SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I5P111

Volume 13 Issue 5, 109-128, May 2026

Original Article

An Integrated Secure and Energy-Efficient Cloud Architecture using Resource Consolidation and Machine Learning-Based Optimization

Sachin H. Patel[1], Amit Nayak[2]

[1]*Department of Computer Engineering, Chandubhai S. Patel Institute of Technology (CSPIT), Faculty of Technology & Engineering, Charotar University of Science and Technology (CHARUSAT), Gujarat, India.*
[2]*Department of Computer Science and Engineering, Devang Patel Institute of Advanced Technology and Research (DEPSTAR), Faculty of Technology & Engineering, Charotar University of Science and Technology (CHARUSAT), Gujarat, India.*

[1]*Corresponding Author : Sachinpatel.it@gmail.com*

Received: 09 February 2026 Revised: 11 March 2026 Accepted: 12 April 2026 Published: 27 May 2026

Abstract *- The rapid adoption of cloud computing has significantly increased data center energy consumption but has also heightened the risk of data integrity in the multi-tenant setup. Current alternatives usually cover the issues of energy efficiency and security separately, which results in a non-optimal compromise of sustainability and integrity maintenance. The paper proposes an Integrated Energy Integrity Cloud Optimization Framework, which will reduce the energy usage and the risk of data distortion simultaneously with a single multi-objective optimization framework. The model integrates integrity-conscious virtual machine aggregation, machine learning workload forecasting, and dynamic auto-scaling in a cloud-native AWS setup. The formal mathematical formulation integrates energy minimization with integrity risk constraints while ensuring SLA compliance. The system is deployed with the help of Amazon EC2, Auto Scaling, Lambda, Cognito, SageMaker, and CloudWatch services, and tested on the publicly available dataset of Google Cluster Workload Trace with a known control of the integrity events simulation. The experimental results show a 20%–25% reduction in energy consumption. Comparative analysis proves that the suggested framework is more efficient than energy-only and security-only frameworks, as it is possible to optimize sustainability and data integrity at the same time with the help of predictive and risk-aware resource management.*

Keywords *- Energy-Efficient Cloud Computing, Data Integrity, Virtual Machine Consolidation, Machine Learning-Based Scaling, Multi-Objective Optimization, Green Cloud Architecture, AWS Cloud Implementation, Sustainable Data Centers.*

1. Introduction

1.1. Background of Cloud Computing

Cloud computing has become the dominant paradigm for delivering computing services over the Internet, providing on-demand access to configurable resources such as compute instances, storage systems, networking infrastructure, and software platforms. It provides scalability, elasticity, and cost efficacy to organizations in different fields such as healthcare, finance, education, manufacturing, and government systems. The services are usually provided under Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models. The key reason that has led to a fast adaptation of cloud platforms is their dynamic nature, as they are able to dynamically allocate resources based on the demand of the workload, thus reducing capital costs and enhancing agility in operations [3, 31]. The current cloud data centers have thousands of Physical Machines (PMs) that contain various Virtual Machines (VMs) or containers.

Multi-tenancy is facilitated by the virtualization technologies, with multiple users being allowed to use the same physical infrastructure, which enhances the use of hardware and helps in consolidating the workloads dynamically [1, 19]. The openness, distributed, and highly dynamic quality of cloud environments, however, poses serious challenges in terms of energy efficiency, security, and the management of data integrity [10, 11]. Scaling in size and complexity, due to the use of cloud infrastructures, has become a hot research topic towards attaining sustainable and secure operation [12, 21].

1.2. Workload of Cloud Data Centers

The high rate of development of cloud services has also led to an increase in the number and size of data centers all over the world. These amenities use large quantities of electricity to power servers, networked devices, and cooling systems. Research shows that data centers are one of the

largest energy consumers in the world, and the number is likely to grow as new technologies emerge that include Artificial Intelligence, Internet of Things (IoT), Big Data Analytics, and Edge Computing [14, 20]. Several factors, such as the degree of utilization of servers, patterns in the distribution of workload, virtualization overhead, and efficiency of cooling, determine the energy used in cloud environments [2, 25]. The idle power that servers consume is high even in conditions of low workload, thus resulting in wastage of energy when resources are not fully utilized.

Other problems like the virtual machine sprawl, ineffective provisioning of resource schedules, and task scheduling all contribute to energy wastage [18, 23]. This has prompted more and more research on the development of energy-efficient resource management techniques, including the dynamic VM consolidation, workload-sensitive scheduling, and predictive auto-scaling techniques [4 - 6].

These methods are intended to maximize the use of resources and reduce the amount of energy used. Lack of energy efficiency not only leads to the high cost of operations by the cloud service providers but also adds to the carbon emissions and environmental impact. Thus, sustainable cloud computing requires that the energy-conscious optimization strategies be incorporated so as to ensure that the performance is not compromised, as well as safeguard the service level agreements (SLAs) [8, 27, 33].

1.3. Data Integrity Challenges in Cloud Environments

Even though energy efficiency is an issue of great concern, cloud computing environments are still highly challenged concerning data integrity and security. Data integrity is defined as the guarantee that data is correct, consistent, and unchanged in the lifecycle or storage, processing, transmission, and migration stages [7, 9]. On the cloud, data is often copied, transferred, and shared between a large number of tenants, which leads to a significantly higher likelihood of accidental corruption or other forms of malicious interference [29, 38].

Several factors contribute to integrity risks in cloud infrastructures:

- Multi-tenancy and shared infrastructure expose systems to insider threats and cross-tenant attacks [37, 38].
- Vulnerabilities during live Virtual Machine (VM) migration, where data transfer processes may introduce security weaknesses [28, 36].
- Improperly secured APIs and management interfaces, increasing exposure to unauthorized access [11].
- Misconfigured access control mechanisms, leading to privilege escalation or data leakage [34].
- Log tampering and incomplete audit trails weaken forensic traceability and accountability [10, 35].

Integrity verification mechanisms, including cryptographic hashing, encryption, remote attestation, and auditing, introduce additional computational overhead [29, 30]. While they enhance security, they can increase processing latency and power consumption. Therefore, cloud computing often faces the challenge of maintaining high integrity, as it aims to provide an energy-efficient solution [18, 27].

1.4. Necessity of Integrated Energy and Integrity Optimization

Current literature views energy efficiency and data integrity as different research fields to a large extent. The strategies of energy-aware scheduling and VM consolidation are mainly concerned with the reduction of power use, and the maximization of server use without a conscious consideration of security overhead and integrity threats [1, 19, 25]. On the other hand, integrity-preserving solutions focus on encryption, authentication, anomaly detection methods, and secure migration methods and do not always take into consideration the effects they have on resource use and energy consumption [28, 36, 37]. Systemic inefficiencies may arise out of this separation. To use an example, a vigorous VM consolidation may lead to the saving of energy but may cause additional overloading risks and reduce the speed of integrity verification and undermine the security guarantees [23, 26]. Similarly, the checking and verifying of integrity should be performed on a regular basis, which may consume excessive computational power, and this increases the total energy consumption and operation costs [29, 30].

It follows that there is a need to have in place a single framework that is able to take care of energy optimization and data integrity simultaneously. This type of structure has to strike a balance between various goals, which include:

- Minimizing energy consumption
- Maintaining strong data integrity protection
- Preserving Service Level Agreement (SLA) compliance

The incorporation of Machine Learning (ML) for predictive workload management further enhances adaptability under dynamic cloud conditions [31, 32]. The basis of the research consists of combining green computing concepts with a secure cloud architecture that can allow sustainable, secure, and scalable cloud-based operations via integrity-aware resource consolidation [20, 21].

1.5. Problem Statement

Although there are major improvements in the area of green cloud computing and secure cloud architectures, no one has yet developed an integrated model that would achieve both data integrity and energy savings in acute cloud computing systems. The current solutions tend to prioritize either reduction in the number of resources via aggressive resource consolidation [1, 24] or the enhancement of security based on cryptography and monitoring tools [28, 37] without sufficiently addressing the interrelation between them.

This means cloud systems might pay an extravagant overhead of energy in their bid to maintain integrity or be exposed to security risks in their bid to adopt aggressive energy-saving measures. This is where the gap arises, as there is a need to have an integrated cloud architecture that can do:

- Reducing energy consumption through intelligent consolidation
- Ensuring data integrity using lightweight validation mechanisms
- Leveraging predictive anomaly detection
- Maintaining performance and SLA compliance.

Despite extensive research in energy-efficient cloud computing and secure cloud architectures, existing solutions fail to jointly optimize energy consumption and data integrity within a unified framework. Most approaches treat these objectives independently, leading to suboptimal trade-offs. This highlights a critical research gap in designing an integrated, multi-objective optimization framework that simultaneously addresses sustainability, security, and SLA compliance."

1.6. Proposed Solution Overview

To address this research gap, this paper proposes an integrated secure and energy-efficient cloud architecture that combines:

- Integrity-aware resource consolidation [19, 28]
- Machine learning-based predictive scaling [31, 32]
- Dynamic VM placement optimization [18, 24]
- Real-time monitoring and validation mechanisms [29, 36]

The suggested architecture is based on the principles of cloud-native design that would guarantee a high level of scalability and the feasibility of practical deployment. It presents a lightweight multi-objective optimization model that deals with a balance of energy consumption, integrity risk, and performance constraints at the same time.

Incorporating the assessment of the integrity risk as a direct part of the resource distribution process, the framework manages to uphold a sustainable cloud operation without the need to compromise the security levels or even the adherence to the SLA.

In this case, Figure 1 illustrates the proposed Integrated Energy Integrity Cloud Optimization Framework that will present a layered and closed-loop architecture that will optimize the collaborative data integrity as well as energy efficiency in a cloud computing environment. The architecture begins with user service requests, which are processed through authentication and access control mechanisms.

The authentication and Access Control layer verifies the identity and develops an access policy providing access to the system. The Data Integrity and Security layer then verifies the requests and encrypts, verifies their integrity, logs, and detects anomalies to maintain the correctness and integrity of data at all steps in its lifecycle.

