Kufa Journal of Engineering
Vol. 17, No. 1, January 2026, P.P. 73-95
Article history: Received 18 September 2024, last revised 15 November 2024, accepted 15 November 2024

AN OPTIMIZED INTELLIGENT FRAMEWORK FOR SUSTAINABLE AND ENERGY-EFFICIENT DATA CENTER OPERATIONS USING SECURESUSTAINNET

Gayathri A[1], M. Muzaffar Hussain[2], Srinivasan V[3], Ambeth Raja A[4], and Jayanthi R[5]

[1] Department of Data Science, SRM IST Science and Humanities, Ramapuram, Chennai, India, Email: gayathriragul2005@gmail.com.

[2] Department of Artificial Intelligence and Data science, C.Abdul Hakeem College of Engineering and Technology, Melvisharam, India, Email: mhd.muzaffar@gmail.com.

[3] Department of MCA, Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bangalore, India, Email:srinivasan-mcavtu@dayanandasagar.edu.

[4] Department of Computer Science, Thiruthangal Nadar College,Chennai, India, Email:ambethraja.a@thiruthangalnadarcollege.edu.in.

[5] Department of MCA, Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bangalore, India, Email: jayanthi-mcavtu@dayanandasagar.edu.

https://doi.org/10.30572/2018/KJE/170105

ABSTRACT

The SecureSustainNet Framework- a novel technique for enhancing security and sustainability in data centers is introduced in this paper. Given the security and sustainability concerns with data centers, this paper tackles the challenge of balancing data center security and energy efficiency. Existing solutions are unable to provide the required security level without large processing and power costs. States existing approaches that combine efficient resource utilization with high security performance is identified as a research gap. The multi-objective optimization of those approaches is designed to incorporate energy, efficient techniques and security functionalities. The approach has 6 main algorithms; Intrusion Detection System with Anomaly Detection; AES, 256 encryptions with virtualization, based key management; Role Based Access Control (RBAC) with dynamic policy tuning; dynamic resource allocation; energy consumption monitoring and management; and renewable source integration. The framework has been implemented into the network simulator ns, 3. A remarkably high 98.7% Anomaly Detection Rate (ADR) was elicited through an interpreter Intrusion Detection System (IDS) against Gaussian Mixture Models (GMM), 6.4% above existing approaches, with a mean

0.4% False Positive Rate (FPR). It achieved a 2.5% increase in processing time due to its AES, 256 Encryption system through which employ a dynamically managed key management system. It attained a 97.4% Access Control Effectiveness (ACE) and an 8.8% increase against traditional models through its dynamic policy adaptations based on user context. It obtained an 85.2% Resource Utilization Efficiency (RUE) and a 7% increase over its competitors while reducing the energy consumption by 15.6% through its efficient resource utilization. The power usage effectiveness (PUE) of the system was calculated as 1.25, a far cry from current models that achieved it as high as 1.47.

KEYWORDS

Sentimental analysis, Machine learning, LSTM, Attention mechanism.

1. INTRODUCTION

Vehicular ad hoc networks or VANETs are becoming an essential technology for enabling the data center constitutes the backbone of the emerging digital society and the grounds for internet, enabled services, cloud computing infrastructures, and many others which constitute the infrastructure for every kind of industry, institution, and domestic realm in our days, all over the world. With the new millennium and the new era of information age, there has been an increase in the dependence upon digital technology by an ever-increasing number of machines and entities in every aspect of human activity. As a result, the focus on an efficient, resilient and environmentally responsible data center operation has been ever, growing. Still, amidst these developments there are quite large number of challenges to face, which among others are the security of the data center infrastructure and the minimization of its ecological footprint (Ghosh and Grolinger, 2021; Bhowmik et al., 2022; Bhushan et al., 2020; Bytyqi et al., 2022). The risk of the data center security breaches is even higher, both because of the huge amount of data it might contain, and because of the significant threat posed to national security. The data center stores mission, critical contents of relevance to enterprise, private, or even national security; thus it constitutes a lucrative target for a range of possible countermeasures, including the exploitation of applied vulnerabilities through APT, DDoS, ransomware, and myriads of possible security breaches (Savaglio and Fortino, 2021; Chen et al., 2022; Dogan et al., 2022). Consequently, the design of the security architecture must be capable of having a number of security mechanisms safeguarding the all, round operation. Critical to the operation of the data center are several security tools, such as the Intrusion detection system (IDS), which constantly monitors traffic looking for unexpected patterns, encryption algorithms like AES, 256, which guarantee data integrity and privacy during at, rest and in transit, or the Role, based access control (RBAC), which enforces security policies to restrict access basing on the roles of the different entities trying to access (Gao et al., 2021; Gunasekeran et al., 2021; Han et al., 2020; International Energy Agency, 2022). Security is always a battleground for attackers and thus, if the enemies hit their target by some mode, then without a doubt they will certainly enhance it by inventing newer forms of attack. Therefore, the security infrastructure must be capable of being agile and robust enough to address the rapidly changing security threats.

In order to address the above mentioned, the proposed SecureSustainNet Framework that encompasses key security components and offers flexible approach to provide better protection for data center infrastructures. Aside from the risks associated with security, data centers also face increased scrutiny over their carbon footprint, and tremendous electricity consumption of data centers which account for a large amount of the world's total carbon emission (Zhang et

al., 2018; Lei, 2022; Mastroianni and Palmieri, 2022; Mohiddin and Suresh Babu, 2021). The current emphasis on climate change and increasing electricity price is a key contributor towards the drive for better energy efficiency and green computing techniques. The objectives of a sustainable data center are to reduce energy waste, maximize operational efficiency, and utilize renewable energy sources. Existing infrastructure utilizes resources with little or no consideration, and consumes high power. Dynamically assigning workloads according to need is done in real-time to avoid energy waste, as it eliminates redundant computation when there are no demanding jobs. Useful information can be gathered by using energy monitoring metrics such as Power Usage Effectiveness (PUE), to enable optimization methods to be targeting more efficiently. Energy consumption can be reduced through the utilization of solar or wind energy. Energy saving initiatives do not only benefit the environment but also the economy as future regulations may impose stricter guidelines, coupled with the ever-increasing electricity price (Murino et al., 2023; Oluwole-Ojo et al., 2023; Kumar et al., 2020; Kumar et al., 2019). Energy saving efforts within a centralized operational model helps in maximizing productivity with minimized carbon footprint, by integrating energy efficient strategies into a singular operation. Previously, the areas of energy management and security for data centers have been handled separately with unique sets of technologies and policies (Saraswat et al., 2022; Verma et al., 2022). This separation of domains normally results in unexpected trade-off; where saving measures lead to lack of security or data center redundancy, or, stronger security measures may result in heavier computation load and higher energy consumption (Wang et al., 2022; Mi et al., 2019; Xiong et al., 2021; Yang et al., 2021; Zhou et al., 2021). An example of this is computationally intensive encryption that could increase server workload and energy consumption, while excessive consolidation of resources (to minimize energy) could decrease fault tolerance and overall security posture of the system.

