

An AI-Driven Digital Twin Approach for Multi-Objective Data Center Security and Sustainability Optimization

Abstract --- An AI-enabled Digital Twin framework is proposed for joint optimization of data center security and sustainability in dynamic operational environment. The proposed approach constructs a virtual representation of the data center by combining operational parameters such as energy consumption, temperature, workload, utilization of resources, and security events. Artificial intelligence is used to continuously update and analyze the Digital Twin to find operating configurations that meet multiple objectives such as reducing energy and carbon emissions while reducing security threats and maintaining system performance. Data center operational and security data are used to conduct experimental evaluation under different workload levels and simulated security threat circumstances. The suggested framework is compared with traditional optimization techniques and assessed using energy consumption, carbon emissions, security risk, resource utilization, and performance as key variables. The findings of the experiment show that the proposed framework can dynamically balance security and sustainability goals, resulting in increased energy efficiency and decreased security risk while preserving dependable data center operation.

Keywords: Artificial Intelligence, Digital Twin, Data Center Security, Sustainability Optimization, Multi-Objective Optimization, Energy Efficiency, Resource Utilization

1. INTRODUCTION

Large-scale digital services, cloud computing, and artificial intelligence all depend on data centers, but growing workloads raise issues with resource usage, energy consumption, and operational effectiveness. A virtual depiction of data-center infrastructure is made possible by digital twin technology, which enables dynamic monitoring and optimization of operational circumstances. Recent experimental studies have shown how AI-enabled Digital Twins can be used for data-center energy optimization and energy-demand prediction [1]. But energy optimization might not be enough to guaranty safe and dependable data center operation.

1.1 Digital Twin for Energy and Resource Optimization

Studies have been undertaken into methods for enhancing energy efficiency in data centers by employing digital twins. Experimental research was performed on the digital twin models for energy-aware operation management and cooling optimization and it proved quantifiable reduction of energy consumption in various operation conditions [2,5]. By projecting future workload and energy requirements, AI-based prediction and optimization can further assist dynamic resource allocation. Although these methods provide approaches for data-center energy and resource management, their main emphasis is still on energy and resource efficiency rather than integrated security and sustainability.

1.2 Digital Twin for Security and Research Gap

Anomaly and intrusion detection are two further ways that digital twins have been used in cyber security. To detect malicious activity and security abnormalities, recent experimental research has combined Digital Twins with federated learning and machine-learning-based detection [3, 4]. These studies demonstrate the application of Digital Twins to security monitoring and anomaly detection.

To bridge this gap, the authors propose an AI-enabled Digital Twin system that combines predictive information about energy and resource demand with the capability of detecting security risk and multi-objective optimization. The Digital Twin considers energy consumption, carbon emissions,

security risk, resource efficiency, and operational efficiency in an integrated manner, thus allowing a data center to meet both the demands of sustainable energy and security in a volatile environment. The performance of the proposed approach is compared to established optimization techniques through experimentation.

2. LITERATURE REVIEW

Leindal et al. [6] presented a context-aware reinforcement learning algorithm for applying aquifer thermal energy systems in data-center cooling operations. Demonstrating its PPO-based approach through experiments, the authors have proved its superiority in improving cooling management activities, thus indicating reinforcement learning's potential for dynamic energy management. Taheri et al. [7], suggests DyTwin, a Digital Twin framework for data-center Surveillance and Anomaly Detection. Through testing, the results revealed that the proposed model can show anomalies and provide solutions for data-center management.

Mutawa and Tolba [8], came up with a different Digital Twin-based approach and proposed a monitoring solution that utilizes sensor data alongside an Extreme Learning Machine. The results claim that the algorithm has good performance when it comes to detection.

3. METHODOLOGY

The proposed system employs Digital Twin technology, time prediction, anomaly detection, and multi-objective optimization processes in managing a dynamic data center. The final system contains the following components: data acquisition, Digital Twin modelling, predictive AI capabilities, security functions, and optimization capabilities.