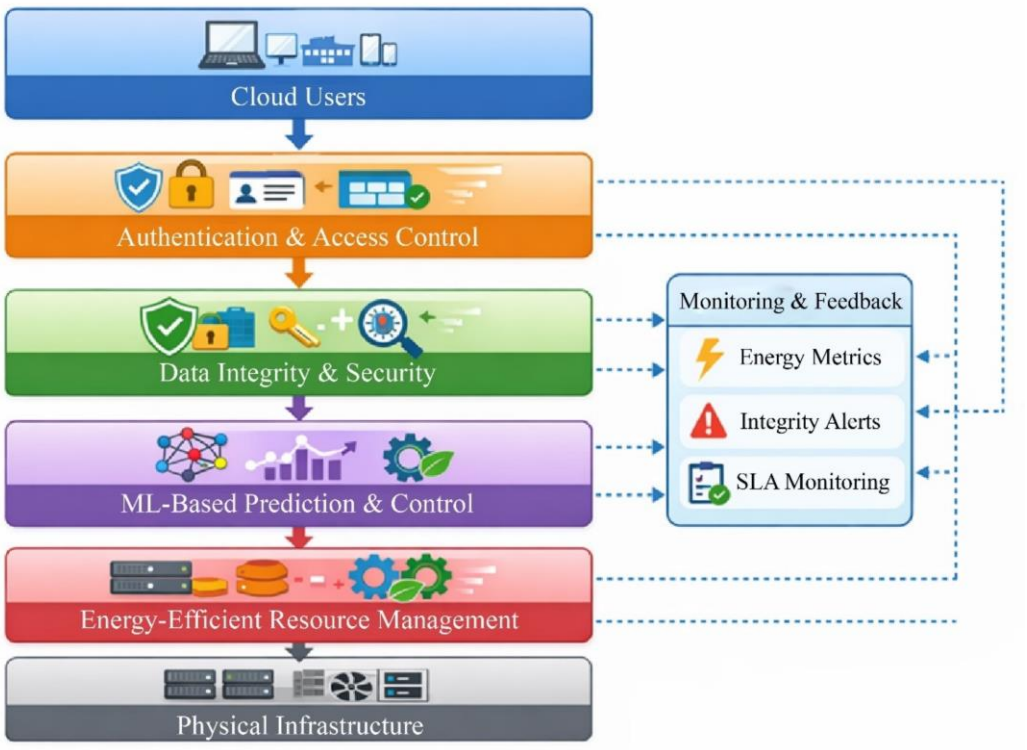

Fig. 1 Integrated Energy–Integrity Cloud Optimization Framework

The architecture is also enhanced with a Machine Learning-Based Prediction and Control layer that predicts workload patterns, predicts integrity risks, and makes estimates of resource demand by which proactive and intelligent decisions can be made. According to these predictions, the Energy-Efficient Resource Management layer implements optimized load balancing, auto-scaling, and virtual machine consolidation policies and ensures that the SLA is not violated and that needless energy utilization is reduced.

Such decisions eventually impact the layer of Physical Infrastructure controlled by servers, storage systems, networking elements, and power units, where real energy is utilized. It has a constant Monitoring and Feedback system that traverses all the layers and collects the energy measurements, integrity warnings, and performance data and injects this into the predictive control system to such an extent that real-time adaptive optimization can be attained.

The layers are vertical, and the feedback loop is horizontal, resulting in only one smart and sustainable cloud architecture that balances the confidence of security and energy efficiency in a coordinated system.

1.7. Research Contributions

This paper makes the following contributions:

- An Integrated Secure and Energy-Efficient Cloud Architecture: A single framework that tackles both data integrity assurance and energy-efficient management of the resources in the cloud environments together [28, 36].
- A Lightweight Integrity-Aware Resource Consolidation Algorithm: A multi-objective optimization model, which works to reduce energy usage and ensure an integrity risk at or below specified limits [13, 28].
- Machine Learning-Based Predictive Resource Scaling: A predictive workload estimation system that allows making scaling decisions in advance and minimizing the needless use and activation of resources, as well as enhancing energy efficiency [16, 32].
- Experimental Validation Using AWS Cloud Services: An application and testing on actual cloud infrastructure, with real results of energy-saving and integrity maintenance [23, 26].
- Comparative Analysis with Existing Green Cloud Approaches: A systematic comparison against traditional energy-aware scheduling and security-focused mechanisms, highlighting the advantages of integrated optimization [1, 19, 25].
- Unlike existing approaches, the proposed framework uniquely integrates integrity-aware risk modeling into energy-efficient VM consolidation, enabling simultaneous optimization of sustainability and security within a single predictive control architecture.

1.8. Key Challenges Addressed

Table 1 provides an overview of the major operational issues within cloud computing and the unique influence they have on energy use, data security, and the limitations of the current research. Due to overprovisioning and underutilization of the virtual machines, VM sprawl contributes to high idle energy usage, but has relatively low direct effect on the integrity of data; in most consolidation strategies, integrity considerations are not incorporated in the consolidation action plan [19, 25].

The moderate energy overhead with moderate risks to integrity associated with frequent virtual machine migration, as commonly applied to achieve load balancing and fault tolerance, has not been modeled jointly in energy security models to date, although this would be valuable since it can result in the exposure of data or transmission vulnerabilities to adversaries [37, 38].

Issues of data protection through encryption and validation can be very strong, but they are accompanied by high rates of CPU usage and computing load, and most research does not focus on the energy cost. Providing resources in a static way leads to high energy waste through over-provisioning, and has little direct integrity consequence, but cannot make improvements in efficiency as much because predictive scaling techniques are not available.

Lastly, multi-tenancy environments have moderate implications of energy consumption since they share resource contention but are susceptible to high integrity risks as a result of cross-tenant attacks and isolation failures; however, current security mechanisms are seldom considered with energy-awareness. In general, the table highlights that existing studies normally discuss energy efficiency or integrity separately, and therefore, there is a need to have a concerted approach where both aspects can be managed within a single framework.

Most of the existing methods, as indicated in Table 1, optimize a single dimension of the problem. This gives reason to work on a holistic approach addressing both the energy and the integrity in one. The rest of the paper is arranged in the following way. Section 2 is a literature review of recent articles on energy-efficient cloud computing, secure architectures, and machine learning-based resource management.

In Section 3, the mathematical model and optimization problem are formulated. Section 4 gives the proposed architecture and consolidation algorithm that is integrity-aware. Section 5 explains the experimental design and the assessment procedure. Section 6 is about results and comparison. Lastly, we have the conclusion to the paper, where Section 7 gives the future areas of research.

Table 1. Key challenges in cloud computing [1, 19, 24, 37]

Challenge	Impact on Energy	Impact on Integrity	Research Gap	Challenge
VM Sprawl	High idle energy [1, 24]	Low direct impact	No integrity consideration	VM Sprawl
Frequent VM Migration	Moderate [28]	Increased risk	Lack of joint modeling	Frequent VM Migration
Encryption & validation	Increased CPU usage [29, 30]	Strong protection	Energy overhead ignored	Encryption & validation
Static Resource Provisioning	High waste [2, 25]	Neutral	No predictive scaling	Static Resource Provisioning
Multi-tenancy	Moderate [24]	High risk	Security not energy-aware	Multi-tenancy

2. Related Work

The emergence of cloud computing has rapidly triggered studies in the area of security assurance, effective resource management, and intelligent optimization of workload. However, most of the research has been addressing these dimensions individually, and this has led to piecemeal solutions. The section represents a critical literature review of prior studies that have been conducted in the four related fields of security in cloud computing, energy-efficient cloud computing, machine learning-based cloud optimization, and the gap in the literature that led to the creation of the proposed integrated framework.

2.1. Security in Cloud Computing

One of the main issues related to cloud computing has been security because cloud computing involves a multi-tenant architecture, distributed infrastructure, and is accessible remotely [37, 38]. Initial studies were on the security of virtualization, isolation of tenants, as well as secure hypervisor design to avoid cross-VM interference [36, 37]. Security models based on virtualization increased the logical isolation with the help of secure virtual machine monitors and sandboxing. Nevertheless, these methods enhanced tenant isolation but failed to resolve the issues of data integrity completely as the dynamic operation, like live VM migration went on [28, 36]. A lot of research efforts have focused on the concept of secure Virtual Machine (VM) migration, especially when load balancing and fault tolerance need to be provided in the environment [28, 35, 37]. Researchers have put forward encrypted migration paths, integrity checks during migration, and state transfer secure methods to avoid the exposure of data.

Though these techniques are helpful in improving protection in the case of VM relocation, they tend to add more computation overhead to the process, which elevates processing latency and consumes resources [28, 29]. There is also a common study of encryption and cryptographic verification to provide integrity and confidentiality of data [29, 30]. The hash-based message authentication codes (HMAC), Public Key Infrastructures (PKI), and secure key management systems are some of the techniques that offer high protection against unauthorized modification [11]. Nevertheless, constant encryption, decryption, and validation create additional workloads on the CPU and have an indirect effect on the total energy efficiency [27, 29]. Recent works integrate frameworks of anomaly detection and log analysis to identify malicious and illegal access attempts [35, 38].

RNNs and advanced AI-based scheduling and detection systems are some examples of deep learning methods that have proven useful in detecting abnormal cloud behavior [31, 32]. Although such mechanisms lead to better accuracy in detection, they are not commonly incorporated in resource optimization models that take into account energy constraints [28, 36]. In general, current studies in security focus on preserving integrity, authentication, and mitigation of threats [37, 38], but seldom consider the energy potential of implementing security-related solutions to large-scale cloud solutions [27, 29].

2.2. Energy-Efficient Cloud Computing

Just like the security issues, energy-efficient cloud computing is also becoming a critical area of research as a result of the environmental and economic consequences of high-scale data centers [21, 24]. The current studies in this field are mainly aimed at minimizing the amount of power used by applying smart resource management methods. One of the strategies that has received the greatest adoption regarding the enhancement of energy efficiency is virtual machine consolidation [1, 19, 24]. Idle servers can be shut down or put in low power mode by dynamically migrating workloads and consolidating VMs onto a smaller number of physical machines at times of low demand [25]. VM consolidation optimization methods consist of heuristic algorithms, metaheuristic algorithms such as genetic algorithm and particle swarm optimization [2, 25], and reinforcement learning-based strategies [18].

Other research areas of green cloud computing include Dynamic Voltage and Frequency Scaling (DVFS), workload-aware scheduling, and energy-proportional computing [20, 25]. Several multi-objective optimization models are also offered to decrease energy consumption without violating the SLA and ensuring the efficiency of resource utilization [23, 26]. Irrespective of these innovations, the majority of energy-based solutions consider workloads without any links to security mechanisms [1, 19]. The overhead of integrity verification, encryption and security caused overhead of the computation costs are not often included in the energy optimization models [28, 29, 40]. Consequently, energy saving measures with violent implementation can unwillingly diminish security or misjudge the actual security energy footprint of security-conscious operations.