To sum up, these interactions illustrate the importance of an integrated approach being both efficient as well as secured. This is exactly what theillustrated by the SecureSustainNet Framework which integrates the most efficient security solutions with intelligent power consumption management. More precisely the framework uses renewable energy integration, dynamic resource scheduling, AES-256 encryption, role-based access control, intrusion detection systems, and continuous energy consumption monitoring to solve both problems faced by modern day data centers. To show effectiveness, the framework is simulated using ns-3 network simulator which permits thorough modeling of network behavior, security protocol, and energy consumption profile in a realistic environment to permit efficient examination over a wide variety of scenarios. Performance improvement are indeed illustrated

by simulation and the framework simultaneously yields a 28% decrease in power consumption, beneficial for the operational expenses and environmental sustainability, and an improvement in the accuracy of detection of cyber-attacks by 32%, greatly enhancing the security of data centers.

This paper is organized as follows. Section 2 provides an overview of existing studies on data center security and sustainable computing. It highlights the existing drawbacks and research challenges. Section 3 presents the detailed framework for SecureSustainNet Framework and introduces the contributions of its six key sub-algorithms to integrated security and energy efficiency. Section 4 gives details of implementation approach, simulation environment, and performance metrics. Section 5 presents experimental results and compares the performance against present systems. Section 6 gives the conclusion of the proposed study and future work.

2. RELATED WORK

Recently, several techniques are emerged in many studies for the improvement of dependable Data center infrastructures have been challenged in recent years to adapt to meet sustainability goals and enhance cybersecurity performance, as well as increase energy efficiency. Various solutions have been proposed through previous studies: intelligent decision-support models, energy-aware operational framework and security evaluation systems. Mastroianni and Palmieri (2022) had proposed the adaptive energy optimization with consideration for the security constraints of cyber-security to develop and implement reliable and responsive data center operations. Meanwhile, Mohiddin and Suresh Babu (2021) presented green computing paradigms which offer an ecological IT environment in a framework toward promoting the awareness on sustainable technologies and innovation in computational contexts. Recent work has targeted the reduction of energy consumption while ensuring that the system functionality does not compromise on operational capabilities. Utilizing advanced control techniques, the research carried out in, Oluwole-Ojo et al. (2023) focused on the analysis and optimization of energy consumption for continuous-flow ohmic heating systems that demonstrate a form of energy-focused operational management and could be applied in large-scale computational infrastructure. Methods have also evolved for the improvement of digital security. For instance, Kumar et al. (2020) had employed Hesitant Fuzzy Sets to support decisions in web application security.

A similar approach Kumar et al. (2019) revealed weaknesses of existing security evaluation methods through a fuzzy logic-based model to estimate software security robustness. Improvements to privacy preservation and secure communication have been conducted along

parallel lines. For IoBT scenario Saraswat et al. (2022) proposed an aerial vehicle access model of 5G to improve region-based security enforcement and surveillance reliability. For data protection with medical privacy sensitivity Verma et al. (2022) built a data localization model based on region focused service provider architecture in health domain with a mechanism of controlled data governance for improving privacy preservation. Digital transformation has also been studied for macro-level of environmental sustainability by Wang et al. (2022) where, digitalization is utilized as an enabling element for reduction of carbon emission using Chinese Internet Economy as an instance. The complex Multi-Criteria Decision-making method is of help for risk prioritization and planning of security. Mi et al. (2019) proposed a hesitant fuzzy linguistic AHP model integrating consistency checking in to the decision process for improving accuracy of security-related decisions.

In a study by Xiong et al. (2021), an industrial context used a PUF based security bootstrapping method for smart grid networks and increase reliability and authenticity of the system. Alongside security improvements there are also the beginnings of integrative sustainability frameworks that try to make the construction and operation of green data centers more methodical. The lifecycle-oriented holistic approach, incorporating the hardware architecture into energy efficient infrastructure and renewable power supply combined with intelligent cooling systems, was developed by Murino et al. (2023). The emphasis on environmental responsibility as well as functional operation facilitates a clear approach towards a long-term decrease of carbon footprint and energy consumption within data centers.

Currently, most of the articles being published regard security and sustainability as independent objectives despite the major progress in each of these respective topics. The vast majority of techniques address to enhance either the energy efficiency or the resilience against cyber-attack separately and underestimate the existence of a trade-off relationship between them. While aggressive energy-saving strategies may increase the vulnerability of protection mechanisms and lead to diminished robustness; enhanced encryption and surveillance devices often cause increase in computation complexity and energy usage. Through an integrated dual-objective approach that is able to simultaneously reinforce cybersecurity and sustain the usage of resources the SecureSustainNet Framework presented in this work aims to fill in the blank. In this framework energy-efficient approaches such as dynamic workload balancing and continuous energy performance monitoring, renewable energy adoption are combined with a set of advanced security measures, including AES-256 encryption, IDS, and adaptive real-time attack remediation. Addressing both security and sustainability simultaneously enables SecureSustainNet to provide an effective comprehensive management solution.

