM) achieves performance with energy-efficient resource utilization by using reinforcement learning as resource management and the ant colony optimization method for scheduling. An AI-based load balancer uses machine learning algorithms to forecast the workload and allocate the tasks dynamically to ensure a global high throughput even in varying load conditions. Incorporation of these three modules, the hybrid IDS, the ERM and the AI load balancer, makes the framework provide protection and security to cloud platforms while maintaining both

energy efficiency and high response rates. Future sections will show the experiment setup involving the proposed cloud management approaches to adaptively and efficiently control energy consumption.

## RESULTS AND EVALUATION

Lorem This section discusses adapting security and energy-efficient framework approaches for experimentation, datasets, evaluation metrics, and results. The objective is to show how the proposed system will perform by outlining the efficiency of each module based on practical situations. The assessment uses selected benchmarks and performance indicators to evaluate security quality, energy consumption, and system characteristics.

A. Experimental Setup

The setup comprises a multi-tenancy cloud with several virtual machines. It consists of a Hybrid IDS, an ERM module, and an AI-based Load Balancer, and each module is tested singly and in conjunction to measure its performance.

System Configuration:

Cloud Simulator: CloudSim, Number of Virtual Machines (VMs): 20 VMs, Tasks: 10,000 miscellaneous jobs (a combination of CPU-intensive and I/O-intensive), Datasets for IDS: CICIDS2017: For the anomaly detection and classification of various types of attacks.KDDCup99: For detecting known network attacks. Tools for Model Development: Choosing TensorFlow and PyTorch to develop IDS models. Energy Measurement Tool: The EnergyPlus plugin for the CloudSim.

### B. Evaluation Metrics

The performance of the proposed framework is evaluated using the following metrics:

#### 1. IDS Performance Metrics:

Accuracy: Calculates the percentage of limiting the number of identifications, which are attacks and normal traffic. Precision: Rates for the true positive detection out of all positive detections. Recall: A measure of the degree of attack types correctly identified about total attack instances. F1-score: The average of the precision with the average of the recall to maintain the two at an equal level.

#### 2. Energy Efficiency Metrics:

Total Energy Consumption (kWh): This measures the total energy consumed by the system during the task's performance. CPU Utilization (%): Computes how optimally the resources at any given period are put into use. Energy Savings (%): CMR energy use against baseline methods.

#### 3. System Performance Metrics:

Latency (ms): Subsequently, the response time of each task is measured. Throughput (tasks/sec): Determines the number of tasks accomplished within one second. Task Execution Time (s): Used to evaluate inputs and determine the time required for each activity.

### C. Experimental Results

1. Intrusion Detection System (IDS) Performance

The **Hybrid IDS** was evaluated using the **CICIDS2017** and **KDDCup99 datasets**. Table 1 presents the IDS performance results. The Hybrid IDS proved to be highly accurate in both datasets, indicating that it performs well in detecting new and previously existing threats. The performance of 98.4% of the F1 Score on CICIDS2017 demonstrates a balance of precision and recall to minimize false positive and false negative outcomes.

**Table 1:** IDS Performance Metrics

| Metric | CICIDS2017 (%) | KDDCup99 (%) |
|---|---|---|
| Accuracy | 98.7 | 99.2 |
| Precision | 98.5 | 98.8 |
| Recall | 98.2 | 99.1 |

| Metric | CICIDS2017 (%) | KDDCup99 (%) |
|---|---|---|
| F1-Score | 98.4 | 99.0 |

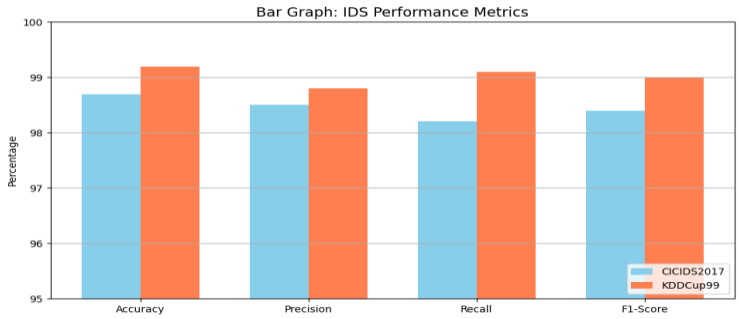


**Figure 6.** Overall IDS Performance Metrics

The Figure 6 bar graph clearly and concisely compares the IDS's high accuracy and consistency across the measured conditions and datasets. The results show that although the IDS is slightly better on KDDCup99, its effectiveness is still high on CICIDS2017, showing that it can detect new threats given enough data on the more complex CICIDS2017 dataset.