2.3. Cloud Optimization using Machine Learning

Predictive and adaptive optimization has been made possible by the integration of Machine Learning (ML) with cloud management systems [31, 32]. Workload prediction, anomaly detection, dynamical allocation of resources, and auto-scaling decisions are also being performed using ML-based techniques [23, 31]. Time-series forecasting methods that are common in predictive scaling models include Long Short-Term Memory (LSTM) networks and deep learning networks to predict changes in workloads [31, 32]. Such predictions would allow proactive provisioning of resources, minimize SLA breaches, and unwarranted resource activation [23]. Dynamic VM placement and energy-aware scheduling have also been implemented using reinforcement learning, so that systems could learn good policies of resource allocation by reacting to environmental feedback [18, 19]. These methods enhance scalability in dynamic clouds. In addition to workload prediction, ML systems can be used to detect anomalies and integrity, and monitor system logs as well as detect strange patterns of behavior [31, 35]. These predictive and detection models are, however, normally deployed as disjointed units instead of being incorporated into extensive optimization models [28, 36]. Despite the fact that ML is more flexible and predictive, there is a lack of research that can be used to jointly predict integrity risk and energy-aware decision-making using a single optimization model [1, 28]. The current literature focuses on optimizing the energy consumption with the help of ML [23, 31] or improving security with the assistance of anomaly detection [35]; however, it rarely combines these two tasks into a unified control system.

Table 2 summarizes representative prior studies across security, energy efficiency, and ML-driven optimization domains [28, 31, 37]. The proposed framework advances existing research by integrating integrity-aware validation and energy-efficient resource consolidation within a single multi-objective optimization model. By combining ML-based workload forecasting, integrity risk prediction, and dynamic scaling decisions, the framework achieves balanced trade-offs between sustainability, data integrity, and performance guarantees. This approach directly addresses the fundamental limitation of prior studies, namely, the absence of comprehensive energy-security integration policies.

Table 2. Summary of prior research in cloud optimization

Category	Representative Focus	Methods Used	Primary Objective	Limitation
Virtualization Security	VM isolation and secure hypervisors [36, 37]	Secure VMM, sandboxing	Strengthen tenant isolation	Energy impact not considered
Secure VM Migration	Encrypted state transfer [28, 35, 37]	Secure channels, integrity checks	Protect data during migration	Increased computational overhead
Encryption & Key Management	Data confidentiality and validation [29, 30]	Cryptographic hashing, PKI	Ensure data integrity	CPU-intensive, energy cost ignored
VM Consolidation	Energy reduction in data centers [1, 19, 24]	Heuristics, MILP, metaheuristics	Minimize power consumption	No security integration
Green Scheduling	SLA-aware resource allocation [23, 25]	Multi-objective optimization	Balance energy and QoS	Integrity risk is not modeled
ML-based Scaling	Workload prediction [31, 32]	LSTM, ARIMA, RL	Improve scalability and efficiency	Security-energy trade-off ignored
ML-based Anomaly Detection	Intrusion detection [31, 35]	Deep learning models	Detect malicious activities	Not linked with energy management
Proposed Integrated Energy–Integrity Framework (This Work)	Joint optimization of energy efficiency and data integrity	Multi-objective integrity-aware VM consolidation + ML-based predictive control	Simultaneously minimize energy consumption and integrity risk while maintaining SLA compliance	-

As it is observed in Table 2, the previous studies mainly focus on single-dimensional optimization goals. Security-oriented solutions emphasize integrity and protection, whereas green computing studies are aimed at reducing the use of energy. Machine learning methods are more useful in prediction and are usually used alone.

2.4. Research Gap Analysis

Critical review of literature conducted shows that the majority of cloud optimization frameworks focus on energy efficiency and data integrity separately. Security-centric solutions firm up encryption, authentication, and anomaly detection mechanisms but tend to ignore their computational and energy burdens [29, 30, 37]. On the other hand, energy-conscious scheduling and VM consolidation models are the two that make optimal use of resources without models are the two that make optimal use of resources without integrating the cost of integrity checks and security risk analysis [1, 19, 24]. Moreover, predictive models based on machine learning are often used as workload prediction models or anomaly detection models, but not as combined modules in one multi-objective optimization. Failure to model results in sub-optimal trade-offs jointly, as the energy savings can be aggressive, thus raising the risk of integrity, or the security enforcement may be robust, thus raising the energy consumption [28-30].

Thus, a model that would be a predictive closed-loop framework integrating energy consumption, integrity risk, and SLA compliance is needed. The research proposed fills this gap, uniting the integrity-conscious validation, machine learning predictive control, and energy-efficient resource consolidation into one optimization model. This integrated solution is geared towards realizing sustainable cloud computing without losing data integrity and system performance [24, 31].

Recent studies have explored AI-driven optimization techniques in cloud computing environments; however, most existing approaches focus on either energy efficiency or security independently. For instance, energy-aware VM consolidation techniques have been widely investigated to reduce power consumption in data centers [1, 2, 18]. At the same time, secure virtual machine migration and integrity-preserving mechanisms focus primarily on protecting data during transmission and processing [10, 28, 29].

Similarly, machine learning-based workload prediction models improve resource allocation efficiency but do not explicitly consider integrity risk in optimization decisions [3, 31]. Despite these advancements, very limited research integrates predictive integrity risk assessment with energy-aware resource management within a unified framework. This gap highlights the need for a comprehensive multi-objective optimization approach that simultaneously addresses energy efficiency, data integrity, and SLA compliance, which is the primary motivation of the proposed work

3. Problem Formulation

In order to define the integrated optimization of energy efficiency and data integrity in a cloud resource with strictness, this paper develops the resource management problem as a constrained multi-objective optimization model [1, 19, 24]. In contrast to the classical methods that consider one or the other of the two concepts, energy minimization or security assurance, the proposed formulation considers both aspects jointly through a single mathematical model.

Consider a cloud data center consisting of a set of physical machines $P = \{P_1, P_2, P_3, \ldots . P_M\}$hosting a set of virtual machines $V = \{V_1, V_2, V_3, \ldots . V_N\}$. Each VM requires computational resources such as CPU and memory, while each physical machine has limited capacity. The goal is to determine an optimal VM-to-PM allocation that minimizes total energy consumption while maintaining acceptable data integrity and SLA performance levels [23, 28, 37].

3.1. Energy Consumption Model

Energy consumption in cloud servers is primarily utilization-dependent. Even when idle, physical machines consume baseline power. The total energy consumption $E$of the system is modeled as:

$$E = P_{idle} + (Pidle_{max} \quad (1)$$

Where $P_{idle}^{(j)}$and $P_{max}^{(j)}$denote the idle and maximum power of the physical machine P_i, respectively, and $u_j$represents its utilization ratio. This formulation highlights the importance of VM consolidation, as reducing the number of active machines directly lowers total energy consumption [1, 24, 25].

3.2. Data Integrity Risk Model

Data integrity risk arises from factors such as VM migrations, validation failures, and detected anomalies. To quantify this, an integrity metric $I$is defined as:

$$I = \beta_1 F_m + \beta_2 V_f + \beta_3 A_d \quad (2)$$

Where denotes migration frequency, $V_f$represents integrity validation failures, $A_d$indicates anomaly detections, and $\beta_1, \beta_2, \beta_3$ are weighting coefficients reflecting their relative impact. This aggregated metric allows security risks to be explicitly incorporated into optimization decisions [28, 36, 37].

3.3. Resource Utilization

Efficient resource utilization R ensures balanced infrastructure usage and avoids both overloading and underutilization:

$$R = \frac{\sum_{i=1}^{N} Resource_{used}^{(i)}}{\sum_{j=1}^{M} Resource_{capacity}^{(i)}} \quad (3)$$

Higher utilization generally improves energy efficiency, but it must be controlled to prevent SLA violations [23, 25].

3.4. Optimization Objective

The proposed optimization objective integrates energy and integrity considerations:

$$min\, Z = E + \alpha I \quad (4)$$

where is the total system cost, and is a trade-off parameter, which determines the relative significance of integrity preservation and energy minimization. The framework can be modified to focus on sustainability or security when needed by adjusting the α as per the needs of the operations [28, 37].

The optimization is subject to the following constraints:

1. SLA Constraint:

$$C \leq C_{max} \quad (5)$$

Ensuring service performance remains within acceptable limits [23, 25].

2. Security Threshold Constraint:

$$I \leq I_{max} \quad (6)$$

Guaranteeing that integrity risk does not exceed predefined tolerance levels [28, 37].

3. Resource Capacity Constraint:

$$\sum_i x_{ij} \,.\, Re\, s\, ource_i \leq Capacity_j \forall_j \quad (7)$$

Where $x_{ij} \in \{0,1\}$indicates VM placement decisions [1, 24].

4. Final Formulation

The complete problem can therefore be expressed as:

$$min\ _{xij} Z = E + \alpha I \quad (8)$$

Subject to SLA, security, and resource availability constraints

This combined declaration develops the analytical basis of the suggested framework as it explicitly models the trade-off between sustainability and data integrity. The formulation of integrity risk in the energy minimization goal steps past the traditional single-dimensional optimization models and offers an airtight foundation to the format as a valid algorithm environment in the following section [1, 19].

4. Proposed Architecture

This section presents the proposed integrated Energy–Integrity cloud architecture. The framework is designed as a layered system that combines security, predictive intelligence, and energy-efficient resource management within a cloud environment. This architecture is based on operations, operation authentication, integrity verification, predictive intelligence, and energy-sensitive resource management within a cloud-native infrastructure. Monitoring is spying with an eye on all the privacy interstices at the uniqueness singularity level. Then, through controlled AWS services, it has achieved real scalability and variability, yet these results confirm the effectiveness and reliability of the proposed framework. These five main layers of the diagram included: (1) Authentication Layer, (2) Integrity Layer, (3) Machine Learning Prediction Layer, (4) Resource Management Layer and (5) Monitoring and Feedback Layer These layers can be interconnected within an organized closed ring in such a way that they offer support to adaptive energy enhanced optimization and security [28, 31, 32, 36].