3.1 System Architecture

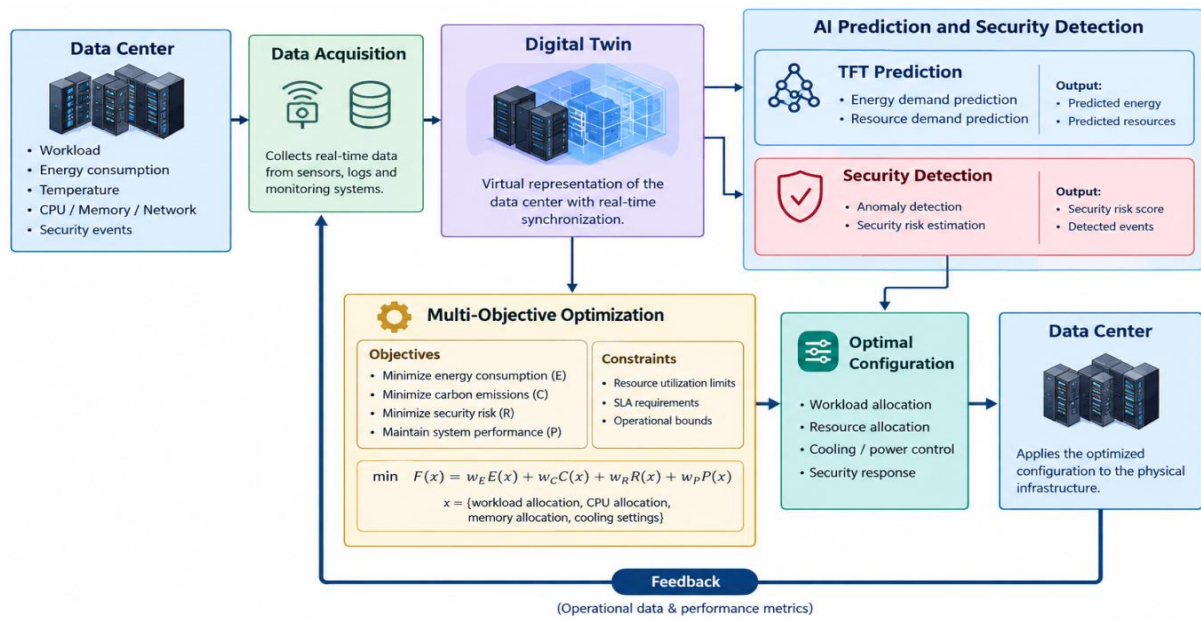


Figure 1. Proposed AI-Driven Digital Twin Architecture

The architecture of the system is composed of five separate stages. First, data is gathered in real-time from the data center regarding the workload, energy consumption, indoor temperatures, CPU and memory utilization, network activity, and security incidents. After that, all of these variables are

constantly synchronized with Digital Twin. The Digital Twin transmits the information to two artificial intelligence systems. First, the Temporal Fusion Transformer predicts the energy demand based on historical performance data. Second, there is a security detection system that monitors security incidents to identify potentially suspicious behaviors and calculate a security rating.

The data collected from the modules are imported to another system called the Multi-Objective Optimization (MOO) model. The MOO will have to study the entire situation and pick the best combination of energy consumption, environmental pollution, security risk, resource consumption and productivity to reach a possible operational layout. The solution is then deployed in the data center and the operational data are sent back to the Digital Twin for further adjustment.

3.2 AI Prediction and Security Detection

The TFT model is being used to forecast future consumption and resource requirement since it can model the effects of temporal dependencies. The effectiveness of the forecasting is evaluated with MAE (Mean Absolute Error) and RMSE (Root Mean Square Error). The security monitoring system is based on an auto encoder based anomaly detection system that detects any strange activities in the normal behaviour of a security system. The anomalies detected are assigned their risk levels in terms of security and are sent to the optimization module.

3.3 Multi-Objective Optimization

The optimizer module finds the data-center layout that reduces the energy consumption, carbon emissions, and safety risk while delivering performance levels.

We denote x as a possible data-center configuration where we have to include the workload distribution, CPU usage, memory appropriate distribution, as well as cooling system settings.