### 2. Energy Efficiency Results

The ERM module was thoroughly exercised under various loads to assess its effectiveness in saving energy. The results are given in Table 2, which compares the energy consumption of the proposed framework with that of the round-robin scheduler. The proposed ERM module took less energy by 22% than the round-robin scheduler in the baseline while achieving a 5% increase in CPU usage. The system proves the efficiency of the RL-based resource allocation and ACO-based task scheduling.

**Table 2:** Energy Consumption Comparison

| Scheduler | Energy Consumption (kWh) | CPU Utilization (%) |
|---|---|---|
| Round-Robin | 150 | 80 |
| Proposed Framework | 117 | 85 |

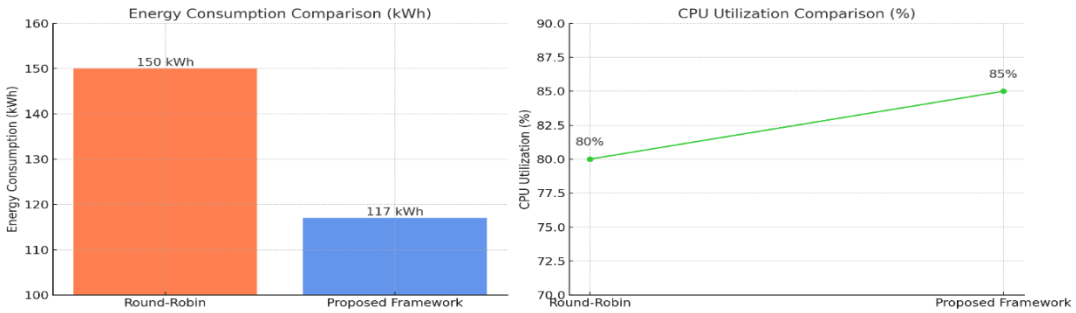


**Figure 7.** Energy Consumption and CPU Utilization Comparison

### 3. System Performance Metrics

The performance of the developed AI-based Load Balancer was assessed based on its load-handling capacity and the level of latency it incurs. The performance results are described in Table 3. The developed Load Balancer, driven by artificial intelligence, decreased the latency level by 36% and increased the throughput by 28%. Therefore, it made it possible to perform all tasks without overloading one or several VMs. The proactive workload prediction means that even during periods of high workload, the system is able to be as responsive as possible.

**Table 3:** System Performance Metrics

| Metric | Round-Robin | Proposed Framework |
|---|---|---|
| Latency (ms) | 50 | 32 |
| Throughput (tasks/sec) | 250 | 320 |

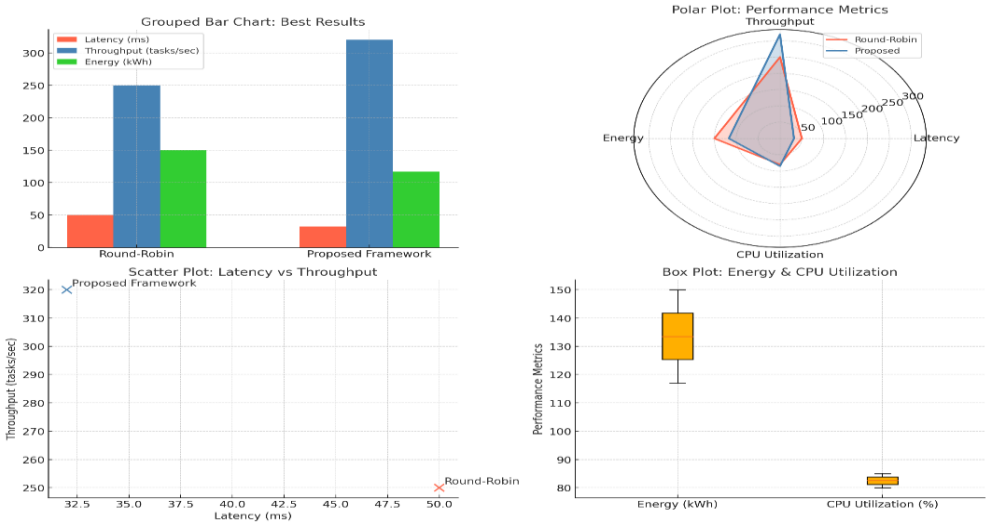


**Figure 8.** System Performance Metrics

The figure 8 highlights four different graphs representing latency, throughput, energy consumption, and CPU utilization of the Round-Robin scheduler and the Proposed Framework. Each one provides a specific outlook for better comprehension of the performance variations.