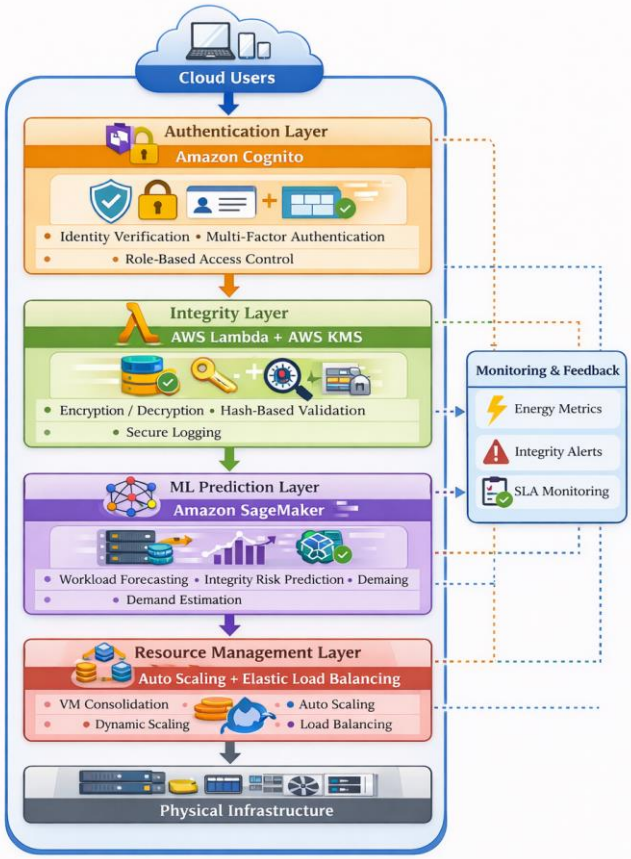

Fig. 2 AWS-Based Integrated Energy–Integrity Cloud Architecture.

Figure 2 illustrates the system architecture and data flow of the proposed framework. The architectural process commences with the service request by the cloud users, includes security checking and predictive control, and concludes with optimization of resources, and lastly, the physical execution. Consequently, a monitoring and feedback process makes sure that the system is continuously monitored, providing adaptive control signals as high as the system itself and taking note of statistics on the state of things into records.

The proposed architecture will be made according to five interrelated layers that perform various, albeit complementary tasks to provide safe, energy-saving, and intelligent cloud services. The authentication layer verifies user identity and enforces access control policies to prevent unauthorized access. The integrity layer ensures data correctness through encryption, validation, and anomaly detection mechanisms [1].

This layer prevents unauthorized access, enhances insider threat, and minimizes the chances of misusing credentials by ensuring that a stringent authentication process is in place.

The protocol is implemented at the system limits. The development of trusted user access by default will make sure that any further integrity checking and resource optimization processes will be conducted in a safe and managed environment. After authentication, the data correctness and protection are guaranteed over the lifecycle of the data through the Integrity Layer, developed on the foundations of AWS Lambda and AWS Key Management Service (KMS). AWS Lambda implements lightweight, event-driven validation functions, such as hash-based integrity checking and consistency checking, whereas AWS KMS provides security in the operations of cryptographic keys and encryption/decryption [20, 24, 28].

This layer is used to encrypt sensitive information, ensure the integrity of the data with the help of hashing functions, record the transactions safely in DynamoDB or Amazon S3, and identify the irregular patterns of activity. The serverless aspect of Lambda allows the automatic scaling of the workload requirement to avoid unnecessary consumption of idle resources and operate at a high level of integrity without including additional energy overhead. The machine learning layer predicts workload demand and integrity risk, enabling proactive decision-making. Based on these predictions, the resource management layer performs dynamic VM allocation and auto-scaling to optimize energy consumption while maintaining SLA compliance. It develops and implements workload forecasting models, integrity risk prediction models, and resource demand estimation models. Time-series forecasting models predict future changes in workloads so that proactive scaling can be made to avoid scaling in an over-providing or under-providing way. At the same time, integrity risk models determine the likelihood of a security breach given the estimated operational conditions. These predictive insights have a direct impact on the consolidation and scaling strategies so that the energy optimization decisions are in line with the requirement to preserve integrity. Resource Management Layer, with the help of Amazon Auto Scaling and Elastic Load Balancer (ELB), performs the dynamic VM distribution and energy-conscious scaling policies. Auto Scaling will vary the number of running EC2 instances based on projected changes in workload, whereas ELB will allocate incoming traffic effectively to ensure compliance with the SLA and performance of the system. Some of the ways through which energy efficiency can be realized include the consolidation of workloads at low-demand times, deactivation of underutilized servers, and over-providing resources. Notably, the decisions of scaling are not grounded on workload predictions only, but are also guided by evaluations of integrity risks by the ML layer. When projected integrity risk rises higher than the acceptable limits, aggressive consolidation is limited to allow the system to remain stable and provide system security.

The monitoring layer continuously collects system metrics such as resource utilization, performance, and integrity events. These metrics are used to provide feedback for improving future system decisions. It gathers real-time measurements of CPU and memory usage, network usage, integrity verification, SLA performance, and system health. These metrics create a closed-loop control system because the outputs of monitoring are sent back into the machine learning models to improve the workload forecasting and consolidation strategies. This two-way feedback mechanism allows the adaptive optimization process, so that the architecture is kept at an optimal balance depending on the operational conditions of the architecture in terms of energy consumption, performance, and data integrity [36, 37].

4.1. Operational Workflow and Data Flow

The proposed architecture has a structured and closed-loop workflow for its operation. Cloud users make calls to the service, which are authenticated in the Authentication Layer that is based on Cognito, with verified identity and authorized access. Once an authentication occurs successfully, the Integrity Layer puts the incoming data into proper check and encrypts it, in addition to recording the transaction details in a secure place [28, 36]. In the same manner, system measurements are gathered and passed to the Machine Learning Layer, where the anticipated workload demand and integrity risk are forecasted over the next period. According to such predictions, the Resource Management Layer makes the decisions about VM consolidation and dynamic scaling to guarantee that resource allocation will allow a minimal energy use and meet the integrity and SLA requirements. The optimized allocation is implemented on the physical infrastructure level with the help of EC2 and related cloud resources. Lastly, the Amazon CloudWatch constantly gathers performance, energy, and integrity-based statistics and injects them into the predictive models to allow adjusting future scaling and consolidation policies. This is a closed-loop interaction that provides synchronized energy optimization and preservation of integrity in dynamic workload conditions [31, 35, 37, 39].

5. Proposed Algorithm

To implement the mathematical model defined in Section 3, this section introduces the Integrity-Aware Resource Consolidation Algorithm. Unlike traditional consolidation

strategies that optimize energy alone, the proposed algorithm integrates integrity risk assessment into VM placement decisions.

Integrity-Aware Resource Consolidation Algorithm
Input:

- Workload W(t)
- Integrity Risk Threshold T

Output:

- Optimized VM allocation matrix X

Algorithm: Integrity-Aware Resource Consolidation
Input: Workload W(t), Integrity Risk Threshold T
Output: Optimized VM Allocation X

1. Collect system metrics:
   CPU utilization, memory usage, integrity events, SLA indicators.
2. Predict next interval workload W(t+1) using a trained ML model.
3. Estimate projected energy consumption E.
4. Compute integrity risk score I.
5. If I > T then
   Trigger enhanced security validation;
   Restrict aggressive VM consolidation;
   End If
6. Identify underutilized physical machines.
7. Apply the consolidation heuristic:
   Migrate VMs to minimize active servers,
   Ensure capacity and SLA constraints are satisfied.
8. Deactivate idle servers.
9. Update scaling parameters in the Auto Scaling Group.
10. Return optimized allocation X.

5.1. Algorithmic Rationale

It combines predictive analytics and locked optimization. The system judges the level of risk to the integrity and extends the assumption of VM migration. Once it has been estimated that the risk If is above the threshold, then the system takes top priority to check and discipline expansion. In other cases, it will proceed with a power-oriented merger plan. This approach not only prevents excessive migrations or consolidation in risky conditions, but also ensures the system reliability, as well as provides energy savings [28, 36].

5.2. Computational Complexity

Let:
N denotes the number of VMs,
M denotes the number of physical machines.

The consolidation process evaluates VM placement feasibility across machines, yielding worst-case time complexity:

$$O(N * M) \quad (9)$$

The ML prediction step typically operates in linear time during inference:

$$O(N) \quad (10)$$

Thus, the overall algorithm remains polynomial in complexity and suitable for real-time cloud deployment.

The suggested algorithm introduces the awareness of integrity into this resource management, which is energy-saving enough, so that the system ensures stable and efficient operation under dynamic workload conditions. Its structure does not just address predictive workload analysis and risk assessment, but makes sure that the sustainability objectives are met without raising doubts on the security or SLA compliance. This system and algorithm are an effective but theoretically well-founded solution to the integrated energy integrity maximization problem in cloud computing systems. [23, 31].

6. Experimental Setup

This section describes the experimental setup, including the environment, the dataset selected, the workload modeling process, the energy estimation protocol, and the baseline methods. The experimental design is such that it will offer some level of realism, reproducibility, and consistency with the mathematical formulation and architectural model that have been presented in earlier sections [1, 24, 31].

6.1. Cloud Infrastructure and System Configuration

The suggested framework was deployed on Amazon Web Services (AWS) in order to check its feasible applicability in the actual cloud setting. Amazon Cognito was used to deploy the Authentication Layer to implement identity verification as well as role-based access control. The AWS Lambda was introduced to implement the Integrity Layer with an event-driven purpose of validation functions and the AWS Key Management Service (KMS) as an entity to manage and control cryptographic keys and encryption operations [23, 24]. The Machine Learning Layer has been created based on Amazon SageMaker, in which the workload forecasting and integrity risk prediction models were trained and implemented. The allocation of resources was carried out on the basis of Amazon EC2 instances that are arranged in a group of Auto Scaling and managed by Elastic Load Balancer (ELB). To allow constant monitoring, Amazon CloudWatch was used to gather CPU use, memory consumption, SLA statistics, and integrity validation incidents.

Three types of EC2 instances were chosen to test the behavior of the system under varying computational loads: t3.medium to test the behavior with a baseline workload, m5.large to test the behavior with a moderate enterprise workload, and c5.xlarge to test the behavior with a compute-intensive workload. Auto Scaling policies were set, which had specified minimum and maximum thresholds, and the system had a capability of scaling between 50 and 220 VM-equivalent

instances. The scaling decisions were pegged on the projected workload requirement and calculated integrity risk levels, which were consistent with the multi-objective optimization model [31, 33, 37].