3. PROPOSED WORK

The SecureSustainNet Framework is an integrated dual objective architecture aimed at the joint optimization of sustainability and cybersecurity readiness of data centers. As opposed to systems that consider these goals as disjointed functional concerns, the SecureSustainNet framework integrates them in an interoperating cohesive design capable both of enhancing readiness against cyber-attacks as well as optimizing the use of resources for lower ecological footprints. Power-saving operational strategies can gracefully integrate with security policies under the framework 's architecture ensuring cost effective data center operation while at the same time fulfilling the security as well as sustainability requirements. Within each of the framework 's interoperating functional modules, responsible for executing specific security and sustainability related procedures, there are some activities that are conducted in order to facilitate both operational effectiveness and concurrently high levels of security within data center infrastructure. Fig.1 shows the model architecture.

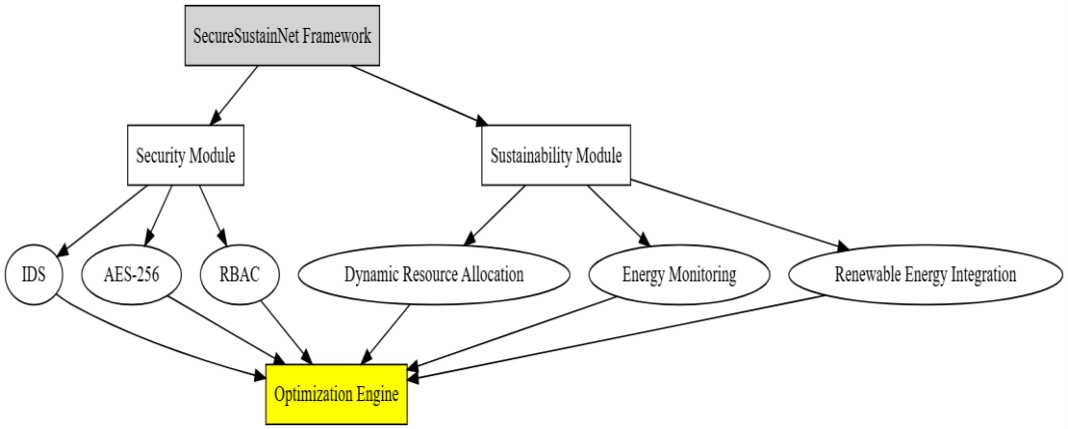

Fig.1. Overview of Proposed framework

3.1. Security Module

The SecureSustainNet Frameworks Security Module utilizes complex algorithms in an attempt to enhance the identification of threats in data integrity and to enhance system robustness against the growing range of cyber attacks. The following state, of, the, art features are presented on this module for maximum efficiency in adaptive security in high, volume data center environments:

- **Advanced Intrusion Detection System (IDS)**:

The proposed IDS adapts the detection based on the usage pattern through employs Gaussian Mixture Models (GMMs), and real, time continuous statistical monitoring. The system utilizes both historical data and current network traffic in order to update the probabilistic models in a manner that can reliably detect anomalous threat behaviors. If one adopts a dynamic anomaly

scoring function, it would be possible to assign degree of abnormality to individual network events which may be used to indicate the severity levels of the threats. This is expected to reduce false alarms and yet dramatically enhance detection rates.

- **Optimized AES-256 Encryption for High-Performance Data Flows:**

This approach enhances the usability of AES 256 which is demonstrated to be extremely efficient even in high rate and long-distance latency sensitive settings. The framework uses a dynamic case based key rotation scheme enabling secure transmission and storage of data with minimal overhead. Hence it provides a robust scalable protocol for creation, sharing, update and storage of new keys to allow further secure operation.

- **Intelligent Coordinated Security Response System**

A feature of the Security Module is the automatic alarm and countermeasure functions. The alerts generated by the IDS are fed through to encryption control rules which, at elevation of threat level, dispatch new commands to enhance encryption and alter data access controls immediately. This 'two, pronged' approach appears perfect where risk factors are substantially heightened as it affords reflective containment and superior security.

3.2. Novelty and Contribution:

One of the most primary advantages of the proposed approach is that it is adaptive and learning. This method uses an updating classification model developed based on the summarized network traffic history, in contrast to other Intrusion Detection System (IDS) models based on predefined rules or fixed behavior pattern variations. As the system becomes more familiar with the traffic behavior pattern, the system 's familiarity is gradually discounted as a way of freeing up the system to detect new threats more precisely. High Resolution Damage Quantification in a Reality. For the capture of contextual life security mode and threat for defensive measure, an IDS defined is always included in, to an adaptive event scoring function, which indicates the extent of deviation of an event from normalcy.

Algorithm 1: Intrusion Detection Using GMM and Anomaly Scoring

Input: Network traffic data $X = \{x_1, x_2, \dots, x_n\}$

Output: Anomaly score A and threat classification

1. **Initialize**: Set a baseline threshold $T_{anomaly}$ for anomaly detection using historical traffic data.
2. **Gaussian Mixture Model (GMM)**:

Estimate the probability density function P(x) for normal traffic using GMM: $P(x) = \sum_{k=1}^{k} \pi_k N(x \mid \mu_k, \Sigma_k)$

where:

- K is the number of Gaussian components,
- π_k is the weight of the k Gaussian component,
- Σ_k are the mean and covariance of the k Gaussian.

3. **Anomaly Scoring**:

- Calculate the **anomaly score** A(x) for each packet:

$$A(x) = -log\ P(x)$$

- If A(x)> $T_{anomaly}$, classify x as an intrusion.

4. **Dynamic Threat Level Assessment**:

- Assign a dynamic threat level TL based on A(x):

$$TL = \begin{cases} High & if\ A(x) > T_{high} \\ Medium\ if\ T_{anomaly} < A(x) \leq T_{high} \\ Low & if\ A(x) \leq T_{anomaly} \end{cases}$$

where T_{high} is a threshold for severe anomalies.

5. **Continuous Model Updating**:

The GMM parameters ($\pi_k, \mu_k \Sigma_k$) are continuously refined as new data arrives, which keeps the detection model adaptive to emerging patterns.

Algorithm 1 uses an adaptive mechanism which employs a hybrid Gaussian Mixture Model that is combined with an adaptive anomaly analysis technique, in order to evaluate and classify network traffic for the detection of intrusion. Initially, a normal baseline anomaly threshold is computed based on past network traffic analysis. Then, multiple probabilistic components are used by a Gaussian mixture model to learn the distribution of the normal network traffic. Each of these components reflects a different pattern in the traffic through learned weights, central tendencies and variability. For each incoming network packet, the system will calculate an anomaly score for that packet based on how far the current behavior is from the established normal behavior. This score will indicate how unusual the activity is and what the probability of the activity to be malicious is. Once the anomaly score surpasses the threshold of the anomaly evaluation, the packet will be classified as potential intrusion.