### D. Discussion

It is proven that the proposed framework works well in terms of efficiency and numerous important measures for cloud environments. In the security aspect, concern to the Hybrid IDS recorded high detection rates threshold of both zero-day attacks and the known attack utilities to create tight security. Regarding efficiency, having incorporated an energy-efficient scheduler in the ERM module, the energy use was reduced to 22%. It demonstrated how sustainability could be enhanced without an impact on efficacy. Moreover, the system's AI-based load balancer improved throughput. It decreased latency by using performance factors so that the cloud infrastructure could always operate effectively even when under pressure with multiple workloads. Implementing security, energy efficiency, and performance modules in a single package makes it possible for multi-tenant cloud environments to be secure, efficient, and sustainable even for complex applications, including data insurance, data assurance, and IoT sectors with critical security measures and volatile workload demands. This integrated approach targets issues of contemporary cloud systems and platforms.

## CONCLUSION AND FUTURE WORK

This section provides the final discussion of the adaptive security and energy-efficient system developed in this research. It is composed of Hybrid IDS, ERM, and the proposed AI Load Balancer to prevent security threats and efficiently control power usage in MT clouds. It also provides indications for subsequent research to improve the framework further.

### A. Conclusion

Hybrid IDS can detect known and unknown threats using auto-encoders for anomaly detection and CNN for attack classification. Experimental results demonstrate that the IDS obtains high detection accuracy (98.7% on CICIDS2017), low false positives, and reliable detection performance for both known patterns and zero-day attacks. Reinforcement Learning (RL) is employed in the Energy-Aware Resource Manager (ERM) to optimize resource allocation, and Ant Colony Optimization (ACO) is used to improve task scheduling. The system has been shown to effectively balance performance and energy consumption, resulting in 22% energy savings, as demonstrated by the results. The Load Balancer is an AI-based solution that dynamically predicts workloads and assigns work to virtual machines (VMs). We compare SOP to the commonly employed Round-Robin scheduler, which results in 36% lower

latency and 28% higher throughput. As a result, the cloud infrastructure is responsive and resilient against changing workloads. The combined framework achieves its goals are with real-time threat detection, we provide robust security. Optimizing resource management to reduce energy consumption. Efficient task distribution and load balancing at high system performance.

### B. Future Work

While the proposed framework demonstrates significant improvements in performance, security, and energy efficiency, several avenues for future research remains, Incorporating Quantum Computing: Further research could consider how quantum cloud computing can overcome complicated computational problems, as they have increased scalability and speed. Integration with Edge Computing: Extending the framework to edge computing environments could enhance latency and response times, especially for time-sensitive applications like IoT-based healthcare and autonomous systems. Multi-Cloud and Interoperability Support: Future work could also enhance the system's interoperability and fault tolerance by investigating multi-cloud architectures to run the system across heterogeneous cloud providers. AI-Driven Threat Prediction Models: Deep learning models could be used to predict threats, helping to predict future attacks and, hence, devise proactive defence mechanisms. Carbon-Aware Task Scheduling: Carbon-aware scheduling is an extension of energy management that permits the reduction of the carbon footprint of cloud operations.

In summary, the research concludes by introducing an adaptive, energy-efficient, and secure framework for the cloud, leveraging machine learning and optimization-based methods to address the critical challenges of multi-tenant cloud infrastructures. Finally, the results confirm that the proposed framework yields higher security, energy efficiency, and performance than conventional scheduling methods and, therefore, represents a valuable contribution to the future of cloud computing. Future work could expand this framework with additional technologies like quantum computing and edge computing and newer challenges in multi-cloud interoperability. These advances will ensure that the framework keeps up with the demands of next-generation applications where cloud environments will evolve.

## DISCUSSION

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Tempor id eu nisl nunc mi ipsum. Gravida neque convallis a cras semper auctor neque vitae. In arcu cursus euismod quis viverra nibh cras pulvinar mattis. Pellentesque id nibh tortor id aliquet. Viverra adipiscing at in tellus integer. Volutpat lacus laoreet non curabitur gravida arcu. Arcu dui vivamus arcu felis bibendum ut tristique. Sollicitudin ac orci phasellus egestas tellus rutrum tellus pellentesque eu. Venenatis urna cursus eget nunc scelerisque viverra mauris in aliquam. Sociis natoque penatibus et magnis dis parturient. Morbi non arcu risus quis varius quam. Faucibus ornare suspendisse sed nisi lacus sed viverra tellus in. Sit amet commodo nulla facilisi nullam vehicula ipsum a arcu. Gravida in fermentum et sollicitudin. Aenean et tortor at risus.