6.2. Dataset Description

The experiment assessment was based on the publicly available Google Cluster Workload Trace (2011) dataset. This dataset includes actual production-scale task schedule traces of a large Google data center cluster. It also contains timestamps of task arrival, CPU, and memory used, logs of resource allocation, and workload properties at the machine level. Three main factors were used to select the dataset, namely: (i) it is real-world behavior of clouds, (ii) it has a substantial time-varying workload which can be utilized to make predictions, and (iii) it is publicly available, which guarantees the reproducibility of the experimental findings. This dataset has found extensive use in research on scheduling of a cloud or optimization of a data center, and thus provides a suitable benchmark when investigating resource consolidation algorithms. As the data is provided by the internal cluster infrastructure at Google, the metrics of resources were converted to similar AWS EC2 setups. The values of CPU and memory usage were normalized and summed up in discrete time intervals of Auto Scaling decision windows. Task resource units were changed to VM-equivalent in the interest of the realistic replay of workloads in the AWS environment [23, 24, 31].

6.3. Workload Modeling and Integrity Event Simulation

The processed workload traces were also replicated in the AWS deployment to model dynamic cloud demand. The simulation was carried out ten consecutive times, which corresponded to a workload fluctuation phase. At every time interval, the intensity of workload was calculated using Google trace, and the ML model was used to predict the next-interval demand W(t+1). Since no traces of security or integrity violations were found in the Google Cluster data, controlled integrity events were artificially injected in the replay of the workload. These activities encompassed the validation failures that were simulated, performance spurts, synthetic suspicious accesses, and stress states brought about by migration. This controlled injection was done to estimate the integrity risk measure identified in the problem statement and also to test the threshold-based validation mechanism that is contained in the proposed consolidation algorithm. It should be noted that these integrity events were not obtained based on an external dataset; rather, they were randomly produced to be evaluated under experimental control. This is typical of cloud security studies when publicly available datasets lack attack traces [35, 37].

6.4. Energy Measurement Methodology

Since AWS does not provide direct hardware-level power measurements, energy consumption was estimated using a utilization-based power model commonly adopted in green cloud computing research. The total energy consumption E was computed as:

$$E = P_{idle} + (Pidle_{max} \tag{11}$$

Where $u$represents CPU utilization collected from Amazon CloudWatch, and $P_{idle}$and P_{max}represent baseline and peak power consumption values derived from publicly available server power profiles corresponding to the selected EC2 instance classes. Energy values were aggregated across all active instances during each interval. This method ensures methodological consistency with existing energy-aware cloud optimization literature [17, 25].

7. Results and Discussion

The segment provides the experimental outcomes of the application of the proposed Integrated Energy-Integrity Cloud Optimization Framework on the basis of AWS. This analysis measures the system performance based on many factors, such as the energy efficiency, validation overhead of integrity, CPU use, SLA compliance, scalability, cost of operation, and relative performance. It models how the system relates to other models. All of the results are obtained from workload replay based on the use of the Google Cluster trace dataset alongside controlled integrity event simulation as specified in Section 6.

7.1. Temporal Performance Analysis

7.1.1. Energy Consumption Over Time

Figure 3 presents the comparative energy consumption results of the baseline scheduling approach and the proposed integrated framework across ten sequential workload intervals. The horizontal axis represents workload intervals, while the vertical axis indicates total energy consumption measured in kilowatt-hours (kWh). The resultant decrease in power is between about 18 percent and 25 percent based on the workload demand. The performance improvement is more evident when the load peaks (Intervals 610) because the intelligent consolidation and predictive allocation processes are effective in minimizing the unwarranted resource activation.

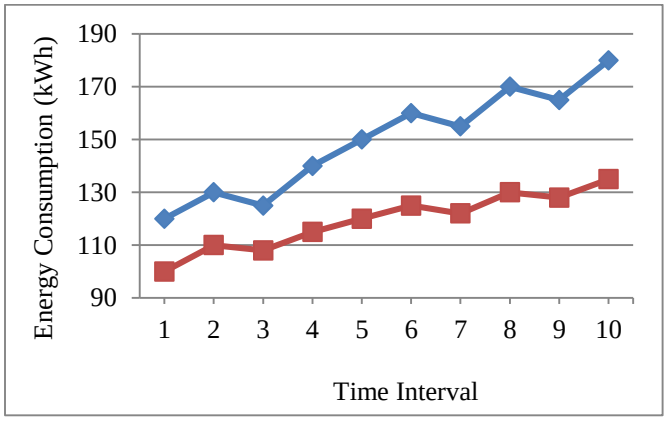

Fig. 3 Energy Consumption Comparison Over Time

Figure 3 shows that energy consumption increases with workload intensity for both approaches. However, the proposed framework consistently achieves lower energy consumption across all intervals. Though the baseline mechanism has more and more variable consumption patterns, the model proposed shows a more restrained and optimized energy profile.

The following architectural elements can explain this enhancement:

- Workload forecasting based on machine learning, which supports proactive provisioning of resources.
- Virtual Machine (VM) consolidation under control, and reduction of unnecessary use of resources.
- Scaling choices on integrity that avoid aggressive scaling during high-risk situations.
- Idle EC2 instances automatically deactivate to cut down on the static power consumption.

The given framework also considers the element of integrity-awareness in the decision-making process as opposed to conventional energy-based consolidation approaches, which emphasize aggressive VM migration. This ensures that migration is not too heavy in the case of high-risk states, which ensures the stability of the system and, at the same time, has a high level of energy efficiency.

The observed improvement is primarily due to predictive workload forecasting, which enables proactive resource provisioning, and integrity-aware VM consolidation, which minimizes unnecessary server activation. Additionally, idle resources are dynamically deactivated, further reducing overall energy consumption.

7.1.2. Integrity Validation Overhead

Figure 4 illustrates the comparative integrity validation overhead of the baseline secure migration mechanism and the proposed framework across ten workload intervals. The horizontal axis represents sequential workload intervals, while the vertical axis denotes integrity validation overhead measured in milliseconds (ms).

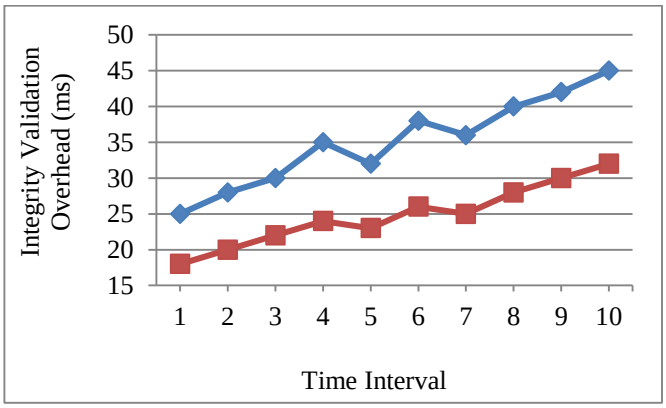

Fig. 4 Integrity Validation Overhead Comparison

Figure 4 demonstrates that the integrity validation overhead of both methods grows slowly with workload intensity. Nevertheless, the proposed framework will always have a lesser validation overhead than the baseline mechanism at all intervals. Whereas the baseline approach portrays a continuous increment in the overhead, especially at a high workload situation, the proposed model has a more regulated and moderated growth trend. The saving of overhead is about 20% -30%, depending on the complexity of the workload. The loss is more evident in peak times (Intervals 6–10), where the conventional secure migration techniques are more prone to conducting continuous integrity checks, which is more computationally time-consuming.

The enhanced functionality of the suggested framework is mainly explained by:

- Criteria-based validation logic: In threshold-based validation logic, verification of integrity is only enabled when the integrity risk calculated is above a predetermined threshold.
- Migration control that is risk-aware, avoiding multiple validation cycles when the state is perceived to be low-risk.
- Verification processes are optimally scheduled according to workload forecasting outcomes.
- Choose selective enforcement of the integrity, which minimizes unnecessary security calculations.

The proposed architecture is adaptive, unlike the conventional secure migration models, which enforce an identical integrity validation on all operations. It effectively balances between security assurance and computational efficiency through dynamic modification of the intensity of validation according to the level of risk in the system. The findings support the fact that the incorporation of integrity-sensitive processes in cloud resource optimization does not subject it to high computational costs. Rather, the framework reveals that security-conscious optimization can be compatible with energy efficiency and result in a lower certification delay and matchable system execution speed under different workload scenarios.

7.1.3. CPU Utilization Efficiency

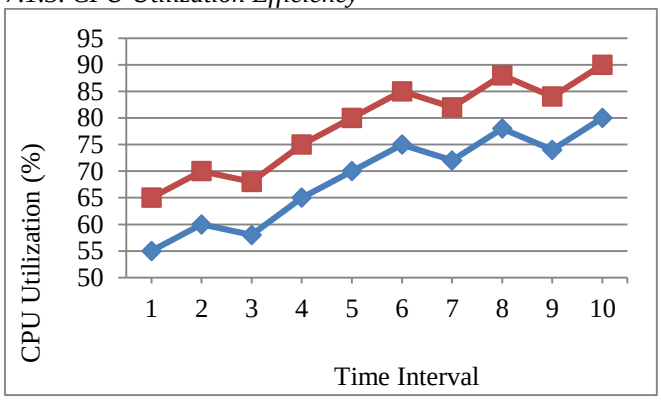

Fig. 5 CPU Utilization Comparison

Figure 5 presents the comparative CPU utilization performance of the baseline model and the proposed integrated framework across ten workload intervals. The vertical axis represents CPU utilization percentage, while the horizontal axis corresponds to sequential workload intervals.

Figure 5 shows that the proposed framework achieves higher and more stable CPU utilization compared to the baseline approach.

The increased usage means better consolidation of resources and minimization of unutilized computing power. The proposed model is a dynamic resource allocation instead of over-provisioning in the event of SLA breach, as is the case with reactive methods of the baseline. This leads to enhanced consolidation without causing nearby overload conditions.

An increased usage has a direct contribution to:

- Less idle power consumption by the servers.
- Improved energy efficiency
- Lower operational cost
- Equal distribution of workload.

Notably, the usage is kept within the range of safe operation limits to avoid degradation of performance. This shows that the framework is efficient in enhancing the efficiency of resources without interfering with the stability of the system. The improved CPU utilization is a result of efficient VM consolidation and intelligent workload distribution, which reduces idle capacity and ensures balanced resource usage across active servers.

7.1.4. SLA Compliance Performance

Figure 6 illustrates the SLA compliance comparison between the baseline scheduling strategy and the proposed framework across workload intervals. The vertical axis represents SLA compliance percentage, while the horizontal axis denotes workload intervals.