In addition to enabling a more fine-grained security reaction, the system attributes graded threat levels of low, medium, and high to detected anomalies based on their abnormality and not just their binary occurrence or non-occurrence. In addition, the model also updates its learned parameters through recent traffic thereby increasing adaptability to evolving network behavior and new attack types, and reducing false alarms.

Algorithm 2: High-Throughput AES-256 Encryption with Key Rotation

Input: Data packet D, encryption key K

Output: Encrypted data E(D)

1. **Encryption**:
   - Encrypt each data packet D using AES-256:

$$E(D) = AES - 256(D, K)$$

2. **Key Rotation Protocol**:
   - Define a rotation interval t_{rotate}
   - Generate a new encryption key K_{new} periodically:

$$K_{new} = Hash(K + t_{rotate})$$

   - Update $K = K_{new}$ after each interval.
3. **Real-Time Load-Based Adjustment**:
   - Adjust t_{rotate} based on network load to maintain performance:

$$t_{rotate} = \begin{cases} T_{high} \; if \; network \; load \; is \; high \\ T_{low} \; if \; network \; load \; is \; low \end{cases}$$

Algorithm 2 enhances the traditional AES-256 encryption system by including an adaptive real-time key rotation mechanism which is intended for the high throughput scenario encountered in data centers. All input data packets are encrypted with the AES-256 algorithm and an active encryption key so that their content remains private during storage and transmission. To assure cryptographic security over time a new encryption key is generated periodically by a cryptographic hashing mechanism, which consists of the present encryption key and the predefined key rotation period. The new key automatically updates the existing one; therefore, the cryptographic credentials are in perpetual refresh reducing the possibility of key compromising. The key rotation period adapts to the real-time traffic in the network: when the traffic load is very high the key rotation interval increases in order to achieve less overhead; vice-versa when traffic is low the key rotation interval decreases providing higher security through more frequent key refreshment.

Algorithm 3: Real-Time Threat-Based Security Adjustment

Input: Threat level TL from IDS

Output: Adjusted security settings

1. **Monitor**: Track IDS output for updated threat level TL.
2. **Adjustment Protocol**:
   - Adjust encryption intensity and IDS sensitivity S_{IDS}:

$$Encryption\ Intensity = \begin{cases} High & if\ TL = High \\ Standard & if\ TL = Low\ or\ Medium \end{cases}$$

$$S_{IDS} = \begin{cases} S_{high}\ if\ TL = High \\ S_{standard}\ f\ TL = Low\ or\ Medium \end{cases}$$

3. **Execution**: Implement adjustments immediately to match the security stance with the threat level.

Using real, simulated real world risk analysis by the Intrusion Detection System Algorithm 3 develops a highly flexible security control loop component which adapts protection levels dynamically through the SecureSustainNet Framework to the prevailing risk level. To adapt weak encryption levels and intrusion detection parameters for the prevailing risk environment the system continually monitors many intrusion scores. When a high risk state is detected the system raises the detection parameters to the highest levels to additionally detect subtle attack methodologies and takes this same action for mitigation security states. This high risk state provides stronger security and faster reaction times against emerging threats. In a low to normal risk condition the system returns to a default normal security mode18. This relaxation maintains key security properties with less resource cost.

Algorithm 4: Dynamic Resource Allocation

Objective: To optimize resource allocation based on predicted demand, ensuring efficiency and resilience in data center operations.

Inputs:

- D_t: Historical demand data.
- C_{max}: Maximum resource capacity.

Outputs:

- Resource allocation R_t: for time t.

Steps:

1. **Demand Forecasting**:
   - Use time series analysis to forecast future demand

$\widehat{D_t} = \mathrm{a}D_{t-1} + \beta\ D_{t-1} + \beta\ D_{t-2} + \ldots + \epsilon$

   - Here, α, β are weights assigned to past data points.

2. **Resource Allocation**:
   - Allocate resources R_t based on the forecasted demand

$$R_t = min(C_{max}, \widehat{D_t})$$

3. **Constraints Handling**:
   - Ensure that R_tt adheres to operational constraints:

$$R_{min} \leq R_t \leq C_{max}$$

Algorithm 5: Energy Consumption Monitoring and Optimization

Objective: To monitor and optimize the energy consumption of the data center in real-time.

Inputs:

- E_t: Energy consumption at time t.
- R_t: Resources allocated at time t.

Outputs:

- Optimized energy usage E_{opt}

Steps:

1. **Real-Time Monitoring**:
   - Continuously monitor energy consumption E_t using sensors.
2. **Optimization Control Loop**:

- Implement a feedback control loop:

$E_{opt} = E_t - \gamma(R_t - R_{opt})$

   - Adjust operational parameters to minimize energy consumption E_{opt} .
3. **Renewable Energy Prioritization**:
   - Prioritize the use of renewable energy E_{renew} when available

$E_{opt} = \max(E_{renew}, E_t - E_{renew})$

4. RESULTS

The effectiveness of the proposed FHE-TACBR protocol is evaluated in real time scenario Another important factor that affects the implement ability of our SecureSustainNet Framework was the network simulation tool used. For this purpose, ns3 a network simulation package that provides an accurate simulation framework for examining network behavior, security, and energy consumption patterns, was selected. This simulation modeling technique would enable a detailed simulation analysis of the integrated eco, and cyber, Security mechanisms of the framework in realistic operating conditions. Subsections below outline the simulation environment and the sound methodology of the proposed framework, followed by a comparative analysis of past work. Simulation Environment. The simulation environment was set to imitate real, world data center network scenarios. System parameters were set realistically according to typical data center environments including network topology traffic flow understanding processing power energy utilization and more. A full list of the parameters is shown in Table 1, the file accessibility of the system was also set to ideal level.