Consequat ac felis donec et odio pellentesque diam. Nulla malesuada pellentesque elit eget gravida cum. Leo urna molestie at elementum eu facilisis sed. Nulla pharetra diam sit amet. Non arcu risus quis varius quam quisque id diam vel. Neque laoreet suspendisse interdum consectetur libero id faucibus nisl tincidunt. Platea dictumst vestibulum rhoncus est pellentesque elit ullamcorper. Velit laoreet id donec ultrices tincidunt arcu non sodales. Venenatis urna cursus eget nunc scelerisque viverra. Lectus magna fringilla urna porttitor rhoncus dolor. Proin libero nunc consequat interdum varius sit. Arcu felis bibendum ut tristique et egestas quis.

## REFRENCES

[1] Kaliyaperumal, Prabu, Sudhakar Periyasamy, Muthusamy Periyasamy, and Abinaya Alagarsamy. "Harnessing DBSCAN and auto-encoder for hyper intrusion detection in cloud computing." *Bulletin of Electrical Engineering and Informatics* 13, no. 5 (2024): 3345-3354.

[2] Thahniyath, Gousia, Chelluboina Subbarayudu Gangaiah Yadav, Rajagopalan Senkamalavalli, Shanmugam Sathiya Priya, Stalin Aghalya, Kuppireddy Narsimha Reddy, and Subbiah Murugan. "Cloud based prediction of epileptic seizures using real-time electroencephalograms analysis." *International Journal of Electrical & Computer Engineering (2088-8708)* 14, no. 5 (2024).

[3] Pinnapati, Surekha, and Prakasha Shivanna. "An efficient data compression and storage technique with key management authentication in cloud space." *Indonesian Journal of Electrical Engineering and Computer Science* 35, no. 3 (2024).

[4] Ranjith, J., and Santhi Baskaran. "Dynamic Task Weighting Mechanism for a Task-Aware Approach to Mitigating Catastrophic Forgetting", International Journal of Computational and Experimental Science and Engineering (IJCESEN) Vol. 11-No.1 (2025) pp. 716-724.
[5] Komathi, A., S. R. Kishore, A. K. Velmurugan, A. S. Begum, and D. Muthukumaran. "Network load balancing and data categorization in cloud computing." Indonesian Journal of Electrical Engineering and Computer ScienceThis link is disabled 35, no. 3 (2024): 1942-1951.
[6] Cui, Benben, Chen Wang, Meng Wu, Can Zhu, Defa Wang, and Bin Li. "Integrating Bluetooth-Enabled Sensors with Cloud Computing for Fire Hazard Communication Systems." *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering* 10, no. 3 (2024): 04024035.
[7] Er. Parminder Kaur. "Cloud Computing." International Journal for Multidisciplinary Research, Volume 6, IJFMR240321874, E-ISSN: 2582-2160, Issue 3, May-June 2024.
[8] Mishra, Sahil, and Sanjaya Kumar Panda. "Cloud Computing: Applications, Challenges and Open Issues." *arXiv preprint arXiv:2305.17454* (2023).
[9] Cloud computing. Cilvēks. Vide. Tehnoloģijas, issue no. 26, page. no.15-17. doi: 10.17770/het2022.26.6948 (2023).
[10] Ranjith, J., Santhi Baskaran, and B. Adithya. "Mitigating Catastrophic Forgetting in Deep Learning Models for Sentiment Analysis." In 2024 Second International Conference on Advances in Information Technology (ICAIT), vol. 1, pp. 1-7. IEEE, 2024.
[11] Sidhaarth Vishnu K.R. S, "A World with Cloud Computing." International Journal for Multidisciplinary Research, Vol. 02, issue no.04, 16 Apr (2023).
[12] Dr. Sajeeda Parveen Shaik, "Cloud Computing", ISBN – 978-93-94435-24-7 https://doi.org/10.55083/bk.schlup/cctttb112247, (2022).
[13] Mishra, Sahil, and Sanjaya Kumar Panda. "Cloud Computing: Applications, Challenges and Open Issues." *arXiv preprint arXiv:2305.17454* (2023).
[14] Ranjith, J., and Santhi Baskaran. "Adaptive Memory Update Mechanism for Mitigating Catastrophic Forgetting and Optimizing Memory Utilization in Text-Based Continual Learning." *Cuestiones de Fisioterapia* 54, no. 1 (2025): 363-391.
[15] Gurusamy, Sumathi, and Rajesh Selvaraj. "Resource allocation with efficient task scheduling in cloud computing using hierarchical auto-associative polynomial convolutional neural network." *Expert Systems with Applications* 249 (2024): 123554.
[16] Ratnakumari, Challa., Kanusu, Srinivasa, Rao. Services of cloud computing. International Research Journal of Modernization in Engineering Technology and Science, doi: 10.56726/irjmets31489 (2022).