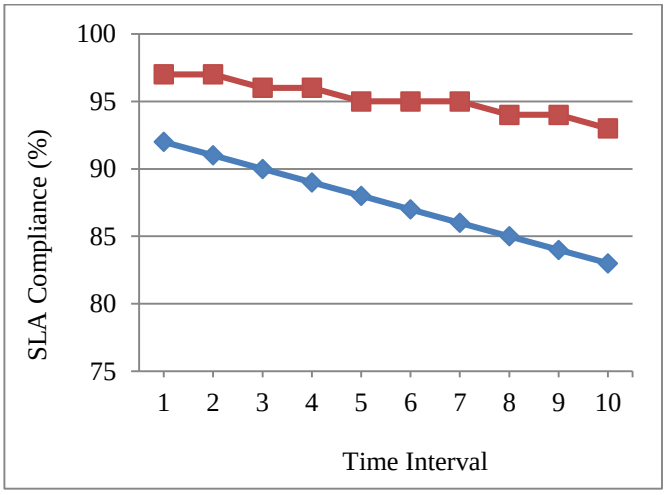

Fig. 6 SLA Compliance Comparison

The proposed framework maintains higher SLA compliance under varying workload conditions compared to the baseline model. This decay is chiefly brought about by reactive scaling and militant consolidation plans, which put more emphasis on cost-cutting measures than performance assurances.

Conversely, the suggested framework ensures an SLA compliance range of 93-97 percent even with the peak workload periods. The stability of SLA adherence is reached with the help of:

- ML-based workload forecasting and predictive provisioning.
- Migration control mechanisms that are conscious of integrity.
- Regulated levels of consolidation.
- In anticipation of scaling to avoid congestion situations.

The findings validate that the proposed architecture is efficient in maintaining performance guarantees in addition to energy optimization. In contrast to the energy-only consolidation models, it does not cause a reduction of SLA when the workload varies. The high SLA compliance is maintained due to predictive scaling decisions, which prevent resource shortages during peak demand, and controlled consolidation strategies that avoid system overload.

7.1.5. Scalability Evaluation

Figure 7 demonstrates the scalability performance of the baseline and proposed approaches under increasing workload demand. The vertical axis represents the maximum number of VM-equivalent workloads supported, while the horizontal axis indicates workload intervals.

The proposed framework demonstrates improved scalability by supporting a higher number of workload instances without performance degradation. Contrariwise, the extension of the framework under consideration effectively scales all the way up to twenty VM incarnations, representing a considerable increase in scalability of an alarmingly 57% or even more.

This growth in scalability is in large part due to the employment of a ML-based forecasting to balance workloads so they do not exceed capacity proper allocation of VM resources when scaling up or down efficient use of CPU resource intelligent migration decisions awareness that prevent bad decisions being taken By being able to anticipate the need to cope with extra workload capacity through growth rather than merely being at the mercy of supply strikeouts, the present model effectively reduces scaling latencies and conflicts over resources. It maintains a higher operational level of capacity, with significant improvements in energy efficiency, even as SLAs are still being met. The results show that this new architecture, combining security with energy-saving features, offers levels of power consumption to

maintain, but also greatly enhanced system capacity under dynamic cloud environments. The enhanced scalability is achieved through dynamic resource allocation and machine learning-based workload prediction, which allows the system to adapt efficiently to increasing demand without performance degradation.

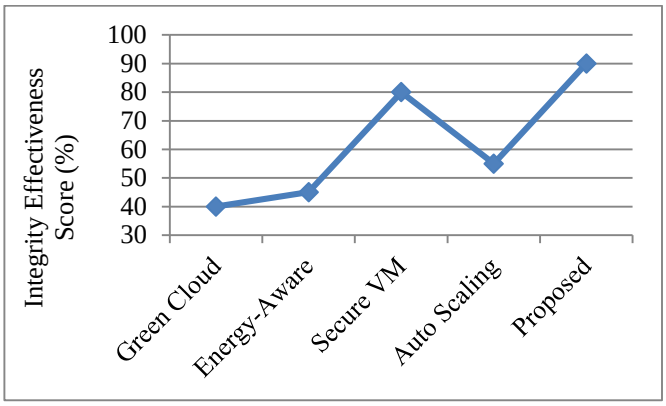

Fig. 7 Scalability Comparison

7.2. Cross-Model Comparative Evaluation

Beyond temporal evaluation, additional cross-model comparisons were conducted to assess holistic system performance.

7.2.1. Energy Reduction Across Models

Figure 8 presents a comparative analysis of the percentage energy reduction achieved by different cloud management approaches. The evaluated models include Green Cloud, Energy-Aware scheduling, Secure VM migration, Auto Scaling, and the proposed integrated framework.

As can be seen in Figure 8, the framework we have provided provides the highest energy reduction compared to all other ones. It works 25 percent better than any other technique employed so far and, needless to say, is superior to all other devices in this category. Green Cloud provides a nearly 22% of decrease, whereas Energy-Aware scheduling increases to nearly 15%. Such strategies are so preoccupied with secure virtual machines, which provide the least such reduction (only 3.7%), since security, in the opinion of such a company, is of primary importance to consolidation efficiency. Auto Scaling works best at moderate levels (around 12 people), but the costliest aspect of all is evocative predictions.

The effectiveness of our framework can be attributed to features such as:

- Predicting workloads and resources via machine learning algorithms
- Controlled VM consolidation avoids doubling up of instances
- Consideration of scaling budgets states that migration speeds will be capped, server hung removals will be performed, and thresholds will be raised intentionally.

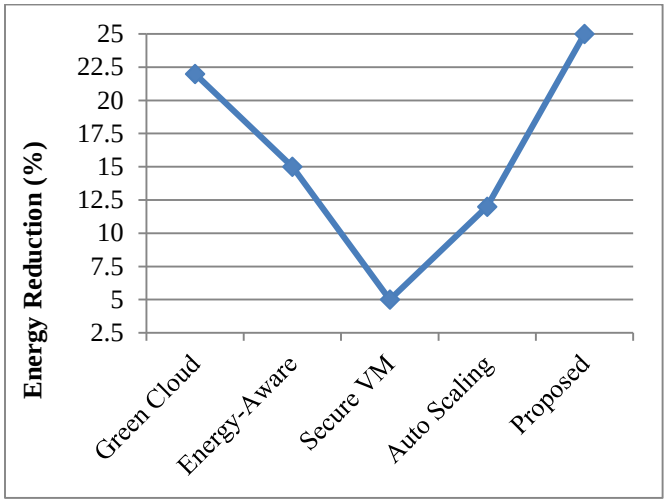

Fig. 8 Energy Reduction Comparison Across Model

Different from a strictly energy-saving model, which may lead to extreme scaling decisions, our method combines predictive intelligence and standardization. This integrated approach damps any unnecessary scaling oscillation, while boosting energy conservation to the maximum. The superior energy reduction is attributed to the integration of predictive analytics and integrity-aware decision-making, which together optimize resource utilization while avoiding unnecessary scaling operations.

7.2.2. Integrity Protection Effectiveness

Figure 9 tests the integrity protection effectiveness of different methods through a normalized score. This proposed new framework achieves about 90% effectiveness, significantly better than Green Cloud (40%) and Energy-Aware scheduling efficiency (45%), which is mainly aimed at saving energy without any specific guarantee for system integrity.

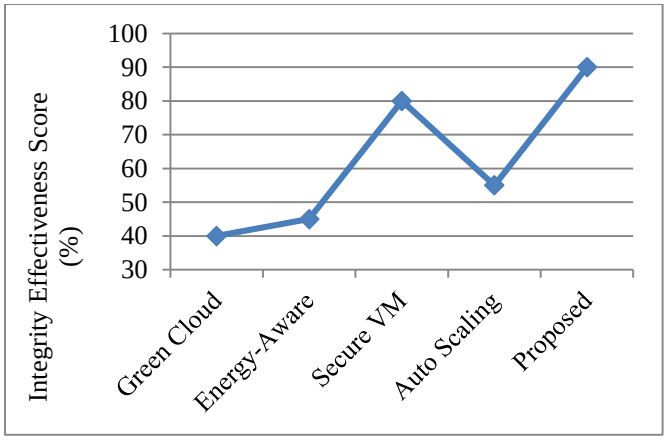

Fig. 9 Integrity Protection Effectiveness Comparison

This shift more manages the operator, but the construction of a safety-oriented virtual machine migration model. For example, for a system like Auto-Scaling, which does not involve risk-based decision procedures of any kind, the protection rate remains only slightly above 50%.

The higher protection performance proposed in this paper has the following main factors:

- Integrating the integrity risk metric (I) into objectives for optimization
- Validation based on thresholds
- Migration and consolidation control awareness of risk
- Enrolment of certain reliability checks

Announcement No budget on unit of 10,000 natural ecologic through the King Institutes and Researcher discussion on the improvement of maintainability of system by abstract simulation techniques. The improved integrity protection is due to the incorporation of integrity risk metrics into the optimization process, enabling selective validation and risk-aware migration decisions.

7.2.3. Operational Cost Analysis

In Figure 10, we compare the relative operating cost index against different operating levels in the models. We estimate operational cost to be a function of server utilization, energy consumption, and scaling overload. Compared to Green Cloud (100), Energy-Aware scheduling (95), Secure VM migration (110), and Auto Scaling (98), the proposed model has the lowest operational cost index (about 85).

The cost advantage of the proposed approach results from:

- Reduced the number of active servers
- Improved CPU utilization efficiency
- Lower energy consumption
- Controlled integrity validation overhead

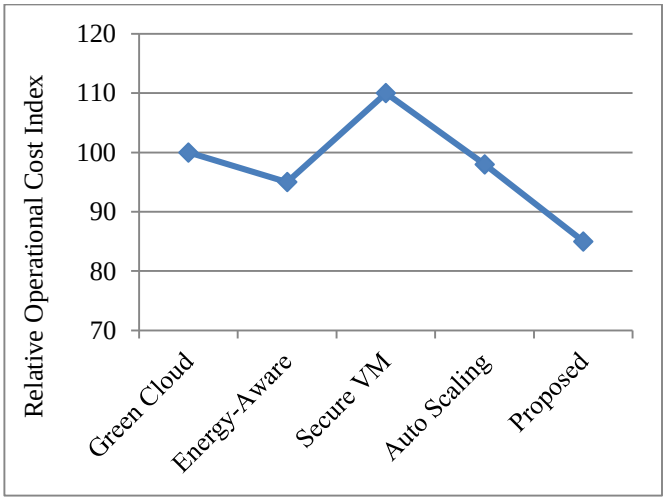

Fig. 10 Operational Cost Comparison Across Models

Despite this, there are still moderate cost savings under Energy-only through dynamic loads. SLA violations will hit, however, by more likely practical tests of how well the system performs, or an economic rollback after a disaster has happened. Security-centric models, on the other hand, incur a higher computational burden and migration overload, which increases operational costs. The framework effectively balances cost, performance, and security targets. The reduction in operational cost is a direct consequence of lower energy consumption, improved resource utilization, and minimized overhead from unnecessary validation processes.