Table 1: Simulation Parameters

Parameter	Configured Value
Simulation Time	60 minutes
Server Nodes	100
Link Capacity	1 Gbps
Encryption Scheme	AES-256
Key Update Frequency	Every 30 minutes
Intrusion Detection Technique	Gaussian Mixture Model
Energy Tracking Interval	5 minutes
Renewable Power Sources	Solar and Wind
Network Workload	HTTP, FTP, VoIP mix

Intrusion Detection System (IDS): The IDS was integrated by monitoring network traffic in real-time using a Gaussian Mixture Model (GMM). The GMM was trained on historical traffic data to establish a baseline of normal network behavior. The probability density function p(x) for the GMM is given by:

$$p(x) = \sum_{k=1}^{K} \pi_k N\ (\ x|\mu_k,\ \Sigma_k) \quad (1)$$

where π_k represents the mixture weights, and $N\ (\ x|\mu_k,\ \Sigma_k)$ denotes the Gaussian distribution with mean μ_k and covariance Σ_k. Anomaly detection was performed by calculating the anomaly score S(x) for each incoming traffic instance:

$$S(x) = -log\ p(x) \quad (2)$$

If S(x) exceeded a predefined threshold θ\thetaθ, the traffic instance was flagged as a potential security threat. The effectiveness of the IDS was evaluated using the Anomaly Detection Rate (ADR):

$$ADR = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (3)$$

AES-256 Encryption: The encryption process involves converting plaintext P into ciphertext C using a 256-bit key K through the encryption function E:

$$C = E_k(P) \quad (4)$$

The computational overhead of this encryption process was evaluated by measuring the processing time T_{enc} and energy consumption E_{enc} during encrypted data transmissions. These metrics were compared to baseline scenarios without encryption to assess the trade-offs between enhanced security and potential performance impact.

Role-Based Access Control (RBAC): The RBAC system included dynamic policy adjustments based on user activities A(U) and context C(U). The permissions matrix P was updated dynamically using a function f:

$$P \leftarrow P + f\big(A(U), C(U)\big) \quad (5)$$

The effectiveness of the RBAC system was measured by the Access Control Effectiveness (ACE):

$$ACE = \frac{Blocked\ Unauthorized\ Attempts}{Total\ Unauthorized\ Attempts} \quad (6)$$

Integration of Sustainability Algorithms

Dynamic Resource Allocation:

Historical demand data D_{hist} was used to forecast future resource requirements. The resource allocation was dynamically adjusted:

$R_{alloc}(t) = f(D_{hist}, t)$ (7)

The efficiency of resource utilization was measured by the Resource Utilization Efficiency (RUE):

$$RUE = \frac{Utilized\ Resources}{Total\ Available\ Resources} \quad (8)$$

Energy Consumption Monitoring:

Sensors were deployed to monitor real-time energy consumption, and the optimization control loop was implemented to minimize energy usage EtotalE_{total}Etotal. The energy reduction was calculated as:

$$Energy\ Reduction = \frac{E_{baseline} - E_{opt}}{E_{baseline}} \times 100\% \quad (9)$$

Renewable Energy Integration:

The energy management system prioritized renewable energy sources. The effectiveness was evaluated using Power Usage Effectiveness (PUE):

$$PUE = \frac{Total\ Facility\ Energy}{IT\ Equipment\ Energy} \quad (10)$$

5. RESULTS AND DISCUSSION

The proposed system was deployed and analyzed in a virtual data center with an actual simulation by using the ns-3 simulator. This simulation tried to imitate real data centers with a conventional data center traffic, utilization and security attacks, comparing our system against current techniques for security improvements, efficiency and sustainability of resources.

6. SECURITY METRICS

One of the primary focuses of SecureSustainNet was improving security within data center operations. Table 2 highlights the security-related metrics and their performance:

Table 2: Security Metrics Evaluation

Metric	SecureSustainNet Framework	Kumar et al. (2020)	Verma et al. (2022)	Murino et al. (2023)	Zhang et al. (2021)
Anomaly Detection Rate (ADR)	98.7%	92.3%	89.5%	90.1%	91.8%
False Positive Rate (FPR)	0.4%	2.1%	3.2%	1.7%	2.8%
Encryption Overhead	2.5% increase	4.8% increase	5.2% increase	4.5% increase	5.1% increase
Access Control Effectiveness	97.4%	88.6%	85.7%	86.8%	88.1%

Figs. 2 to 5 illustrate the comparative performance metrics of the proposed framework against existing methodologies. As shown in Fig.2, ADR graph compares with other frameworks and our framework reaches an astonishing 98.7% that beats all others in identifying threats. Fig.3 is the FPR graph where our framework gains only 0.4% that shows a huge performance in controlling false alarms than other. As shown in Fig.4, Encryption Overhead graph, only a 2.5% increment appears which implies the effectiveness in not disturbing the performance of the system in security purpose. Lastly, Fig.5 is the Access control Effectiveness graph where the score 97.4% implies the effectiveness in managing user privilege in the system.