After we come up with configuration x , we calculate the following metrics related to it:

$E(x)$ = Energy Consumption

$C(x) = E(x) \times EF$

$R(x)$ = Security Risk Score

$P(x)$ = Performance Penalty

The combined optimization objective is:

$$\min F(x) = w_E E(x) + w_C C(x) + w_R R(x) + w_P P(x) \quad (1)$$

where w_E , w_C , w_R , w_P are the weights assigned to energy, carbon, security risk, and performance, respectively.

The optimizer searches for the configuration x^* that gives the minimum objective value:

$$x^* = \arg \min_x F(x) \quad (2)$$

The selected x^* represents the operating configuration used by the data center. Resource utilization and SLA requirements are included as constraints during optimization.

3.4 Evaluation Metrics

The approaches are compared using the following metrics:

Table 1: Key Evaluation Categories and Performance Metrics

Category	Metrics
Energy	Energy Consumption (kWh)
Sustainability	Carbon Emissions (kg CO ₂ e)
Security	Security Risk Score, Precision, Recall, F1-score, False Positive Rate
Prediction	MAE, RMSE
Resources	CPU, Memory Utilization
Performance	Response Time

The experimental findings enable assessment of the extent to which the proposed framework achieves an optimal balance between the various factors including energy efficiency, carbon reduction, security, resource utilization, and system performance in different workloads and security conditions.

4. RESULTS AND DISCUSSION

The suggested framework is assessed against standard optimization and the baseline method of DT + LSTM with different workload and security conditions. The output is produced by applying the same workload and security conditions to the approaches and calculating the energy, carbon, security, resource consumption, and performances metrics subsequently.

4.1 Generating Results

For every experimental time interval, the workload and other parameters are provided to the models used. The conventional method relies on the current state of the system, while DT + LSTM takes advantage of the Digital Twin and prediction based on LSTM. The presented method makes use of Digital Twin, TFT prediction, security detection, and multi-objective optimization.

The following metrics are calculated for experimental comparison.

Energy Consumption is calculated from the average power consumed over the operating time.

$$E = P \times t \quad (3)$$

Carbon Emissions are estimated from energy consumption and the corresponding emission factor.

$$C = E \times EF \quad (4)$$

Security Risk score represents the normalized severity of the detected security events, where a lower value indicates lower risk.

$$R = \frac{\sum_{i=1}^n S_i}{n \times S_{max}} \quad (5)$$

CPU Utilization represents the percentage of available processing capacity being used.

$$U_{CPU} = \frac{CPU_{used}}{CPU_{total}} \times 100 \quad (6)$$

Memory Utilization represents the percentage of total memory currently being utilized.

$$U_{Memory} = \frac{Memory_{used}}{Memory_{total}} \times 100 \quad (7)$$

Prediction Performance

Mean Absolute Error (MAE) measures the average difference between actual and predicted values, with lower values indicating better prediction accuracy.

$$MAE = \frac{1}{n} \sum_{i=1}^n |y_i - \hat{y}_i| \quad (8)$$

Root Mean Square Error (RMSE) measures prediction error while giving greater importance to larger errors.

$$RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2} \quad (9)$$

Security Detection Performance

Precision measures how accurately detected security events are classified as actual threats.

$$Precision = \frac{TP}{TP + FP} \quad (10)$$

Recall measures the ability of the security model to identify actual threats.

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

F1-Score provides a combined measure of Precision and Recall, with higher values indicating better detection performance.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (12)$$

False Positive Rate measures the proportion of normal events incorrectly identified as security threats.

$$FRP = \frac{FP}{FP + TN} \quad (13)$$

4.2 Overall Performance Comparison

All three approaches are assessed in terms of the same workload and security conditions. The framework presented utilizes predictive and security information prior to optimization in choosing the operating configuration of the system based on various targets.

Table 2: Performance Comparison Between Conventional, DT + LSTM, and Proposed Models

Metric	Conventional	DT + LSTM	Proposed
Energy Consumption (kWh) ↓	1280	1145	980
Carbon Emissions (kg CO ₂ e) ↓	576	515	441
Security Risk ↓	0.42	0.31	0.18
CPU Utilization (%)	71.2	68.5	66.8
Memory Utilization (%)	69.4	66.7	64.9
Response Time (ms) ↓	182	161	143

Table 2 compares important operational and performance parameters of three system methods. The proposed framework achieved lower energy consumption, carbon emissions, security risk, CPU utilization, memory utilization, and response time than both comparison methods under the evaluated conditions.