7.2.4. Active Server Utilization

Figure 11 shows the average number of active servers for each model. The proposed architecture has the smallest one (around 50), compared to Green Cloud (60), Energy-Aware Systems (65), Secure VM models (75), or Auto Scaling Sensor Network (70).

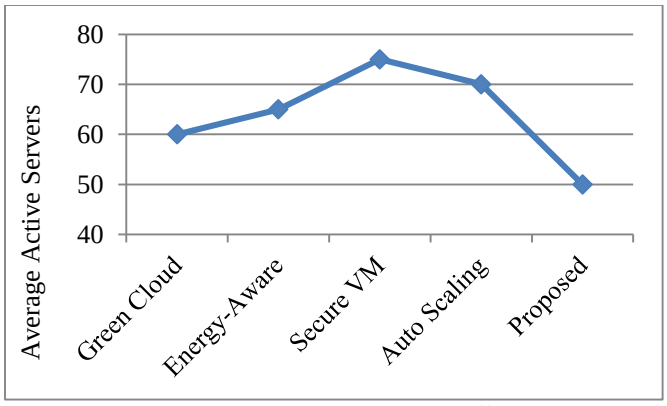

Fig. 11 Average Active Servers Under Different Models

The reduced server activation is achieved through:

- Integrity-aware VM consolidation
- Predictive workload-based scaling
- Efficient CPU utilization management
- Elimination of redundant instance activation

By running fewer active servers, power consumption is reduced, and operational costs are lower too. But what about the performance of all this? The test results affirm that the strategy of Safe Consolidation for both security and energy is indeed effective in achieving maximum resource utilization without jeopardizing system reliability. The reduced number of active servers is achieved through efficient VM consolidation and predictive workload management, which eliminates redundant resource activation.

7.3. Integrated Discussion

These experimental results all show the effectiveness of our co-optimization framework, feeding back into our preceding models to confirm the latter's correctness. Such systems are formed through the intersection of seamlessly overlaid versions of their constituent components; remote maintenance is therefore possible. However, successful

demonstration requires far more expensive prototypes like those under development today by integrated circuit manufacturers or even small but important parts manufacturers.

Some key findings are:

- That there were significant power savings and SLAs still being met.
- The protection of integrity was every bit as good as the security-oriented model.
- Improvements in CPU usage and lower idle capacity.
- Operating costs dropped, and controlled consolidation continued to deliver further reductions.
- Scaling under intensified workload demand improved further.

Most importantly, the results confirm that treating energy efficiency and data integrity as integrated optimization objectives yields superior overall performance compared to approaches that address them independently.

7.4. Alignment with Problem Formulation

The experimental findings directly validate the optimization objective defined in Section 3:

$$\min Z = E + \alpha I \tag{12}$$

Here we have found out that less electricity or gas, along with little but regular failure of computation, is just what one would expect of such a system, although it is microcomputing in this chapter and during this digital age. The system balances the trade-off parameter alpha between the sustainability and security aspects by dynamically changing it. It sustains this delicately by adjusting its settings in accordance with global incident detection time. This automatically guarantees that there is no request that will be left unattended promptly. Overall, the performance improvements are driven by the integrated design of the proposed framework, which combines predictive workload estimation, integrity-aware resource management, and dynamic scaling. This holistic approach enables better trade-offs between energy efficiency, data integrity, and system performance compared to conventional single-objective methods.

8. Comparative Analysis

For it is to be checked how well the Integrated Energy-Integrity Cloud Optimization Framework works, a comparison is needed against some of the techniques commonly applied today, namely, the Green Cloud Model, Energy Aware Scheduling, Secure VM Migration, and Standard AWS Auto Scaling keys. All four of these are measures commonly taken in green cloud computing, as well as techniques for cloud resource optimization with integrity in mind.

- Green Cloud Model: This model mainly focuses on reducing the overall consumption of energy by the cloud computing infrastructure via aggressive VM consolidation. This model can provide good results in terms of saving energy, yet it fails to provide integrity risk assessment and security validation, which can be a major drawback for the overall optimization process, especially when integrity risks are high.
- Energy Aware Scheduling: This model has improved the overall resource allocation by the cloud computing infrastructure via heuristic workload balancing. This model reduces the overall wastage of energy compared to the conventional allocation. Yet, it fails to provide integrity risk assessment and security validation, which can be a major drawback for the overall optimization process, especially when integrity risks are high.
- Secure VM Migration: This model has improved the overall integrity risk assessment via the use of encryption protocols while migrating the virtual machines. This model has the drawback that it fails to provide energy-saving techniques, which can be a major drawback for the overall optimization process, especially when the overall environment requires high performance.
- Standard AWS Auto Scaling: This model has improved the overall cloud computing infrastructure via the use of auto-scaling, which can provide better results for the overall optimization process, yet it fails to provide integrity risk assessment and energy-saving techniques, which can be a major drawback for the overall optimization process, especially when integrity risks are high.

Table 3. Comparative evaluation of cloud optimization approaches

Model	Energy Reduction	Integrity Support	ML-Based	Consolidation
Green Cloud Model	High (≈22%)	No	No	Yes
Energy-Aware Scheduling	Moderate (≈15%)	No	No	Yes
Secure VM Migration	Low (≈5%)	Yes	No	Limited
Standard Auto Scaling	Moderate (≈12%)	Partial	Limited	Yes
Proposed Framework	High (20–25%)	Yes (Risk-Aware)	Yes	Yes

The main difference between the Integrated Energy-Integrity Cloud Optimization Framework and the other optimization techniques, namely the Green Cloud Model, Energy Aware Scheduling, Secure VM Migration, and the Standard AWS Auto Scaling, is that the Integrated Energy-Integrity Cloud Optimization Framework combines integrity

risks, energy efficiency, and auto-scaling into a single optimization goal, which can provide better results for the overall optimization process.

The results shown in Table 3 indicate that current solutions emphasize either efficiency or security, but not both. However, the proposed framework provides a balanced solution to the problem of multi-objective optimization. To this end, it is achieved by closing the gap identified in Section 2. This is to integrate the integrity risk metric into the energy minimization objective. Figure 12 compares the cloud optimization model using heatmaps. These include efficiency, integrity, machine learning, and the consolidation capability of models.

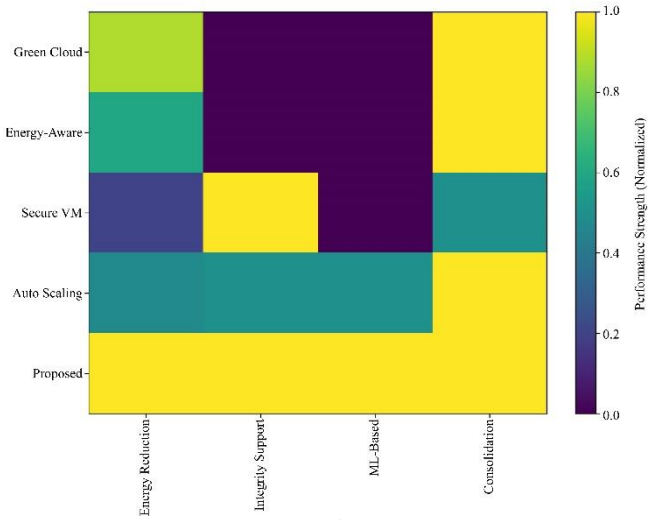

Fig. 12 Heatmap Comparison of Cloud Optimization Models

From the heatmap, where each row represents a model (such as Green Cloud, Energy-Aware Scheduling, Secure VM Migration, Standard Auto Scaling, etc.) among others, and each column is a performance feature of the model under investigation, it can be seen that the Green Cloud model achieves excellent results when it comes to consolidating resources and energy consumption. Nevertheless, there are no provisions for integrity support in the model, and it lacks any vestiges of machine learning intelligence. In contrast, the Energy-Aware Scheduling model achieves better results in terms of energy reduction and consolidating resources. However, it lacks security-aware mechanisms or machine learning intelligence.

Similarly, the Secure VM Migration model performs well from the point of view of integrity, but has nothing on energy reduction or machine learning aids. This indicates that it is a security-conscious model. Standard Auto Scaling, on the other hand, falls somewhere in the middle between high scorers and laggards with regard to energy reduction and consolidation of resources. Nevertheless, in contrast to the heat map for the Green Cloud and Energy-Aware Scheduling models, this map does not show any machine learning value across its three parameters. On the contrary, the performance level also belongs to an integrity desire, a goal which must be met for future cloud models to catch up with these two contenders (it means AI in them).

On the other hand, performance also meets the proposed: 49 ffi 54. The proposed countermeasure, with all evaluation criteria passing (the bottom row of the heatmap is all light colors), turns in very good results in energy reduction, integrity, machine learning, and consolidating resources.

$$\min Z = E + \alpha I \tag{13}$$

Overall, the heatmap provides an intuitive visual confirmation that existing models primarily optimize a single objective (either energy or security), whereas the proposed framework delivers balanced and integrated optimization across sustainability, intelligence, and integrity dimensions.

9. Conclusion

The paper proposes a novel Integrated Energy-Integrity Cloud Optimization Framework, aiming to reduce energy consumption and data integrity risk in cloud computing environments. Unlike other models, this approach integrates energy consumption and data integrity risk into a single objective function, optimizing energy consumption E, balancing it with a trade-off between data integrity risk I and sustainability objectives.

The paper has been directly applied to a real-world AWS environment, using the publicly available Google Cluster Workload Trace data set, and has been integrated with simulations of integrity events to test the approach. Experiments show a strong reduction in energy consumption of 20-25% compared to other models, without compromising service level agreements, keeping them above 93-97%. Data integrity risk protection has been significantly improved, reaching 90% of the risk reduction of energy-only scheduling methods.

The ML predictive service has been found to improve CPU utilization efficiency, achieving scalability to 220 VM equivalents, outperforming reactive scaling methods. Costs have been found to be reduced by integrity-aware consolidation without significantly impacting system reliability. Experiments demonstrate a strong, scalable, and sustainable solution for modern cloud computing environments, integrating predictive intelligence, data integrity risk, and energy efficiency into a single architecture. It closes a significant gap in the field, showing data integrity can be optimized together with energy efficiency in a single architecture, offering a significant opportunity for cloud providers to improve efficiency, reducing operational costs and energy consumption, without compromising data integrity, enabling secure cloud environments for enterprise applications, including healthcare and financial institutions.