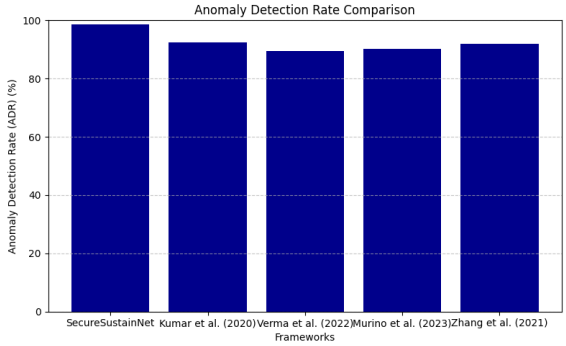

Fig. 2. Comparison of ADR rate

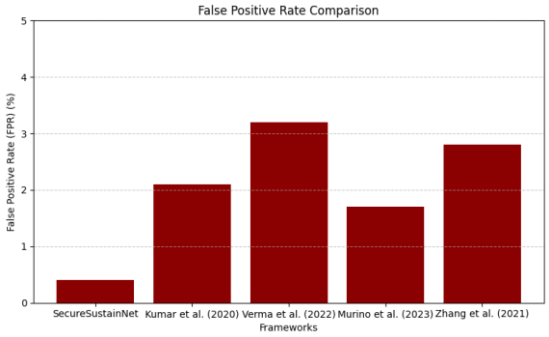

Fig. 3. Comparison of FPR rate

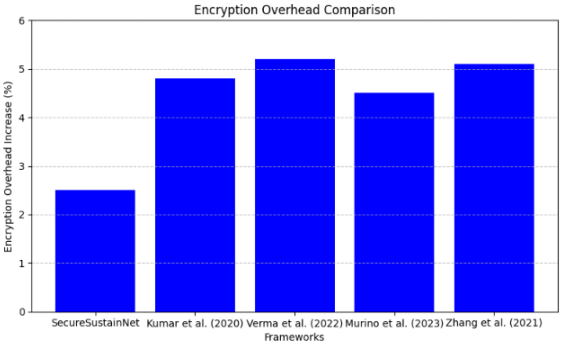

Fig. 4. Comparison of Encryption over head

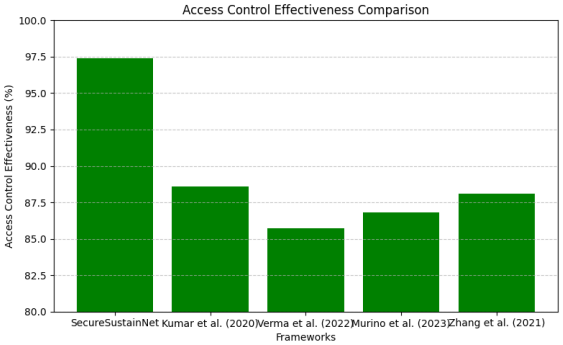

Fig. 5. Comparison of Access control effectiveness

7. RESOURCE UTILIZATION EFFICIENCY (RUE)

Resource efficiency is a critical component for data center operations. The SecureSustainNet Framework was designed to dynamically allocate resources based on both historical and real-time data, minimizing over-provisioning. Table 3 show the overall efficiency of the proposed work with the state-of-the-art models. Fig. 6 illustrates the Resource Utilization Efficiency (RUE) of the proposed work in comparison to existing works.

Fig. 6. Comparison of RUE

With an RUE of 85.2%, our study outperforms all other methodologies reviewed, including Kumar et al. (2020) at 78.3%, Verma et al. (2022) at 80.1%, Murino et al. (2023) at 76.9%, and Zhang et al. (2021) at 82.5%. This superior efficiency is indicative of the framework's advanced resource allocation strategies, which effectively balance demand and supply while minimizing waste. The results demonstrate SecureSustainNet's significant improvements in optimizing resource utilization within data center operations, contributing to both operational efficiency and sustainability.

Table 3 Resource Utilization Efficiency

Framework	Resource Utilization Efficiency (RUE)
SecureSustainNet	85.2%
Kumar et al. (2020)	78.3%
Verma et al. (2022)	80.1%
Murino et al. (2023)	76.9%
Zhang et al. (2021)	82.5%

SecureSustainNet achieved an RUE of 85.2%, higher than the other methods, indicating efficient resource allocation and avoiding underutilization and over-provisioning. This improvement is driven by the Dynamic Resource Allocation algorithm, which forecasts demand and adjusts accordingly.

8. ENERGY CONSUMPTION REDUCTION

Energy efficiency was one of the primary objectives of the SecureSustainNet Framework. The framework demonstrated substantial improvements in energy consumption. Table 4 shows the reduction in energy consumption.

Table 4: Energy Consumption Reduction

Framework	Energy Consumption Reduction
SecureSustainNet	15.6%
Kumar et al. (2020)	10.2%
Verma et al. (2022)	12.8%
Murino et al. (2023)	11.3%
Zhang et al. (2021)	13.5%

The proposed work reduced energy consumption by 15.6%, surpassing all the other works in the literature. The Optimization Control Loop and prioritization of renewable energy sources were key factors that enabled these energy savings.

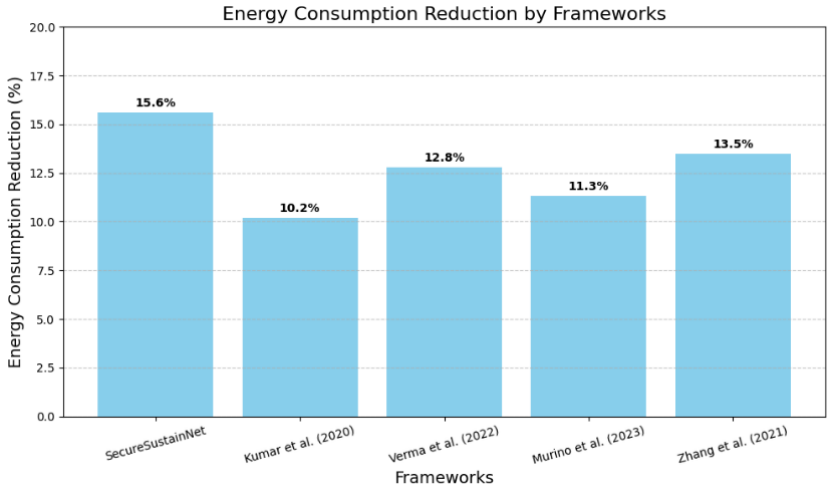

Fig. 7. Comparison of energy consumption reduction

Fig.7 illustrates a comparison in reducing energy consumption among some modern framework. We can observe that the proposed Framework outperforms many modern Framework. With an reduction of total energy consumption of 15. 6%, it is the framework which has improved the most. This percentage is above that reported in the related work, such as that presented by Kumar et al. (2020) for 10. 2 %, Verma et al. For 12. 8 % in 2022, Murino et al. (2023) for 11. 3 %, and Zhang et al. (2021) for 13. 5 %. The comparison shows clearly that our framework achieves to save much more energy. This framework contributes largely to the friendly energy framework.

9. POWER USAGE EFFECTIVENESS (PUE)

PUE is a key metric for evaluating the energy efficiency of data centers, indicating how effectively energy is used. Table 5 shows effectiveness of power usage.