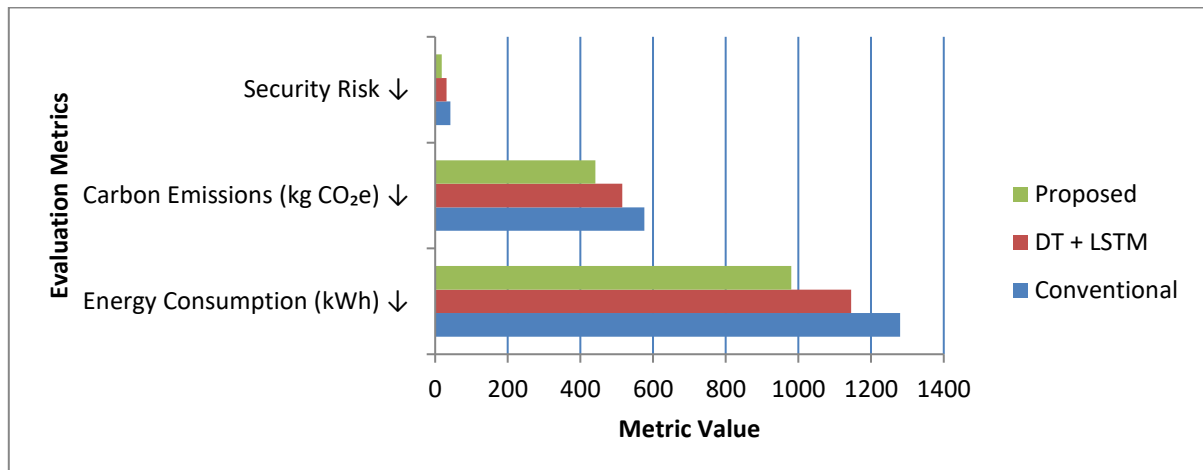


Figure 2. Sustainability and Security Performance Comparison

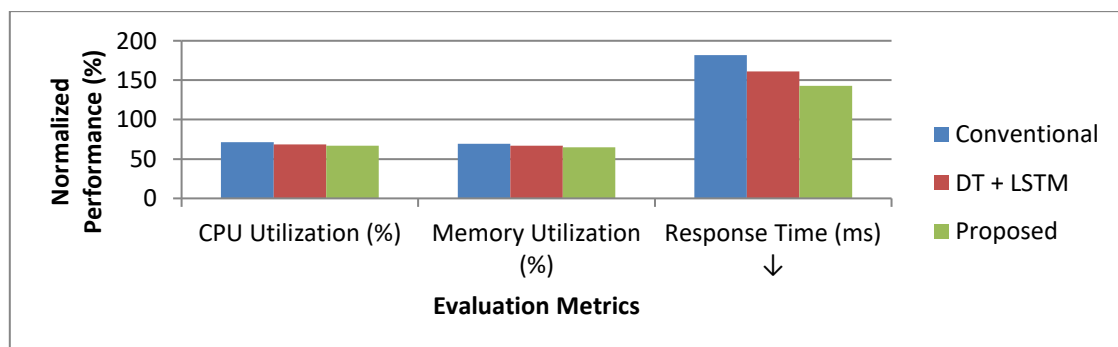


Figure 3. Resource Utilization and System Performance Comparison

The figure shows the overall outcome of the advances at the system level presented in normalized performance measures which facilitate evaluation of energy requirements, carbon footprint, risk of security breach, resources employed and response time.

4.3 Prediction and Security Detection Results

The prediction accuracy is judged on the basis of MAE and RMSE comparison of LSTM and TFT. The security detection accuracy is evaluated through metrics like Precision, Recall, F1 score, false positive ratio and detection latency.

Table 3: Model Performance Metrics

Model	MAE ↓	RMSE ↓	Precision ↑	Recall ↑	F1-score ↑	FPR ↓
LSTM + Security Baseline	0.184	0.247	89.1%	87.6%	88.3%	6.2%
TFT + Proposed Security Module	0.121	0.169	94.8%	93.5%	94.1%	3.1%

In table 3, the prediction accuracy and security detection metrics are compared and noted that the TFT-based configuration achieved higher precision, recall, and F1-score, together with lower MAE, RMSE, and false-positive rate than the LSTM-based baseline..