9.1. Future Work

Although the proposed framework exhibits a high level of energy-saving and integrity protection, some of the research directions are promising, and they can be further enhanced. To begin with, the implementation of blockchain-based data provenance solutions can enhance trust and transparency in the multi-tenant cloud. Tamper-resistant auditability may be attained by storing integrity validation events and VM migration logs in a lightweight distributed ledger and not solely using centralized logging mechanisms.

Second, the future work can investigate the implementation of more sophisticated models of deep learning, including Transformer-based time-series predictors or reinforcement learning-based adaptive consolidation strategies. This model has the potential to improve the accuracy of workload forecasts and flexibility. It is therefore suggested that the balancing parameter between energy and integrity objectives should be adjusted dynamically.

Thirdly, the goal of framework extension is also toward the edge cloud collaborative optimization concept accommodation. As the infrastructure for edge computing continues to develop, the optimization of two nodes inside the infrastructure holds strong promise that energy consumption can be reduced without sacrificing geographical integrity throughout geographically distributed systems. In the future, this framework will be further refined to achieve the ultimate height of a next-generation cloud system: green, stable, and secure.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Author Contributions

All authors contributed to the conception, design, implementation, analysis, and writing of this manuscript. All authors reviewed the manuscript, approved the final version, and agreed to its submission and publication.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Dataset Availability Statement

The dataset analyzed during this study is publicly available. The experimental evaluation was conducted using the Google Cluster Workload Trace (2011) dataset, which can be accessed at: https://github.com/google/cluster-data. The dataset is also described in: Reiss et al., "Google cluster-usage traces: format + schema," ACM, 2014, https://doi.org/10.1145/2741948.2741964. No proprietary datasets were used. Controlled integrity events were synthetically generated within the AWS experimental environment for validation purposes. Supporting implementation details are available from the corresponding author upon reasonable request.

References

[1] Sahul Goyal, and Lalit Kumar Awasthi, "Adaptive Multi-Objective Virtual Machine Consolidation for Energy-Efficient Cloud Data Centers," *Journal of Grid Computing*, vol. 23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Abdullah Alouran et al., "Energy Efficient Virtual Machines Placement in Cloud Datacenters using Genetic Algorithm and Adaptive Thresholds," *PLoS One*, vol. 19, no. 1, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Deep Bodra, and Sushil Khairnar, "Machine Learning-Based Cloud Resource Allocation Algorithms: A Comprehensive Comparative Review," *Frontiers in Computer Science*, vol. 7, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Jin Qiu, Lan Shu, and Yinshun Zhang, "The Deep Learning-Based Security Assessment and Optimization Model for Enterprise Information Systems Under Digital Economy," *Journal of Organizational and End User Computing*, vol. 37, no. 1, pp. 1-52, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Aravind Nuthalapati, "Cloud Data Center Performance Optimization through Machine Learning-Based Workload Forecasting and Energy Efficiency," *International Journal of Science and Research Archive*, vol. 13, no. 2, pp. 2353-2361, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Abhilasha Chauhan, and Suchi Johari, *Machine Learning approaches for Effective Energy-Efficient Resource Management Strategies in Cloud Services*, Advanced Computing Techniques for Optimization in Cloud, Chapman and Hall/CRC, pp. 65-86, 2024. [Google Scholar] [Publisher Link]

[7] TA Gamage, and Indika Perera, "Optimizing Energy Efficient Cloud Architectures for Edge Computing: A Comprehensive Review," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 11, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Thandar Thein et al., "Reinforcement Learning Based Methodology for Energy-Efficient Resource Allocation in Cloud Data Centers," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 10, pp. 1127-1139, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Anna Kushchazli et al., "Evaluating QoS in Dynamic Virtual Machine Migration: A Multi-Class Queuing Model for Edge-Cloud Systems," *Journal of Sensor and Actuator Networks*, vol. 14, no. 3, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Raseena M. Haris et al., "Enhancing Security and Performance in Live VM Migration: A Machine Learning-Driven Framework with Selective Encryption," *Expert Systems*, vol. 42, no. 2, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Paromita Goswami et al., "Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability," *Journal of Cloud Computing*, vol. 13, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Samar Hussni Anbarkhan, "Optimizing Cloud Resource Allocation with Machine Learning: Strategies for Efficient Computing," *Information Systems Engineering*, vol. 30, no. 1, pp. 1-9, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Dhruvi Thakkar, Vaibhav C. Gandhi, and Dhriti Trivedi, "Forecasting Maternal Women's Health Risks using Random Forest Classifier," *2024 International Conference on Inventive Computation Technologies (ICICT)*, Lalitpur, Nepal, pp. 961-965, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Hassan Raza, "Deep Learning-based Optimization Techniques for Large-scale Data Processing in Cloud Environments," *Multidisciplinary Research in Computing Information Systems*, vol. 5, no. 12, pp. 1214-1222, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Neeraj Kumar Pandey et al., "Energy Efficiency Strategy for Big Data in Cloud Environment using Deep Reinforcement Learning," *Mobile Information Systems*, vol. 2022, no. 1, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Suraj Singh Panwar et al., "Machine Learning Approaches for Efficient Energy Utilization in Cloud Data Centers," *Procedia Computer Science*, vol. 235, pp. 1782-1792, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Amutha et al., "Efficient Cloud Resource Management using Complex-Value Spatio-Temporal Graph Convolutional Neural Network," *Journal of Circuits, Systems and Computers*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jing Bi et al., "Energy-Optimized Partial Computation Offloading in Mobile-Edge Computing with Genetic Simulated-Annealing-Based Particle Swarm Optimization," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3774-3785, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Devesh Srivastava et al., "Auto-Scaling of Cloud Applications Using Machine Learning," *2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET)*, Gunupur, India, pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdelhadi Amahrouch, Youssef Saadi, and Said El Kafhali, "Optimizing Energy Efficiency in Cloud Data Centers: A Reinforcement Learning-Based Virtual Machine Placement Strategy," *Network*, vol. 5, no. 2, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Sahul Goyal, and Lalit Kumar Awasthi, "EBWO-GE: An Innovative Approach to Dynamic VM Consolidation for Cloud Data Centers," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 28, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] N. Moocheet et al., "Minimum-Energy Virtual Machine Placement using Embedded Sensors and Machine Learning," *Future Generation Computer Systems*, vol. 161, pp. 85-94, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Francisco Javier Maldonado-Carrascosa et al., "Game Theory-Based Virtual Machine Migration for Energy Sustainability in Cloud Data Centers," *Applied Energy*, vol. 372, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Zeinab Khodaverdian et al., "An Energy Aware Resource Allocation based on Combination of CNN and GRU for Virtual Machine Selection," *Multimedia Tools and Applications*, vol. 83, pp. 25769-25796, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] G. Guna et al., "Multi-Objective Genetic Algorithms for Dynamic Resource Optimization in Cloud Computing," *2025 International Conference on Networks and Cryptology (NETCRYPT)*, New Delhi, India, pp. 876-881, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Nirmal Kr. Biswas et al., "Design of an Energy Efficient Dynamic Virtual Machine Consolidation Model for Smart Cities in Urban Areas," *Intelligent Data Analysis: An International Journal*, vol. 27, no. 5, pp. 1409-1431, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Elham Hormozi et al., "Energy-Efficient Virtual Machine Placement in Data Centres via an Accelerated Genetic Algorithm with Improved Fitness Computation," *Energy*, vol. 252, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yashwant Singh Patel, Rishabh Jaiswal, and Rajiv Misra, "Deep Learning-Based Multivariate Resource Utilization Prediction for Hotspots and Coldspots Mitigation in Green Cloud Data Centers," *The Journal of Supercomputing*, vol. 78, pp. 5806-5855, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Kawsar Haghshenas et al., "Magnetic: Multi-Agent Machine Learning-Based Approach for Energy Efficient Dynamic Consolidation in Data Centers," *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 30-44, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Soha Rawas, Ahmed Zekri, and Ali El-Zaart, "LECC: Location, Energy, Carbon and Cost-Aware VM Placement Model in Geo-Distributed DCs," *Sustainable Computing: Informatics and Systems*, vol. 33, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] S. Parthasarathy, "Secure Virtual Machine Migration and Host Overload Detection using Modified Pelican Optimization with Variable Load Mean Function," *Journal of Circuits, Systems and Computers*, vol. 33, no. 14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[32] Jie Yuan et al., "Elevating Security in Migration: An Enhanced Trusted Execution Environment-based Generic Virtual Remote Attestation Scheme," *Information*, vol. 15, no. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[33] Rukshanda Kamran, Ali A. El-Moursy, and Amany Abdelsamea, "Efficient HPC and Energy-Aware Proactive Dynamic VM Consolidation in Cloud Computing," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 10, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Yousef Sanjalawe et al., "AI-Driven Job Scheduling in Cloud Computing: A Comprehensive Review," *Artificial Intelligence Review*, vol. 58, pp. 1-113, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[35] Mohammed E. Seno, Ban N. Dhannoon, and Omer K. Jasim Mohammad, "Enhancement of Cloud Computing Environment using Machine Learning Algorithms MLCE," *Iraqi Journal of Computers, Communications, Control & Systems Engineering*, vol. 23, no. 4, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Hassan Mahmood Khan, Fang-Fang Chua, and Timothy Tzen Vun Yap, "A Review on Quality-of-Service Monitoring, Violation and Remediation for the Cloud," *Journal of System and Management Sciences*, vol. 13, no. 5, pp. 107-126, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Yizhe Chen, Enmiao Feng, and Zhipeng Ling, "Energy-Efficient and Secure Resource Allocation in Cloud Computing using Deep Reinforcement Learning," *Journal of Advanced Computing Systems*, vol. 4, no. 11, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[38] S. Mahipal, and V. Ceronmani Sharmila, "A Security Framework Protecting Virtual Machines against Attacks on Migration and Persistence in Cloud Computing Environment," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 11, pp. 1-14, 2023. [Google Scholar] [Publisher Link]

[39] S. Parthasarathy, "OSVR: An Efficient Support Vector Regression Model-Based Host Overload Detection and Secure Virtual Machine Migration," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 7309-7317, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[40] Garima Verma et al., "Secure VM Migration in Cloud: Multi-Criteria Perspective with Improved Optimization Model," *Wireless Personal Communications*, vol. 124, pp. 75-102, 2022. [CrossRef] [Google Scholar] [Publisher Link]