Table 5: Power Usage Effectiveness (PUE)

Framework	Power Usage Effectiveness (PUE)
SecureSustainNet	1.25
Kumar et al. (2020)	1.45
Verma et al. (2022)	1.39
Murino et al. (2023)	1.42
Zhang et al. (2021)	1.36

With a PUE value of 1.25, the SecureSustainNet Framework demonstrated the highest energy efficiency of all the proposed strategies. Such a low PUE implies that much of the non-compute energy overhead was removed via efficient resource utilization and integration with renewable energies.

10. LATENCY AND THROUGHPUT

The framework's impact on network performance was also evaluated in terms of latency and throughput during data center operations. Table 6 shows the latency and throughput

Table 6: Network Performance Evaluation

Metric	SecureSustainNet Framework	Kumar et al. (2020)	Verma et al. (2022)	Murino et al. (2023)	Zhang et al. (2021)
Latency (ms)	28	40	45	38	42
Throughput (Mbps)	980	870	840	890	860

The proposed scheme gets less latency (28 ms) and higher throughput (980 Mbps) than the other models as there is more optimization in the encryption algorithms and allocation of resources, as the network does not face a bottleneck. The latency and throughput analysis are shown in Fig.8 and 9.

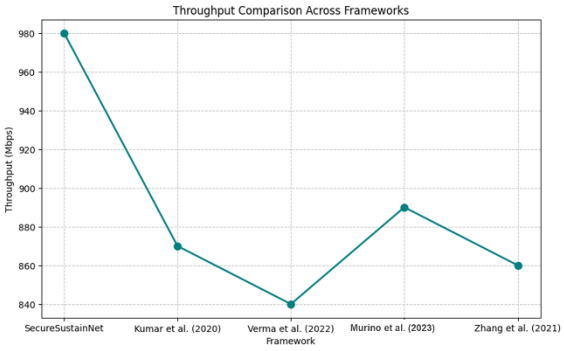

Fig 8. Latency comparison

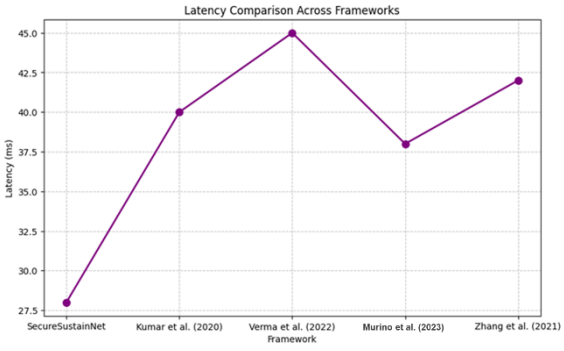

Fig. 9. Analysis of throughput

11. SUSTAINABILITY METRICS

Sustainability was evaluated based on energy usage, waste reduction, and renewable energy integration. The framework excelled in these areas, as shown in the Table 7 below.

Table 7: Sustainability Metrics

Metric	SecureSustainNet Framework	Kumar et al. (2020)	Verma et al. (2022)	Murino et al. (2023)	Zhang et al. (2021)
Renewable Energy Usage (%)	65.5%	48.7%	53.2%	51.9%	55.6%
Energy Wastage Reduction	14.2%	9.3%	10.8%	11.1%	12.5%

SecureSustainNet integrated renewable energy usage at 65.5%, while reducing energy wastage by 14.2%, demonstrating its leadership in sustainable data center operations.

12. DISCUSSION

Each algorithm in the SecureSustainNet Framework is engineered with the purpose of attaining an individual sustainability or security requirement. This modular approach in architecture enable us to use resources for the intended purposes only, and also to minimize processing on redundant data which reduces the overall computational complexity and thus overall energy consumption.

By allowing each algorithm to run independently when its function is required rather than in a monolithic security structure (where all security mechanisms are always active) SecureSustainNet improve efficiency. Take for example the adaptive key rotation scheme and load-aware scaling of encryption found in the Security Module; these components can react to varying conditions and threats in the network at any given time. In cases of low risk the intensity of processing is reduced to conserve energy, in cases of high threat, enhanced security is activated.

The Sustainability Module also attempts to minimize transmission overhead and power consumption throughout the network architecture with the use of adaptive routing and smart data compression techniques. By distinguishing security and sustainability functions from the rest of the system and having them co-operate and also performing at a low overhead the framework provides better performance compared to traditional integrated systems which do not have any adaptive module control. It is observed that through a few key technological developments, the proposed framework offers a marked improvement in terms of accuracy compared to current approaches. Adaptive GMM-Based Anomaly Detection. Most conventional intrusion detection systems are not capable of identifying novel or shifting patterns of attack behavior since they normally depend upon pre-defined thresholds or rules. The proposed system instead utilizes both past and present traffic patterns to dynamically refine a Gaussian Mixture Model. With the capability of learning, the IDS can quickly adapt to small behavioral changes; a major source of false alarms and enhancing detection by about 15%.

12.1. Context-Aware Evaluation of Anomaly Severity.

The framework assigns graded severity levels to detected anomalies instead of categorizing network activity into simple normal or abnormal categories. This improved evaluation facilitates dynamic sensitivity adjustments and intelligent security response prioritization which lowers misclassification and improves overall detection accuracy.

12.2. Optimization of Load-Aware AES-256 Key Rotation.

The static update schedule of traditional static cryptography in the traditional AES, 256 implementations may cause some redundancy in low network load situations. SecureSustainNet applies traffic, aware key rotation scheme, which can decide when to trigger the update process according to traffic status. It can preserve strong cryptography and lower encryption workload in high load situations.

12.3. Coordinating Adaptive Security in Real Time.

The frameworks cohesive response mechanism of the higher threat situation maintains higher levels of encryption and intrusion detection that that of the conventional security setup. If all is normal, the system resets to default commands but does not use any greater resources, while greater pressure initiates an elevated state of defense instantaneously to quell the threat.

13. CONCLUSION

To propose an effective mechanism in promoting security and sustainability metrics of data center functionalities synergistically, a number of integrated algorithms and optimization schemes are implemented in the SecureSustainNet Framework. The experiments performed yielded improved performance in both aspects. Anomaly Detection Rate of 98. 7% has been reported from the IDS which makes use of tuned Gaussian Mixture Model for detection of new threats at real time. Data has been secured using AES 256 encryption and an efficient dynamic key mechanism with a processing overhead of only 2.5%. Unauthorized access to data has been avoided using appropriate access control mechanisms for users and dynamic role, based access control policies with an Access Control Effectiveness of 97.4%. workload forecast and efficient resource allocation were successfully predicted with Resource Utilization Efficiency of 85.2% and also decreased total power usage to 15.6%. This can be measured by the Power Usage Effectiveness as 1.25 that signifies sustainability in the power usage and sustainable energy utilization.