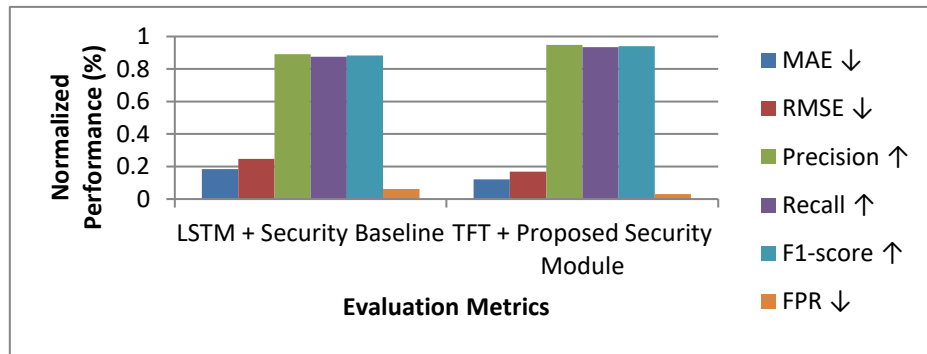


Figure 4. Prediction and security detection performance.

In Figure 4, we have combined the prediction error with the security detection performance for determining the improvements offered by implementing the TFT and the security module we proposed.

4.4 Discussion

The results of this comparison demonstrate the advantages offered by the proposed framework as it can reach lower energy consumption and carbon emissions and lower security risks while maintaining the resource usage within acceptable bounds. The TFT-based configuration achieved lower MAE and RMSE than the LSTM-based baseline, showing lower prediction error under the evaluated conditions.

5. CONCLUSION

The suggested Digital Twin framework assisted by AI combines TFT-sourced predictions, detection of security anomalies and optimization through multiple objectives, making it secure and eco-friendly in using a data center. The framework views energy consumption, carbon emissions, safety risks, utilization of resources, and functioning of a system jointly, thus providing one solution for optimizing data centers. Further research will be directed towards implementation of the framework in real data centers while optimizing their work in dynamics.

6. REFERENCES

- [1] R. H. de Souza Gonçalves and W. M. dos Santos, "A scalable Digital Twin framework for energy optimization in data centers," arXiv preprint arXiv:2605.05581, 2026.
- [2] S. A. Jadhav and Z. Liu, "Digital Twin-based cooling system optimization for data center," arXiv preprint arXiv:2603.01198, 2026.
- [3] A. A. Hamwi and M. Mittal, "FL-TWIN: A unified federated learning system for intrusion detection with digital twins modelling," *Scientific Reports*, vol. 16, Art. no. 28249, 2026.
- [4] A. Sayghe, "Digital Twin-driven intrusion detection for industrial SCADA: A cyber-physical case study," *Sensors*, vol. 25, no. 16, Art. no. 4963, 2025.
- [5] X. Zhan, X. Zhu, P. Cheng, X. Hu, Z. He, H. Geng, J. Leng, H. Zheng, C. Liu, T. Hong, Y. Liang, Y. Liu, and F. Zhao, "Data center cooling system optimization using offline reinforcement learning," in *Proc. Int. Conf. Learn. Representations (ICLR)*, 2025.
- [6] L. Leindals, P. Grønning, D. F. Dominković, and R. G. Junker, "Context-aware reinforcement learning for cooling operation of data centers with an aquifer thermal energy storage," *Energy and AI*, vol. 17, Art. no. 100395, 2024, doi: 10.1016/j.egyai.2024.100395.
- [7] E. Taheri et al., "DyTwin: Federated Adaptive Digital Twins for Data Centers – Visualization and Anomaly Detection," in *Proc. SC24-W*, 2024, pp. 847–852, doi: 10.1109/SCW63240.2024.00120.
- [8] "Digital Twin of a data center at an educational institution," *Journal of Engineering Research*, vol. 11, no. 1, pp. 57–67, 2023, doi: 10.36909/jer.15973.