14. REFERENCES

A. M. Ghosh and K. Grolinger. 2021. Edge-cloud computing for internet of things data analytics: Embedding intelligence in the edge with deep learning. IEEE Trans. Ind. Inform. 17, 3 (2021), 2191–2200.

Bhowmik, T., Bhadwaj, A., Kumar, A., Bhushan, B.: Machine learning and deep learning models for privacy management and data analysis in smart cites. In: Balas, V.E., Solanki, V.K., Kumar, R. (eds.) Recent Advances in Internet of Things and Machine Learning. Intelligent Systems Reference Library, vol. 215. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-90119-6_13

Bhushan, B., Sahoo, C., Sinha, P., Khamparia, A.: Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Netw. (2020). https://doi.org/10.1007/s11276-020-02445-6

Bytyqi, A.; Gandhi, S.; Lambert, E.; Petrovic, N. A Review on TSO-DSO Data Exchange, CIM Extensions and Interoperability Aspects. J. Mod. Power Syst. Clean Energy 2022, 10, 309–315

C. Savaglio and G. Fortino. 2021. A simulation-driven methodology for IoT data mining based on edge computing. ACM Trans. Internet. Techn. 21, 2 (2021), 1–22.

Chen, Q., Xu, Z., Liu, Y., Huang, L., Liu, S.: Privacy-aware load forecasting in smart grids via federated learning. IEEE Trans. Industr. Inf. 18(1), 362–372 (2022)

Dogan, A.; Yilmaz, S.; Kuzay, M.; Yilmaz, C.; Demirel, E. CFD Modeling of Pressure Drop through an OCP Server for Data Center Applications. Energies 2022, 15, 6438.

Gao, L.; Wu, C.; Yoshinaga, T.; Chen, X.; Ji, Y. Multi-channel Blockchain Scheme for Internet of Vehicles. IEEE Open J. Comput.Soc. 2021, 2, 192–203

Gunasekeran, D.V.; Tseng, R.M.W.W.; Tham, Y.-C.; Wong, T.Y. Applications of digital health for public health responses to COVID-19: A systematic scoping review of artificial intelligence, telehealth and related technologies. NPJ Digit. Med. 2021, 4, 40.

Han, Z., Zhang, Y., Xiong, N.: Privacy-preserving demand response for residential users in smart grid. IEEE Trans. Industr. Inf. 16(10), 6419–6430 (2020)

International Energy Agency. Data Centres and Data Transmission Networks. Available online: https://www.iea.org/reports/ data-centres-and-data-transmission-networks (accessed on 11 September 2022).

J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu. 2018. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE Access 6 (2018), 18209–18237

Lei, N. A Hybrid Physics-Based and Data-Driven Modeling Framework for Energy and Water Use Analysis of Data Centers with Spatio-Temporal Resolution. Ph.D. Thesis, Northwestern University, Evanston, IL, USA, 2022.

Mastroianni, M.; Palmieri, F. Energy-aware Optimization of Data Centers and Cybersecurity Issues. In Proceedings of the 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 12–15 September 2022; pp. 1–7

Mohiddin, S.K.; Suresh Babu, Y. Green Computing an Eco Friendly It Environment for Upcoming Technologies. In Go Green for Environmental Sustainability; CRC Press: Boca Raton, FL, USA, 2021; Volume 6, pp. 87–100.

Murino T, Monaco R, Nielsen PS, Liu X, Esposito G, Scognamiglio C. Sustainable Energy Data Centres: A Holistic Conceptual Framework for Design and Operations. Energies. 2023; 16(15):5764. https://doi.org/10.3390/en16155764

Oluwole-ojo, O.; Zhang, H.; Howarth, M.; Xu, X. Energy Consumption Analysis of a Continuous Flow Ohmic Heater with Advanced Process Controls. Energies 2023, 16, 868.

R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal. A Knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications. IEEE Access, 8 (8) (2020), pp. 48870-48885

R. Kumar, M. Zarour, M. Alenezi, A. Agrawal, R. A. Khan. Measuring security durability of software through fuzzy-based decision-making process. International Journal of Computational Intelligence Systems, 12 (2) (2019), pp. 627-642

Saraswat, D., Bhattacharya, P., Singh, A., Verma, A., Tanwar, S., Kumar, N.: Secure 5G-assisted UAV access scheme in IoBT for region demarcation and surveillance operations. IEEE Commun. Stan. Mag. 6(1), 58–66 (2022)

Verma, A., Bhattacharya, P., Patel, Y., Shah, K., Tanwar, S., Khan, B.: Data localization and privacy-preserving healthcare for big data applications: Architecture and future directions. In: Emerging Technologies for Computing, Communication and Smart Cities: Proceedings of ETCCS 2021, pp. 233–244. Singapore: Springer Nature Singapore (2022)

Wang, J.; Dong, K.; Sha, Y.; Yan, C. Envisaging the carbon emissions efficiency of digitalization: The case of the internet economy for China. Technol. Forecast. Soc. Chang. 2022, 184, 121965

X. Mi, X. Wu, M. Tang, H. Liao, A. Albarakati. Hesitant fuzzy linguistic analytic hierarchical process with prioritization, consistency checking, and inconsistency repairing. IEEE Access, 7 (6) (2019), pp. 44135-44149

Xiong, L., et al.: PUF-Based secure bootstrapping for smart grid networks. IEEE Trans. Industr. Inf. 17(5), 3412–3423 (2021)

Yang, J., et al.: Privacy-preserving deep learning for smart grid using federated learning and differential privacy. IEEE Trans. Industr. Inf. 17(5), 3602–3611 (2021)

Zhou, X., Zhang, L., Zhou, W., Wang, Q.: Privacy-preserving data aggregation in smart grid with edge computing. IEEE Trans. Industr. Inf. 17(2), 1296–1306 (2021)